RODO - GDPR

PRZEDMIOT I CELE

ZAKRESY

PRAWA I WOLNOŚCI

DEFINICJE

Jakub Rzymowski

UNIWERSYTET MEDYCZNY W ŁODZI

RODO – GDPR

PRZEDMIOT I CELE, ZAKRESY, PRAWA I WOLNOŚCI, DEFINICJE

Jakub Rzymowski

Uniwersytet Medyczny w Łodzi

Numer ORCID 0000-0003-0538-8895

Recenzja naukowa:
Profesor zwyczajny
Doktor habilitowany **Zdzisław Brodecki**

Autor jest adiunktem w Katedrze Europejskiego Prawa
Gospodarczego Wydziału Prawa i Administracji
Uniwersytetu Łódzkiego.

Projekt okładki: Magdalena Rzymowska

ISBN 978-83-953697-9-7

Wydawca:
Uniwersytet Medyczny w Łodzi

Wydanie I, Łódź 2020

Spis treści

Wstęp

Wstęp

Rola RODO

RODO jest częścią prawa ochrony danych osobowych. Uważam, że takie sformułowanie jest uprawnione. Uprawnione z dwóch względów.

Po pierwsze, istnienie prawa ochrony danych osobowych, rozumianego jako ogół przepisów poświęconych ochronie danych osobowych, jest niewątpliwe. Z uwagi na dużą ilość przepisów, rozsianych po różnych aktach prawnych – przepisów, które bądź to poświęcone są ochronie danych osobowych, bądź to tej ochrony dotykają, bądź mimo że regulują coś innego niż ochrona danych osobowych, to na tę ochronę mają wpływ – dostrzegam w tym nurcie przepisów, osobną podgałąź prawa. RODO jest częścią tej podgałęzi. Można oczywiście prowadzić dyskusję, czy prawo ochrony danych osobowych to część dogmatyki prawa, rozumianej jako „trzon dyscyplin prawniczych", czy raczej „szczegółowa dyscyplina prawnicza", która do tego trzonu nie należy. Rozważania takie, oczywiście o charakterze ogólnym, prowadzi J. Wróblewski[1] - i właśnie autor ten zwraca uwagę na fakt, że należy pamiętać o historycznej zmienności tego, co wchodzi w zakres dogmatyki prawa. Innymi słowy, jedynie trywializując nieco wypowiedź J. Wróblewskiego: prawo ochrony danych osobowych kiedyś istotne nie było, teraz istotne się stało.

Po drugie, RODO odgrywa w prawie ochrony danych osobowych rolę szczególną. Jest to rola przepisów ogólnych tego prawa. Stanisław Kasznica pisał, że: „Szczególnie dotkliwie daje się odczuwać brak części ogólnej, zawierającej podstawowe pojęcia i przewodnie zasady, a także brak kodyfikacji ogarniającej całokształt tego prawa."[2]. Pisał to nie o prawie ochrony danych osobowych a o prawie administracyjnym. Uwaga S. Kasznicy odnosząca się do prawa administracyjnego nadal zachowuje aktualność. Jego myśl, która w zacytowanej uwadze przetrwała ponad 70 lat, może zostać wykorzystana w odniesieniu do prawa ochrony danych osobowych.

---

[1] J. Wróblewski w: W. Lang, J. Wróblewski [red.], S. Zawadzki, *Teoria państwa i prawa*, Warszawa 1979, s. 11.

[2] S. Kasznica, *Polskie prawo administracyjne. Pojęcia i instytucje zasadnicze*, Poznań 1946, s. 21.

Pozycja RODO w prawie ochrony danych osobowych jest szczególna, ma ono bowiem charakter przepisów ogólnych tego prawa. RODO ustanawia cały szereg uprawnień materialnych, jednak wielką jego rolę dostrzegam w tym, że dotyczy ono niemal całości („niemal" – z uwagi na wyłączenia) zjawiska rozumianego jako ochrona danych osobowych. RODO nadaje temu zjawisku ogólne ramy. Dzięki istnieniu RODO nie dostrzegamy braku przepisów ogólnych prawa ochrony danych osobowych. Oczywiście RODO mogłoby być sformułowane lepiej, bardziej ogólnie, krócej, bardziej lapidarnie, bardziej kompetentnie – jednak takie postulaty, o bardzo szczegółowym charakterze, stawiam dalej i tu świadomie ich nie precyzuję.

RODO mogłoby być lepsze. Mogłoby być, jednak jest jakie jest i to właśnie istnieniu RODO zawdzięczamy pewien ogólny ład w dziedzinie ochrony danych osobowych. RODO nie ma charakteru kodyfikacji. Z uwagi na fakt przenikania się prawa tworzonego przez instytucje UE z prawem tworzonym przez państwa członkowskie UE, kodyfikacja prawa ochrony danych osobowych wydaje się niemożliwa, a przynajmniej ogromnie trudna. Jednocześnie nie sposób nie zauważyć, że RODO zawiera podstawowe pojęcia istotne dla prawa ochrony danych osobowych oraz to co (inspirując się słowami S. Kasznicy[3]) nazwać można przewodnimi zasadami prawa ochrony danych osobowych. Smutnym skandalem jest sposób zdefiniowania niektórych zasad, faktem jednak jest, że ułomnie bo ułomnie zdefiniowane, ale jednak zasady te są obecne. Słowa o smutnym skandalu mogą się wydawać nadmierne, jednak publikacja niniejsza powstaje równolegle z publikacją, w której właśnie zasady są analizowane. Zasady te są ważne i doniosłe, co więcej – porządkują system ochrony danych osobowych, jednak obstaję przy poglądzie, że zdefiniowane są one w sposób skandaliczny.

Jeśli chodzi o rolę RODO w systemie ochrony danych osobowych, to dostrzegam jeszcze jedno arcyciekawe zjawisko. Joanna Wyporska-Frankiewicz pisze: *Kodeks postępowania administracyjnego jawi się jako akt prawny zapewniający szeroką ochronę stronie postępowania. Jej pozycja została ukształtowana w sposób jasny i silny.*[4]. Taki sam charakter jak KPA w ujęciu cytowanej autorki ma

[3] S. Kasznica, *loc. cit.*

[4] J. Wyporska-Frankiewicz, *Pozostawienie podania bez rozpoznania w świetle przepisów kodeksu postępowania administracyjnego a standardy współczesnej admi-*

właśnie RODO. Stronę postępowania wystarczy zastąpić przez „osobę, której dane dotyczą", zaś „Kodeks postępowania administracyjnego" przez RODO i poza tym, reszta stwierdzenia zachowuje aktualność. Można wręcz posunąć się do strawestowania zdania J. Wyporskiej–Frankiewicz, by uzyskać zdanie: „RODO jawi się jako akt prawny zapewniający szeroką ochronę osobie, której dane dotyczą. Jej pozycja została ukształtowana w sposób jasny i silny."[5] Podobnie jak wyżej, można się zastanowić i tu nad jakością regulacji, można zadać sobie pytanie o to, czy tak poważne wzmocnienie pozycji osoby, której dane dotyczą, wobec administratora, jest celowe i słuszne. Można to uczynić, jednak wysokiej pozycji osoby, której dane dotyczą, zignorować nie sposób. Możemy w RODO dostrzec ukształtowanie pozycji prawnej osoby, której dane dotyczą, na drodze przepisów – przepisów, których realizacja zabezpieczona jest sankcjami.[6]

Konstrukcja pracy

Praca składa się z rozdziałów. Każdy rozdział poświęcony jest jednemu artykułowi RODO. Każdy rozdział składa się ze stałych elementów, a elementy te z uwagi na ich ułożenie i powtarzalność w kolejnych rozdziałach nazywam warstwami. Warstwy te wymieniam poniżej. Charakteryzuję je i omawiam jeszcze niżej, w pozycji: ***Uzasadnienie konstrukcji pracy i cele pracy***. Warstwy, które składają się na każdy rozdział można również nazwać podrozdziałami, jednak uważam, że określenie warstwy lepiej je charakteryzuje, z uwagi na odmienne cele, jakie pragnę zrealizować przy pomocy poszczególnych warstw - podrozdziałów. Podrozdziały to często po prostu kolejne jednostki redakcyjne tekstu, tu rola różnych poszczególnych kategorii podrozdziałów jest odpowiednio różna. W samej publikacji nie posługuję się określeniami typu: „warstwa pierwsza, warstwa druga …", za to każdej warstwie nadałem nazwę np.: komentarz, analiza etc., i tej konwencji się trzymam. Podejście takie może wiąże

---

nistracji, w: *Standardy współczesnej administracji i prawa administracyjnego*, red. nacz. Z. Duniewska, M. Stahl, A. Rabiega-Przyłęcka, Warszawa-Łodź 2019, s. 449.

[5] Zdania te ujmuję w cudzysłów, mimo że nie są cytatem z pracy J. Wyporskiej-Frankiewicz, ale są cytatu tego adaptacją; ponieważ zaś są adaptacją, nie przypisuję sobie ich autorstwa, niejako odkładając na bok sprawę dzieła oryginalnego, i dzieła inspirowanego.

[6] Por. J. W. Salmond, *The first principles of jurisprudence*, London 1893, s. 18.

nieco ręce, jednak jednocześnie przymusza do dokładnej analizy przepisów, które są przedmiotem namysłu. Dokładna analiza jest zresztą tym, co podczas pisania pracy i towarzyszących jej prac kolejnych szczególnie leży mi na sercu. Marek Zirk-Sadowski pisze, że *(...) na zawodzie tym ciąży szczególna odpowiedzialność za prawidłowe działanie państwa i mechanizmów społecznych*.[7] Cytowany autor pisze tu o zawodzie prawnika, dalej zaś pisze o monteskiuszowskim podziale władzy, w którym sądy są jedną z trzech władz. Uważam, że pogląd M. Zirk-Sadowskiego ma wymiar o tyle uniwersalny, że można odnieść go do każdego prawnika. Prawnik – każdy prawnik – sprawuje pewną władzę. Istotą tej władzy jest to, że prawnik dokonuje interpretacji przepisu. Powinno to rodzić świadomość związanej z tym odpowiedzialności, którą M. Zirk-Sadowski nazywa szczególną.

W związku z tą odpowiedzialnością, podejmuję dostępne mi kroki, by odczytać treść poszczególnych przepisów, jednak odczytać tę treść w sposób, który nie wypacza intencji prawodawcy w tych przepisach zapisanej. Uświadomienie sobie tej odpowiedzialności prowadzi do wniosku, że zadanie, którego podejmuje się odpowiedzialny prawnik, jest karkołomne. Prawodawca zapisuje przepis, prawnik odczytuje treść przepisu i ustala jego znaczenie, ustala je w sposób możliwie bliski temu, co w przepisie zapisał prawodawca, jednak jednocześnie jest w stanie ustalić to, co zapisał prawodawca, jedynie dzięki odczytaniu treści przepisu i ustaleniu jego znaczenia. Jak widać, kształtuje się tu swoiste błędne koło, wydaje się jednak, że nie ma możliwości wyjścia poza nie. Zdając sobie z tego sprawę, jedynym co można tu zrobić jest uczciwe, szczegółowe, drobiazgowe i w ogóle jak najbardziej precyzyjne odczytanie przepisu, po to by prawidłowo ustalić jego treść.

O twórczej interpretacji prawa pisze T.T. Koncewicz[8]. Autor ten odnosi słowa o tej interpretacji do sędziów. RODO stawia przed sędziami poważne wyzwania. Czy karać za niezrealizowanie źle napisanych przepisów? Czy karać za zrealizowanie przepisów, których zrealizować się nie da? Czy karać za niewłaściwą realizację przepisów, które zawierają elementy ocenne? Przed sędziami stoją tu wiel-

[7] M. Zirk-Sadowski, *Wprowadzenie do filozofii prawa*, Kraków 2000, s. 18.

[8] T.T. Koncewicz w: *Europa Sędziów*, pod red. Z. Brodeckiego, Warszawa 2007, s. 25.

kie wyzwania i uważam, że praktyka sędziowska powinna – na gruncie RODO – uświadomić prawodawcy, że RODO w postaci w jakiej musimy je stosować to to hybryda Hydry i prawa. Tak widzę tu rolę sędziów. Rola pozasądowych interpretatorów RODO jest jednak inna, muszą oni RODO odczytać, odczytać i zastosować, jednak bez elementu kreacyjnego w wykładni – ten trzeba pozostawić prawodawcy a wcześniej sędziom. Takie podejście skłoniło mnie właśnie do nadania pracy struktury warstwowej – to na poziomie pracy, jak również do zastosowania etapowej analizy semantycznej, jako metody wykładni przepisów – to na poziomie każdego przepisu, a nawet każdej jednostki redakcyjnej przepisu.

Jednocześnie założyłem, że przyjęcie warstwowej konstrukcji pracy nadaje jej, oprócz waloru pracy prawniczej, walor prawoznawczy, zwłaszcza z uwagi na usystematyzowanie wypowiedzi na temat prawa obowiązującego.[9] Założeniem moim było, by praca była znacząca dla różnych kategorii czytelników – zarówno dla tych, którzy szukają informacji o prawie i wskazówek dotyczących jego stosowania, jak i tych, którzy szukają informacji o niedoskonałościach przepisów i wskazówek dotyczących możliwości usunięcia tych niedoskonałości. Należy przy tym zwrócić uwagę na fakt, że niedoskonałości przepisów mają pewną wagę również dla praktyków. Jeżeli przepis jest źle napisany, jeżeli nie wiadomo jakie obowiązki z niego wynikają, lub przynajmniej jeżeli nie wiadomo tego z dużą dozą pewności, to ukaranie za niezrealizowanie takiego przepisu zdaje się być niemożliwe.

Poniżej wymieniam poszczególne warstwy.

- **Warstwa pierwsza** – ***Komentarz***. Warstwa ta powstaje jako druga, jednak dla jasności wywodu zapisana jest w każdym rozdziale jako pierwsza. Jednocześnie umieszczenie tej warstwy jako pierwszej pozwala na korzystanie z niniejszej publikacji jako z komentarza do czterech pierwszych artykułów RODO. Publikacja nie została pomyślana jako komentarz, komentarz jest jej częścią, jeżeli jednak Czytelnik nie jest zainteresowany rozważaniami prowadzonymi w kolejnych warstwach każdego rozdziału, to warstwę pierwszą i drugą może potraktować jako komentarz.

[9] J. Wróblewski, *op. cit.* s. 7.

- **Warstwa druga** – ***Analiza***. Warstwa ta powstaje jako pierwsza. Od jej napisania zaczynam pracę nad każdym rozdziałem.
- **Warstwa trzecia** – ***Uwagi***.
- **Warstwa czwarta** – ***Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa***.
- **Warstwa piąta** – ***Konkretyzacja zasad*** (zasady).
- **Warstwa szósta** – ***Postulaty de lege ferenda***.
- **Warstwa siódma** – ***Rozważania historyczne***.

Dla przyjętej struktury publikacji widzę uzasadnienie w konieczności odróżnienia dwóch rodzajów zastosowanej metodologii nauk prawnych. Wersji opisowej i wersji dyrektywalnej.

W wersji opisowej metodologii nauk prawnych, badacz odnosi się do tego „jak jest" czyli odnosi się do badanego tekstu prawnego w ten sposób, że ustala jakie uprawnienia i obowiązki z danego tekstu prawnego wynikają.

W wersji dyrektywalnej metodologii nauk prawnych, badacz odnosi się do tego „jak być powinno" czyli odnosi się do badanego tekstu prawnego w ten sposób, że wskazuje jakie uprawnienia i obowiązki z danego tekstu prawnego wynikać powinny.

O zjawisku dwoistej metodologii nauk prawnych pisze Z. Ziembiński, z tym że odnosi się on do nauk prawnych w ogólności, a nawet do badania tych nauk.[10] Twierdzenia jego odnoszą się do metanauki prawa. Badania moje, ze względu na tematykę pracy, odnoszą się do konkretnego prawa, a właściwie nawet do jego wycinka uregulowanego na gruncie RODO. Namysł metodologiczny ma charakter meta (metanamysłu) wobec metod analizy przedmiotu badań w poszczególnych kategoriach rozdziałów.

[10] Z. Ziembiński, *Problemy podstawowe prawoznawstwa*. Warszawa 1980, s. 58.

Cele poszczególnych kategorii podrozdziałów

W poszczególnych rozdziałach pracy realizowane są różne cele. Nie są to cele tożsame z celami pracy, o których piszę w Rozdziale 1, zatytułowanym: *Cele pracy i uzasadnienie konstrukcji pracy*.

Cel podrozdziałów warstw: *Analiza* oraz *Komentarz*.

W podrozdziałach warstwach-kategoriach *Analiza* i *Komentarz* realizowany jest cel, który ogólnie można nazwać celem komentarzowym. W ujęciu Z. Ziembińskiego jest to cel opisowy. Tu jednak właściwy opis znajduje się w podrozdziałach z warstwy-kategorii *Komentarz*. W podrozdziałach warstwy-kategorii *Analiza* znajduje się, zgodnie z nazwą tych rozdziałów, analiza tekstu prawnego przeprowadzona metodą Etapowej Analizy Semantycznej.

Podobne podejście do analizy prawa znaleźć można u J. Wróblewskiego. Jerzy Wróblewski pisze, że: *Analiza (...) przebiega na różnych szczeblach" i oddziela dogmatyczną analizę prawa od analizy „na szczeblu teoretycznoprawnym*.[11]

Cel podrozdziałów warstwy: *Uwagi*

Podrozdziały warstwy-kategorii *Uwagi* realizują cel, który w odniesieniu do aparatury pojęciowej Z. Ziembińskiego wręcz doprasza się o rozszerzenie tej aparatury o dodatkowe pojęcie, a mianowicie o pojęcie rozszerzonego celu opisowego. Nie jestem zwolennikiem wprowadzania nowych pojęć, uważam jednak, że przy opisie zjawiska ważne jest, by zjawisko to opisać w sposób możliwie adekwatny, z tego właśnie względu wszelkie rozważania, które nie mają charakteru ścisłej analizy tekstu prawnego, umieściłem w podrozdziałach warstwy-kategorii *Uwagi*, miast umieszczać je w podrozdziałach warstwy-kategorii *Analiza*, a skoro zawartość poszczególnych warstw jest odmienna, to odmienne ich tytułowanie okazało się koniecznością

Jak wskazuję wyżej, rozważania umieszczone w podrozdziałach warstwy *Uwagi* nie mają charakteru ścisłej analizy tekstu prawnego, ponieważ odnoszę się w nich również do poglądów doktryny. Tam, gdzie uważam to za właściwe, do poglądów tych odnoszę się

[11] J. Wróblewski, *Zagadnienia procesowego modelu stosowania prawa.* Studia Prawnicze. Zeszyt 1 – 2 (87 – 88) 1986, s. 3-29.

aprobatywnie. Aprobatywnie do tego stopnia, że niektóre z poglądów rozwijam lub uzupełniam. Tam, gdzie uważam to za właściwe, odnoszę się do poglądów doktryny w sposób polemiczny. Dyskusja, czy to aprobatywna, czy to polemiczna, z poglądami doktryny, nie jest jedynym celem jaki realizuję w rozdziałach warstwy Uwagi. Poszczególne podrozdziały warstwy Uwagi poświęcone są rozmaitym zagadnieniom związanym z przepisami którym dane rozdziały odpowiadają. Realizuję tam zatem cel opisowy, z tym, że właśnie jak piszę wyżej, rozszerzony cel opisowy, opisuję bowiem nie tylko to co wynika z samego tekstu prawnego (opisowi są poświęcone podrozdziały warstwy Analiza), ale odnoszę się również do kwestii teoretycznoprawnych, oraz do zagadnień o charakterze praktycznym.

Cel podrozdziałów warstwy:
Podsumowanie w duchu konceptualizmu prawniczego
– ogólnej teorii prawa

Cel podrozdziałów warstwy *Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa* jest nieco bardziej złożony. Obecny jest tu element opisowy, wskazuję bowiem w tych podrozdziałach jakie obowiązki i jakie uprawnienia wynikają z konkretnych analizowanych przepisów RODO. Wskazanie praw i obowiązków wynikających z konkretnych przepisów RODO, odbywa się w podrozdziałach tej warstwy w pewnym założonym porządku, który polega na tym, że w podrozdziałach tej warstwy wskazuję jaki obowiązek, a następnie jakie uprawnienie wynikają z kolejnych przepisów RODO.

Podkreślam, że zgodnie z wypracowaną na gruncie konceptualizmu prawniczego metodą wykładni, w odniesieniu do każdego przepisu RODO wskazuję zarówno prawo jak i obowiązek, które z tego przepisu wynikają, niezależnie od językowego ujęcia przepisu, czyli innymi słowy: niezależnie od tego czy w warstwie językowej przepis nakłada obowiązek na administratora lub na podmiot przetwarzający, czy w warstwie językowej przepis przyznaje uprawnienie osobie której dane dotyczą, analiza przepisu przeprowadzona w warstwie *Analiza* i podsumowana w warstwie *Komentarz* pozwala, w odniesieniu do każdego z analizowanych przepisów, ustalić jakie prawa i obowiązki z niego wynikają, niezależnie od tego jak w sensie redakcyjnym prawodawca sformułował przepis.

Obecny jest tu również element dyrektywalny, element ten jest nieco słabszy od elementu opisowego w rozdziałach warstwy Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa, odnoszę się w nich bowiem do badanego tekstu prawnego i wskazuję jakie uprawnienia i obowiązki z tego tekstu wynikają. Uważam jednak, że element dyrektywalny jest tu również obecny – nie widzę bowiem powodu, dla którego konkretne przepisy prawa, w tym przypadku przepisy RODO, nie mogłyby być sformułowane w taki sposób, by jasne było, na kim jaki obowiązek spoczywa, a właściwie jaki dokładnie obowiązek spoczywa na administratorze oraz komu jakie uprawnienia przysługują, a szczególnie jakie dokładnie uprawnienia przysługują osobie, której dane dotyczą. Powiem więcej, uważam, że przepisy tak właśnie powinny być napisane. W tym właśnie dostrzegam element dyrektywalny opisywanej warstwy. Piszę tu oczywiście o elemencie dyrektywalnym z punktu widzenia podejścia o charakterze meta (metapodejścia) do rozważań nad konkretnym prawem. Zwracam na to uwagę, ponieważ w analizowanej warstwie obecny jest element wskazania adresatów przepisów czy adresatów norm (jak powiedziałby normatywista), oraz wskazania jakie obowiązki na nich spoczywają i jakie uprawnienia im przysługują.

Odkładając na chwilę podział na podejście opisowe i podejście dyrektywalne, uzupełniam, że w podrozdziałach warstwy-kategorii: Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa zrealizowany jest jeden jeszcze cel. W podrozdziałach tej warstwy, w odniesieniu do konkretnych analizowanych przepisów, wskazuję, że teoria znajdująca się w tytule każdego podrozdziału-warstwy, czyli konceptualizm prawniczy – ogólna teoria prawa, nie jest teorią pustą, konceptualizm prawniczy umożliwił bowiem wypracowanie metody, która pozwala na powtarzalną, a przede wszystkim jasną i czytelną analizę, jak się wydaje, każdego przepisu prawa, czyli Etapowej Analizy Semantycznej.

Konceptualizm Prawniczy jako Ogólna Teoria Prawa jest moją autorską teorią obowiązywania i wykładni prawa. Po raz pierwszy teoria ta została ogłoszona w trakcie XX Jubileuszowego Zjazdu Katedr Teorii i Filozofii Prawa, który miał miejsce w dniach 6-9 września 2012 roku w Łodzi. Teoria ta oparta jest o koncepcję powszechników w ujęciu Arystotelesa i Piotra Abelarda. Osią teorii jest stanowisko, zgodnie z którym prawa takie jak np. prawo własności istnieją o tyle, o ile przejawiają się w poszczególnych prawach własności

(uprawnieniach), które przysługują poszczególnym ludziom do poszczególnych rzeczy – jest to element czerpiący z teorii powszechników czyli uniwersaliów w ujęciu Arystotelesa. Jednocześnie prawa te istnieją w rozumach ludzi, którzy rozumieją istotę tych praw – jest to element czerpiący z teorii powszechników w ujęciu Piotra Abelarda. W przepisach zapisane są uprawnienia. Ustalając znaczenie przepisów, ustalamy treść uprawnień, które są w przepisach zapisane. Jednocześnie uprawnienia te są cechami osób fizycznych (jak się wydaje czasem również osób prawnych i innych podmiotów). Cechami, takimi jak wzrost, płeć czy uroda. Cechami, o których można powiedzieć, że są osobie fizycznej przypisane w sposób naturalny, nie są jej one przez nikogo nadane. Z uprawnień tych wynikają obowiązki. Nie ma problemu z przejściem ze sfery powinności do sfery bytu, ponieważ w duchu filozofii Parmenidesa, zarówno uprawnienia, jak i osoby, w umysłach których uprawnienia te się znajdują i konkretyzują, jak i osoby, którym uprawnienia te przysługują, należą do bytu. Byt jest jednolity, nie ma stopni, przerw ani różnic. Uprawnienia są częścią bytu podobnie jak ludzie, którym przysługują. W jednolitym, parmenidejskim ujęciu bytu, wydaje się tkwić pewna intuicja – intuicja, zgodnie z którą myśli ludzkie są w jakimś sensie (na poziomie zjawisk atomowych w mózgu) fizykalne. Z drugiej strony zarówno ludzie, jak i otaczający ich świat są jakąś formą energii, co również przemawia za parmenidejską jednolitością bytu.

Cel podrozdziałów warstwy: *Konkretyzacja zasad*

Podrozdziały warstwy-kategorii ***Konkretyzacja zasad***, z metodologicznego punktu widzenia realizują cel opisowy. W rozdziałach tych wskazuję, które przepisy szczegółowe RODO i w jaki sposób, służą realizacji których zasad. Rozdziały tej warstwy mają pewien walor praktyczny. Przypominam, że na administratorze spoczywa obowiązek realizacji zasad zapisanych w artykule 5 RODO i że na administratorze spoczywa obowiązek wykazywania realizacji tych zasad. Zasady, o których tu mowa, podlegają realizacji przez przepisy szczegółowe RODO – w ogólnym zarysie przez przepisy od art. 6 RODO do art. 38 RODO (w szerszym ujęciu do art. 50 RODO). Administrator zatem, który pragnie zrealizować konkretną zasadę, musi zrealizować odpowiadające tej zasadzie (czy, jak to nazywam w tekście publikacji: konkretyzujące tę zasadę) przepisy szczegółowe

RODO. Żeby zrealizować przepisy szczegółowe RODO odpowiadające konkretnej zasadzie, administrator musi wiedzieć, które przepisy której zasadzie odpowiadają. Tego właśnie administrator dowiedzieć się może z podrozdziałów warstwy: ***Konkretyzacja zasad.***

Obowiązek wykazania realizacji zasady przekłada się na obowiązek wykazania realizacji przepisów, które tej zasadzie odpowiadają, czyli które tę zasadę konkretyzują. I znowu: w podrozdziałach tej warstwy dostrzec można również pewien ślad podejścia dyrektywalnego, nie widzę bowiem powodów, dla których nie miano by przy konkretnych przepisach w tekście prawnym umieścić wskazań, które zasady są przez dany przepis realizowane. Niestety, jak widać, prawodawca powody te widział…

Cel podrozdziałów warstwy: *Postulaty de lege ferenda*

Podrozdziały warstwy: ***postulaty de lege ferenda*** realizują głównie, o ile nie jedynie, cele dyrektywalne. W rozdziałach tych wskazuję jak, moim zdaniem, kolejne przepisy RODO brzmieć powinny. Oczywiście czynię to jedynie w przypadkach, w których uważam, że brzmienie przepisów jest niewłaściwe, niejasne, złe.

Cel podrozdziałów warstwy: *Rozważania historyczne*

Podrozdziały warstwy-kategorii: ***Rozważania historyczne*** realizują głównie cel opisowy. W podrozdziałach tej warstwy wskazuję przede wszystkim na to, jakie przepisy *Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*[12] i jakie przepisy *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*[13] odpowiadają przepisowi RODO, który jest podstawą namysłu w danym rozdziale. Tam, gdzie uważam to za konieczne, wskazuję na czynniki historyczne, na przykład na historyczne poglądy doktryny. Warstwa ta, nie bez powodu, znajduje się na końcu każdego rozdziału, mimo mojego

[12] *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, 23.11.1995, OJ 281/31. (Dalej: Dyrektywa 95/46/WE).

[13] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz.U. 1997 nr 133 poz. 883. ze zm. t.j. Dz.U. 2016 poz. 922. ze zm. (Dalej: UODO97).

szacunku dla dorobku doktryny, nie uważam, iżby był sens upartego trzymania się doktryny, zwłaszcza w sytuacji pojawienia się nowego prawa. Prawo zmieniło się radykalnie, w związku z tym, pracę nad nim trzeba niejako zacząć od nowa, dlatego też każdy rozdział zaczynam analizą i komentowaniem przepisu, od których podążam dalej z wywodami, zaś odniesienia do poprzedniego stanu prawnego traktuję jedynie sygnalnie.

Uzasadnienie konstrukcji pracy i cele pracy

Uzasadnienie konstrukcji pracy i cele pracy

Uzasadnienie konstrukcji pracy

Praca niniejsza jest jednym z kilku elementów większego założenia badawczo-naukowo-wydawniczego. Celem założenia largo jest analiza RODO i zbadanie wewnętrznej jego spójności. W tej części prezentuję analizę RODO, zaś zbadanie wewnętrznej spójności RODO jest celem jaki zakładam do realizacji w ostatniej planowanej pracy z cyklu.

Jako pierwszy, wydany w formie książkowej, element tego założenia, powstała praca: *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. W książce tej, na co wskazuje tytuł, omawiam dokumentację związaną z przetwarzaniem danych osobowych, zwracam przy tym uwagę na fakt, że ta właśnie dokumentacja jest najlepszym narzędziem realizacji zasady rozliczalności, która wynika z art. 5 ust. 2 RODO.

Niniejsza praca poświęcona jest analizie zakresów obowiązywania RODO i podstawowym definicjom, które w RODO występują. Jednak celem pracy nie jest jedynie analiza przepisów prowadzona w sposób, w jaki prowadzi się zwykle analizę w komentarzach do aktów prawnych. Cele tej pracy są inne, omawiam je poniżej w odniesieniu do poszczególnych elementów formalnych, które składają się na każdy rozdział pracy. Jeszcze niżej, dla porządku, w podrozdziale ***Cele pracy*** cele te wymieniam już bez drobiazgowego ich omawiania, które to omawianie odbywa się w podrozdziale niniejszym.

Treść przepisu

Pierwszym elementem każdego rozdziału jest omawiany przepis. Uznałem, że umieszczenie przepisu na początku rozdziału ułatwi lekturę rozdziału. Poza tym z uwagi na fakt, że przyjąłem etapową analizę semantyczną, jako podstawową metodę analizy przepisu, uznałem, że dobrze by czytelnik publikacji mógł na bieżąco konfrontować wnioski z analizy przepisu umieszczone w pozycji *Komentarz*, z treścią przepisu analizowanego w pozycji *Analiza*.

Analiza tekstu prawnego RODO jako cel pracy

Analiza tekstu prawnego **nie jest podstawowym celem pracy**, jest jednak narzędziem, które pozwala na prowadzenie dalszych rozważań, niżej wyjaśniam, dlaczego uważam, że drobiazgowa analiza tekstu prawnego jest konieczna dla namysłu nad prawem.

Jestem zwolennikiem rozpoczynania rozważań prawniczych od drobiazgowej analizy tekstu prawnego. Uważam, że w pułapkę może wpaść badacz, który badania prawa opiera wyłącznie na cudzej analizie tekstu prawnego. Badacz taki nie poznaje tekstu prawnego, nie dowiaduje się ani nie ustala, co z tekstu prawnego wynika, a zamiast tego dowiaduje się tego, co inni badacze uważają na temat tekstu prawnego będącego przedmiotem jego namysłu. Nie zniechęcam oczywiście, do zapoznawania się z poglądami doktryny, do analizowania tych poglądów, do rozwijania tych poglądów ani do polemiki z nimi. Czynności te są konieczne - jednak uważam, że analiza tekstu prawnego nie powinna się od nich zaczynać. Uważam, że jeżeli badacz rozpoczyna analizę tekstu prawnego od analizy poglądów doktryny, to ryzykuje on, że kiedy przystąpi do właściwej, czyli własnej analizy tekstu prawnego, to będzie on patrzył na ten tekst przez pryzmat cudzych analiz. Badacz może w takiej sytuacji patrzeć przez pryzmat cudzej analizy w sposób wobec niej aprobatywny lub polemiczny, może rozwinąć poglądy poprzedników, jednak traci szansę na własną, autonomiczną analizę przepisu.

Prezentacja etapowej analizy semantycznej, jako cel pracy

By ustrzec się przed wpadnięciem we wskazaną wyżej pułapkę, w publikacji niniejszej (jak i w pozostałych publikacjach serii), dokonuję właśnie drobiazgowej analizy tekstu prawnego, będącego przedmiotem mojego namysłu.

Analizy tej dokonuję za pomocą metody, którą nazywam etapową analizą semantyczną[14]. Metoda ta, polega na analizie kolejnych

[14] Etapową Analizę Semantyczną zaprezentowałem w toku konferencji naukowej, połączonej ze zjazdem Stowarzyszenia FONTES, który odbył się 6 listopada 2020 on line. Konferencja nosiła tytuł *Legislacja w czasach kryzysu państwa prawnego*. Wykład miałem zaszczyt wygłosić w sesji plenarnej zatytułowanej *Aksjologia inicjatyw legislacyjnych w dobie lęku przed nieznanym*. Sesję moderował prof. dr hab. P. Chmielnicki. Wcześniej ww metoda była wykorzystywana na łamach książki J. Rzymowskiego, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*, Kraków 2019.

fragmentów przepisu, jednak na analizie poprzedzonej szczegółowym podziałem przepisu. Podziałem na fragmenty, które nadają się do omówienia. Czasem są to zwroty, zestawienia słów, czasem pojedyncze litery, spójniki etc. Do analizy przystępuję po podzieleniu przepisu na fragmenty i zaopatrzeniu tych fragmentów w zwroty wprowadzające i w zwroty łączące.

Podzielenie przepisu w taki sposób, żeby żaden fragment, żadne słowo ani znak z przepisu nie zostały pominięte, zabezpiecza przed przypadkowym lub intencjonalnym pominięciem analizy jakiegokolwiek, najmniejszego nawet, fragmentu przepisu.

Kluczem do podziału przepisu na fragmenty, które podlegają analizie, jest możliwość ustalenia ich znaczenia, w oderwaniu od pozostałych fragmentów przepisu. Pozostałe fragmenty przepisu są analizowane w ten sam sposób. Zastosowanie w pracy etapowej analizy semantycznej pozwala mi na zaprezentowanie tej metody analizy tekstu prawnego i to od razu w postaci zaaplikowanej do analizy konkretnych przepisów.

Etapowa analiza semantyczna to metoda wykładni rozumianej – odwołując się do terminologii użytej przez S. Wronkowską[15] – jako proces zmierzający do zrozumienia przepisów prawnych, czyli wykładnia w sensie pragmatycznym, czyli interpretowanie prawa.

Warstwa - *Analiza*

Warstwa ***Analiza*** występuje w każdym rozdziale na drugiej pozycji, jednak powstaje jako pierwsza.

W pozycji tej (warstwie-podrozdziale) prowadzę analizę przepisu. Jednym z **celów pracy jest prezentacja etapowej analizy semantycznej**. Z tego względu, przy analizowaniu kolejnych przepisów, używam różnych zwrotów, które łączą ujęty w cudzysłów analizowany fragment przepisu z właściwą analizą przepisu. Stosując te metodę, używam różnych zwrotów łączących. W niniejszej publikacji, przy analizie kolejnych przepisów używam zwrotów: „wnioskujemy, że", „należy wnosić, że", „wynika, że", „wnosimy, że". Ta różnorodność wprowadza więcej możliwości komunikacyjnych i jest zastosowana świadomie. Świadomie użyłem różnych zwrotów łączących, aby wskazać ewentualnym naśladowcom, że metody tej można

[15] S. Wronkowska. Podstawowe pojęcia prawa i prawoznawstwa. Poznań 2005. s. 76.

używać niezależnie od stosowanego zwrotu łączącego. Tytułem uzupełnienia dodam, że przy stosowaniu przyjętej metody analizy, można nie stosować żadnego zwrotu łączącego. Można, po cudzysłowie zamykającym analizowany fragment przepisu, postawić kropkę, po czym rozpocząć pierwsze zdanie danego etapu analizy semantycznej. Tak jak piszę wyżej, prezentacja etapowej analizy semantycznej jest jednym z celów pracy. Celem pracy jest nie tylko prezentacja metody, ale i przekonanie ewentualnych naśladowców, że metoda naprawdę pozwala na sprawną, drobiazgową analizę przepisu.

Przyjęcie etapowej analizy semantycznej, jako podstawowej metody analizy przepisu pozwala badaczowi na ustrzeżenie się przed pewnym niebezpieczeństwem. Niebezpieczeństwo to pojawia się kiedy badacz przeczyta literaturę dotyczącą przepisu, który jest przedmiotem jego badań, wcześniej niż dokona własnej analizy przepisu. W takiej sytuacji badacz patrzy na przepis przez pryzmat lektur, które na temat danego przepisu przeczytał, czyli w istocie, przez pryzmat poglądów i wiedzy autorów tych lektur. Metaforycznie rzecz ujmując, badacz nie patrzy wtedy na przepis własnymi oczami, ale oczami wcześniejszych badaczy. Spoglądanie cudzymi oczami może spowodować, że badacz nie wyjdzie w swoich rozważaniach poza rozważania prowadzone przez poprzedników. Nie wyjdzie ponieważ podlegnie sugestii, że z analizowanego przepisu wynika to, co zauważyli poprzednicy badacza. Oczywiście, zwykle tak jest, zwykle poprzednicy badacza, trafnie zauważyli co wynika z przepisu, może się jednak zdarzyć inaczej. Może się zdarzyć, że poprzednicy badacza powtarzają błąd, który popełnił jeden z pierwszych badaczy danego przedmiotu. Powtarzają, ponieważ sami wpadli w pułapkę, przed wpadnięciem w którą ja staram się ustrzec dzięki stosowaniu swojej metody. Może się też zdarzyć, że poprzednicy badacza nie popełniają żadnego konkretnego błędu, a jedynie, w sposób swoiście niewolniczy, powtarzają różnymi słowami tę samą analizę przepisu, a tym samym, mimo, że nie popełniają konkretnego błędu, to jednocześnie nie są w stanie poczynić postępu w badaniach nad danym tekstem prawnym, żyją bowiem w wygodnym przeświadczeniu, że wszystko zostało powiedziane, ustalone i zbadane. Etapowa analiza semantyczna, stosowana konsekwentnie, pozwala ustrzec się również przed tym niebezpieczeństwem – drobiazgowa analiza tekstu, każdego jego słowa, potrafi zaprowadzić w rejony, w których nikt nie był, co jest może ryzykowne, ale na pewno ciekawe i jak sądzę – wartościowe.

Tytułem uzupełnienia rozważań dotyczących etapowej analizy semantycznej, podkreślam, że w żadnym wypadku nie jestem zwolennikiem lekceważenia głosu doktryny, który zwykle jest doniosły, bez względu na treść. Jeżeli poprzednicy badacza prowadzą trafne rozważania, to badacz powinien się do nich w ten czy inny sposób odnieść, lub przynajmniej zaznaczyć, że jest ich świadom, że jest świadom, że nie kroczy po „ziemi nieznanej". Jeżeli poprzednicy badacza prowadzą rozważania obciążone błędami, to badacz powinien wykazać te błędy i ewentualnie zaprezentować własne poglądy na kwestie będące przedmiotem błędnych, w jego opinii rozważań. Jeżeli poprzednicy badacza prowadzą rozważania, które może nie są błędne, ale badacz posiada inne poglądy na kwestie będące przedmiotem rozważań, to badacz powinien swoje poglądy zaprezentować i uzasadnić. Jeżeli wreszcie poprzednicy badacza, prowadzą rozważania niepełne, niedokończone, niepodsumowane, niekompletne, to badacz powinien te rozważania dopełnić, dokończyć, podsumować, uzupełnić.

Metodą, która jest stosowana często w rozważaniach filozoficznych, uważam jednak, że w rozważaniach prawniczych też może, a nawet powinna ona być stosowana, jest kontynuowanie rozważań w miejscu, w którym ukończył je poprzednik badacza. Niestety kontynuowanie rozważań jest czasem trudne, z uwagi na opisane przeze mnie wyżej, spoglądanie na przepis oczami poprzednika. Na przepis należy spojrzeć najpierw własnymi oczami, wynik tego spojrzenia zapisać, po czym zapoznać się z rozważaniami poprzedników i skonfrontować te rozważania z własnymi rozważaniami.

Jak z powyższych rozważań wynika, **celem publikacji, realizowanym w warstwie *Analiza* jest drobiazgowa i dokładna analiza tekstu prawnego**. Analiza ta prowadzona jest z wykorzystaniem opisanej wyżej metody.

Ze względu na przekonanie o konieczności korzystania z dorobku doktryny i ze względu na szacunek do niej, w podrozdziałach *Analiza* odnoszę się miejscami do poglądów doktryny. Odnoszę się w pozycji *Analiza* do poglądów doktryny wtedy, kiedy są one zbieżne z moimi poglądami, lub wtedy kiedy są one rozbieżne z moimi poglądami, jednak kiedy konfrontacja poglądów doktryny z moimi poglądami nie wymaga dłuższych rozważań. Jeżeli wymaga, to prowadzę je w pozycji *Uwagi*.

Warstwa - *Komentarz*

Warstwa (podrozdział, pozycja) *Analiza* występuje w każdym rozdziale na drugiej pozycji, jednak powstaje jako pierwsza.

Po przeprowadzeniu analizy przepisu w warstwie *Analiza* przechodzę do kolejnego etapu omawiania przepisu, a mianowicie dokonuję skrótu rozważań prowadzonych na drodze etapowej analizy semantycznej. Usuwam części wprowadzające, usuwam cytowane i analizowane fragmenty przepisów, usuwam części łączące. Usuwam też część rozważań, zwłaszcza wtedy kiedy mają one charakter przekonywania do moich poglądów. Tekst, który otrzymuję w wyniku skrócenia rozważań prowadzonych w warstwie *Analiza*, umieszczam w warstwie *Komentarz*. Warstwa *Komentarz* pozwala mi zaprezentować moją interpretację przepisu w wersji spójnej, skróconej i nieco bardziej lapidarnej niż w warstwie *Analiza*. Podkreślam, że *Komentarz* nie stanowi wyczerpującego komentarza do analizowanego przepisu. Gdyby praca niniejsza była komentarzem do RODO, w dosłownym rozumieniu tych słów takim jak komentarze, do których się w publikacji odnoszę, to składałaby się z rozważań prowadzonych w warstwie *Analiza*, pozbawionych części wprowadzających, cytatów i części łączących, jednak nie skracałbym rozważań tak, jak skracam je w niniejszej publikacji na etapie redagowania warstwy *Komentarz*. Rozważania w części *Komentarz* skracam bez szkody dla jasności wywodu, ponieważ w wersji pełnej dostępne są w części *Analiza*. Warstwa *Komentarz* ma też charakter wniosku z pozycji *Analiza*. Zwracam na to uwagę pod koniec omawiania warstwy *Analiza,* ponieważ wniosek w warstwie *Komentarz* ma raczej charakter wniosku technicznego niż merytorycznego, raczej podsumowania analizy niż rzeczywistego z niej wniosku – wniosku rozumianego jako coś nowego co jest własnym wkładem autora w doktrynę.

Warstwa - *Uwagi*

Trzecią warstwą, (podrozdziałem) każdego rozdziału publikacji jest pozycja *Uwagi*.

W pozycji *Uwagi* zamieszczam rozważania, co do których podjąłem decyzję, że zaciemniłyby one rozważania prowadzone w pozycji Analiza, dlatego że ich zakres wykracza, mniej lub bardziej, poza samą analizę przepisu.

Pierwszym **celem tej pozycji jest umieszczenie rozważań własnych** – poczynionych na gruncie przepisu – co do których uznałem, że jednak wykraczają one poza zakres czystej analizy przepisu. Omawiam tam klauzule odsyłające znajdujące się w przepisie, dokonuję zestawień pojęć związanych z treścią przepisu, na przykład zestawienie praw i wolności wynikających z RODO w uwadze: ***3.5. Art. 1. Uwaga 5***. Jakie prawa i wolności można wskazać na gruncie RODO.

Drugim **celem tej pozycji jest prezentacja poglądów doktryny**, w zakresie szerszym niż w pozycji *Analiza* i ewentualne rozwijanie tych poglądów.

Trzecim **celem tej pozycji jest polemika z poglądami doktryny** wtedy, kiedy uważam, że poglądy te są mylne.

Czwartym **celem tej pozycji jest wskazanie błędów w RODO** czy to błędów techniki prawodawczej, czy to miejsc w przepisach, które nie są błędami w rozumieniu dosłownym, jednak mogłyby zostać napisane lepiej, bardziej kompetentnie, czasem po prostu jaśniej. Będące konsekwencją tego celu, propozycje nowelizacyjne stawiam w pozycji ***Postulaty de lege ferenda***.

Warstwa - Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa

Czwartą pozycją (warstwą, podrozdziałem) każdego rozdziału publikacji jest pozycja ***Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa***.

Konceptualizm prawniczy jako ogólna teoria prawa jest teorią nową, zaprezentowany został na Zjeździe Katedr Teorii i Filozofii Prawa, który odbył się w dniach: 6–9.09.2012 r. w Łodzi. Teoria ta wydaje się być wprost idealna jako narzędzie, dzięki któremu można wskazać uprawnienia – wszelkie uprawnienia jakie zapisane są w jakichkolwiek przepisach. Osią konceptualizmu prawniczego, a właściwie tej jego części, która poświęcona jest wykładni prawa, są uprawnienia wynikające z przepisów. Dlatego właśnie użyłem metody opartej na konceptualizmie prawniczym jako metody do wskazania praw, jakie wynikają z RODO. Prawa wynikają z art. 5 RODO oraz z wielu przepisów szczegółowych RODO.

Z uwagi na posługiwanie się konceptualizmem prawniczym jako narzędziem do wskazywania praw, które wynikają z RODO, pozycję, w której wskazuję te prawa w odniesieniu do każdego przepisu,

nazywam ***Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa***. Pozycja ta ma w każdym rozdziale numer „4".

W warstwie tej, w każdym rozdziale, wskazuję jakie prawa wynikają z przepisu analizowanego w tym rozdziale - oczywiście o ile jakieś wynikają – co jest regułą, która jednak znajduje wyjątki.

Konceptualizm prawniczy jako ogólna teoria prawa.
Krótka charakterystyka teorii.

Konceptualizm prawniczy pozwala, odpowiednio do potrzeby, na sprowadzenie uprawnień do obowiązków i na sprowadzenie obowiązków do uprawnień. Wykorzystując tę możliwość, w podrozdziałach Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa, umieszczam informacje nie tylko o tym, jakie uprawnienia-prawa, wynikają z danego przepisu, ale również jakie obowiązki z niego wynikają. **Celem** jest tu zatem wskazanie uprawnień jakie wynikają z przepisów RODO i wskazanie obowiązków jakie wynikają z przepisów RODO.

Uprawnienia, nazywane na gruncie RODO prawami, są niezwykle istotne dla rozumienia i wykładni wielu przepisów RODO. W kilku przepisach RODO znajdują się odwołania do „praw i wolności" czy też do „praw lub wolności". Można się zastanowić, czy prawodawca świadomie stosuje czasem koniunkcję, a czasem alternatywę. Jednak bez względu na ewentualny wynik tego zastanowienia faktem jest, że zarówno „prawa" jak i „wolności" są w RODO wspominane. Dla zastosowania przepisów, w których odsyła się do „praw i wolności" albo do „praw lub wolności" kluczowe jest co najmniej oznaczenie tych praw i wolności. Piszę o tym w uwadze: *3.6. Art. 1. Uwaga 3. Konieczność identyfikacji i zdefiniowania praw i wolności na gruncie RODO.* Dla zastosowania wielu innych przepisów ważne jest by rozumieć, że zapisane są w nich prawa i obowiązki. Rozumienie tego, że przepis to nie tylko zapisana administracyjną metodą regulacji niedogodność dla administratora ale również obowiązek admini-stratora i prawo osoby, której dane dotyczą, pozwala na pełne zrozumienie każdego przepisu, co z kolei pozwala na jego zastosowanie, co z kolei chroni administratora przed odpowiedzialnością.

Wykorzystywanie konceptualizmu prawniczego do prowadzonych rozważań pozwala mi zaprezentować metodę opartą na tej teorii, a także (oraz przede wszystkim) wykazać, że konceptualizm praw-

niczy nie jest teorią pustą, że może być skutecznie wykorzystywany w pracy prawnika. Kolejnym celem jest zatem prezentacja Konceptualizmu Prawniczego i wykazanie jego przydatności.

Warstwa - Konkretyzacja zasad

Piątą pozycją (warstwą, podrozdziałem) każdego rozdziału publikacji jest pozycja *Konkretyzacja zasad*.

W pozycji tej opisuję, jakie zasady z art. 5 ust. 2 RODO realizuje przepis będący podstawą rozważań w danym rozdziale. Ustalenie związku między przepisem a zasadą lub zasadami jest niezwykle istotne z kilku względów.

Po pierwsze zasady z art. 5 ust. 2 RODO podlegają realizacji głównie przez przepisy szczegółowe RODO, zatem aby zrealizować zasadę trzeba zrealizować przepisy szczególne RODO, które zasadę konkretyzują. Właśnie fakt, że przepisy konkretyzują zasadę jest źródłem tytułu omawianej warstwy rozważań.

Po drugie z art. 5 ust. 2 RODO wynika obowiązek wykazania realizacji zasad. Skoro zasady są realizowane przez przepisy szczegółowe RODO, to jedynym narzędziem, środkiem, metodą wykazania realizacji zasad jest wykazanie realizacji przepisów szczegółowych RODO, które konkretyzują odpowiednie zasady. Pisałem o tym już w książce *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*[16]. Podałem tam[17] nawet propozycję dokumentu, który służyć może właśnie do wykazania realizacji przepisów szczególnych, co pozwala na wykazanie realizacji zasad. Dokument ten to *Polityka ochrony*, przy czym jest to polityka ochrony rozumiana jako narzędzie wykazania realizacji zasad nie zaś jako dokument, który dotyczy technicznego bezpieczeństwa przetwarzania danych osobowych.

Polityka ochrony tak rozumiana, to również idealne narzędzie odwrócenia ciężaru dowodu w sytuacji, kiedy administrator danych jest kontrolowany przez PUODO.

W książce o dokumentacji opisałem rzecz następująco: *Jeśli ADO nie jest w stanie wykazać realizacji któregokolwiek przepisu*

[16] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora,* Kraków 2019, s. 326.

[17] J. Rzymowski, *op. cit*. s. 327-349.

szczególnego, to w realiach kontroli musi sobie zdawać sprawę z kilku zagrożeń.

***Zagraża** mu odpowiedzialność administracyjna za brak realizacji przepisu szczególnego, do wykazania realizacji którego wezwał go kontrolujący. Jest tak, ponieważ jeżeli ADO nie może wykazać, że realizuje przepis, to wynika z tego, że go nie realizuje.*

***Zagraża** mu odpowiedzialność administracyjna za brak realizacji którejś z zasad z art. 5 ust. 1 RODO. Jest tak, ponieważ jeżeli ADO nie może wykazać, że realizuje przepis, to wynika z tego, że go nie realizuje, więc tym samym, że nie realizuje którejś z zasad z art. 5 ust. 1 RODO.*

***Zagraża** mu odpowiedzialność administracyjna za brak realizacji zasady wykazania realizacji którejś z zasad z art. 5 ust. 1 RODO, czyli za naruszenia art. 5 ust. 2 RODO w zw. z art. 5 ust. 1 RODO.*

Zagrożeń tych można bardzo łatwo uniknąć. Jeżeli ADO, opisze jak realizuje wszystkie zasady z art. 5 ust. 1 RODO, czyli jeżeli ADO opisze za pomocą których i jak realizowanych przepisów szczególnych realizuje które zasady z art. 5 ust. 1 RODO, to tym samym ADO realizuje obowiązek wykazania, że realizuje zasady. Obowiązek ten wynika z art. 5 ust. 2 RODO w zw. z art. 5 ust. 1 RODO.[18].

Bardzo dobrym narzędziem odwrócenia ciężaru dowodu jest też dokument, który administrator danych tworzy jako wynik audytu przestrzegania RODO. Dokument ten bywa nazywany raportem z audytu. Podkreślam, że piszę tu o audycie przestrzegania RODO, czyli o badaniu przestrzegania wszystkich przepisów RODO, nie zaś o audycie bezpieczeństwa danych. Bezpieczeństwu poświęcone jest w RODO od 2% do 5% tekstu RODO (zależnie od przyjętej metody dokonywania obliczeń), najlepiej zatem zrobiony audyt bezpieczeństwa ochrony danych, przy najprzychylniej liczonych procentach, zapewnia wykazanie najwyżej 5 % obowiązków, które musi zrealizować administrator.

Celem warstwy *Konkretyzacja zasad* jest zatem wskazanie jakie zasady konkretyzuje dany przepis, co z kolei prowadzi do realizacji celu jakim jest odpowiednia, ostrożna i dokładna, realizacja przepisu. Realizacja przepisu jest jedyną drogą do realizacji zasady, którą przepis konkretyzuje.

[18] J. Rzymowski, *op. cit.* s. 330-331.

Warstwa - Postulaty de lege ferenda

Szóstą pozycją (warstwą, podrozdziałem) każdego rozdziału jest pozycja ***Postulaty de lege ferenda***.

Jak sama nazwa wskazuje, **celem tej warstwy jest postawienie postulatów w zakresie prawa przyszłości**. Kolejne, numerowane, postulaty zapisywane w tej pozycji nawiązują zwykle do kolejnych, numerowanych, uwag z pozycji należącej do kategorii: ***Uwagi***. Postulaty nawiązują do niektórych, wybranych uwag, do tych, w których omówione są momenty w RODO, które uważam za błędy. Jeżeli postulat odnosi się do uwagi, to jest ona w nim wskazana przez powołanie jej numeru i tytułu. Następnie w postulacie takim odnoszę się w sposób skrócony, czasem jednozdaniowy, do treści uwagi. Po odniesieniu się do treści uwagi stawiam właściwy postulat nowelizacyjny lub – o ile jest to niezbędne ze względów jasności wywodu i mojego poczucia czy wszystko wyjaśniłem, uzasadniam taką a nie inną treść postulatu nowelizacyjnego. Jeżeli „uwaga" w pozycji *Uwagi* poświęcona jest błędowi w RODO, to omawiam ten błąd jako pewne zjawisko, wskazuję dlaczego uważam dane słowa przepisu za błąd, wskazuję niebezpieczeństwa jakimi fragment przepisu uważany przeze mnie za błąd, może skutkować. W „postulacie" uzasadniam dlaczego uważam, że błędny przepis powinien zostać zmieniony w ten a nie inny sposób.

Dalej w pozycji warstwy: ***Postulaty de lege ferenda*** opisuję zmiany jakich należy dokonać w przepisie, a dalej jeszcze w tej pozycji, podaję ostateczną treść przepisu, po proponowanych zmianach. Dodatkowo, dzięki możliwościom jakie daje mi współczesna technika edycji tekstu, zaznaczam jakie słowa należy do przepisu dodać lub jakie słowa należy z przepisu usunąć.

Warstwa - Rozważania historyczne

Siódmą pozycją (warstwą, podrozdziałem) każdego rozdziału publikacji jest pozycja ***Rozważania historyczne***.

Celem tej warstwy rozważań jest wskazanie, jaki przepis Dyrektywy 95/46/WE regulował daną dziedzinę, oczywiście o ile regulacja ta miała miejsce. Celem tej kategorii podrozdziałów jest też przywołanie wybranych, historycznych poglądów doktryny.

Rozważania historyczne prowadzone w pracy zbudowane są zwykle w oparciu o doktrynę zajmującą się prawem ochrony danych

osobowych w czasie przed pojawieniem się RODO. Historyczna doktryna jest łatwo i powszechnie dostępna, uznałem zatem, że nie ma potrzeby niewolniczego jej przytaczania w modelu, w którym wskazywałbym jak dana instytucja jest uregulowana dziś i jak była uregulowana poprzednio. Dla uniknięcia niepotrzebnego przytaczania historycznych poglądów przyjąłem, że w ***Rozważaniach historycznych*** omawiam jedynie poglądy, które do dziś zachowały szczególną doniosłość i aktualność, jednak sama aktualność nie była tu wystarczająca. Wiele poglądów zachowało aktualność z racji stałości instytucji prawa ochrony danych, przy zmianie na poziomie tekstu prawnego, cytowanie takich poglądów uznałem za bezcelowe. Celem podrozdziałów kategorii ***Rozważania historyczne*** jest zatem prezentacja doniosłych nadal poglądów doktryny.

Świadomie nie omawiam w publikacji wszelkich możliwych asocjacji historycznych, poza miejscami, kiedy zagadnienia te mają istotne znaczenie dla interpretacji obecnie obowiązujących przepisów. Tam gdzie uznałem to za konieczne, umieściłem „warstwę" siódmą, oznaczoną jako: „7. Art. (…) ust. (…) pkt (…). Rozważania historyczne.". Pominąłem zwłaszcza zagadnienia związane z kształtowanie się koncepcji ochrony danych osobowych, zasługują one na dokładne omówienie w osobnej publikacji, zaś nie zasługują na pobieżne relacjonowanie, jakim, z konieczności byłyby w niniejszej publikacji potraktowane, z uwagi na jej tematykę.

Cele pracy

Wyżej omówiłem konstrukcję pracy i to, jakie cele realizuję w której „warstwie" rozważań. Tu wymieniam cele pracy.

Zygmunt Ziembiński pisze o problemie *(...) należytego zorganizowania współpracy przedstawicieli szczegółowych nauk prawnych i ogólnej teorii prawa.*[19] Cytowany autor odwołuje się do poglądów T. Rabskiej. Ze względu na fakt, że niniejsza publikacja ma charakter jednoautorski oszczędzona mi jest konieczność organizowania współpracy przedstawicieli różnych dyscyplin prawniczych. Mimo, że nie mam konieczności organizowania tej współpracy, to na kartach niniejszej publikacji staram się osobno prowadzić rozważania dogmatyczne i osobno rozważania teoretyczne. Staram się zwłaszcza oddzielać czyste omówienie przepisu od rozważań, których dalekie źródło leży, co prawda, w analizie tekstu prawnego, jednak źródło to jest dalekie, zaś rozważania prowadzone są na gruncie: już to poglądów doktryny, już to własnych obserwacji i analiz, które jednak nie mają charakteru czystej analizy tekstu prawnego. Staram się też oddzielać interpretację przepisu takiego jakim jest od tego, jakim chciałbym by przepis był, wystrzegam się bowiem czegoś, co można by nazwać życzeniową wykładnią przepisu. Jednocześnie jednolite autorstwo pracy pozwala mi, tam gdzie to konieczne, łączyć czujność teoretyka prawa z praktycyzmem dogmatyka.

Analiza tekstu RODO

Pierwszym celem pracy jest analiza tekstu RODO. Nie jest to główny cel pracy i mógłby być równie dobrze wymieniony na końcu. Analiza tekstu RODO pozwala mi jednak na realizację pozostałych celów pracy, w oparciu o własne ustalenia, poczynione właśnie na etapie analizy tekstu prawnego. Analiza tekstu prawnego daje substrat prawniczy do prowadzenia dalszych rozważań. Uzyskanie substratu intelektualnego do dalszych rozważań zbieżne jest z jednym z problemów, na jakie w ujęciu J. Wróblewskiego napotyka sąd. Jerzy Wró-

[19] Z. Ziembiński, *Problemy podstawowe prawoznawstwa*, Warszawa 1980, s. 28, *op. cit.* T. Rabska, *Kooperacja interdyscyplinarna w badaniach nad administracją oraz rola prawników w tym zakresie*, w *Problemy metodologiczne nauki prawa administracyjnego*, *Prace Naukowe Uniwersytetu Śląskiego* nr 98, Katowice, 1976. s. 54-62.

blewski pisze[20] o ustalaniu norm obowiązujących co nazywa decyzją walidacyjną i o precyzowaniu znaczenia norm obowiązujących co nazywa decyzją interpretacyjną. Jeśli chodzi o decyzję walidacyjną, to nie wdaję się nigdzie w pracy w rozważania dotyczące tego zjawiska. Jeśli chodzi o decyzję interpretacyjną, to jest ona podejmowana zwłaszcza w warstwie Analiza, oraz nieco w warstwie Uwagi. Dopiero na gruncie wyników tej decyzji podejmuję rozważania w pozostałych warstwach pracy.

Prezentacja rozważań własnych poczynionych na gruncie analizy przepisu

Drugim celem pracy jest prezentacja rozważań własnych, poczynionych na gruncie analizy przepisu. Rozważania te prowadzę głównie w podrozdziałach warstwy ***Uwagi***. Podstawowe efekty tych rozważań są dwa.

Pierwszym efektem rozważań własnych są komentarze do kolejnych przepisów RODO. Nie uważam tego efektu za pierwszoplanowy, uznałem jednak, że skoro przepisy drobiazgowo analizuję, to szkoda by było nie uzyskać komentarza jako wyniku tej analizy. Komentarze umieszczone są w podrozdziałach warstwy *Komentarz*.

Drugim efektem rozważań własnych jest wskazanie błędów w RODO i postawienie postulatów de lege ferenda. Postawienie postulatów de lege ferenda uważam za efekt celu, jakim jest prezentacja rozważań własnych jak również za osobny cel pracy.

Wskazanie błędów w RODO

Trzecim celem pracy jest wskazanie błędów w RODO. Wskazanie błędów Z celem tym związany jest cel kolejny, czyli zaproponowanie postulatów de lege ferenda.

Zaproponowanie postulatów de lege ferenda

Czwartym celem pracy jest zatem zaproponowanie postulatów de lege ferenda. Efekt ten i cel uważam, za istotny. Istotny z dwóch powodów.

[20] J. Wróblewski, *Zagadnienia procesowego modelu stosowania prawa. Studia Prawnicze,* Zeszyt 1 – 2 (87 – 88) 198, s. 3-29.

Pierwszy, można rzec naukowy, **powód** jest taki, że znaczna ilość postulatów nowelizacyjnych wskazuje na fakt, że jakość analizowanego aktu prawnego wysoka nie jest.

Drugi, można rzec praktyczny, **powód** jest taki, że można założyć czy też dopuścić, praktyczne wykorzystanie postulatów przez prawodawcę. Postulaty nowelizacyjne umieszczone są w podrozdziałach warstwy *Postulaty de lege ferenda*.

Wskazanie które zasady z art. 5 RODO są konkretyzowane przez które przepisy szczegółowe RODO

Piątym celem pracy jest wskazanie, które mianowicie zasady z art. 5 RODO są konkretyzowane przez które przepisy szczegółowe RODO. Cel ten może pomóc Czytelnikom pracy w realizacji kolejnych zasad i tym samym pomóc im uchronić się przed odpowiedzialnością za nierealizację tych zasad. Zasady zapisane są w art. 5 RODO. Zdefiniowane są tam w sposób daleki od doskonałego. Niektóre nie są zdefiniowane a jedynie nazwane w przepisie. Szerzej piszę o tym w publikacji, która towarzyszy niniejszej, a to w książce: „***RODO – GDPR. Zasady. Zgodność z prawem przetwarzania danych osobowych***.", dlatego tu zwracam uwagę jedynie na cel umieszczenia warstwy poświęconej konkretyzacji zasad. W niniejszej publikacji, podrozdziały poświęcone konkretyzacji zasad są skromne. Konkretyzacja zasad, w pełni rozpoczyna się od art. 6 RODO, dopiero bowiem o tym przepisie, patrząc po kolei na przepisy RODO, można powiedzieć, że konkretyzuje on zasadę. Rozważania poświęcone zasadom umieszczone są w podrozdziałach warstwy Konkretyzacja zasad.

Prezentacja i analiza poglądów doktryny

Szóstym celem pracy jest prezentacja i analiza współczesnych poglądów doktryny, w zakresie w jakim uważam, że jest to konieczne dla ujęcia możliwie szerokiego spektrum poglądów na kwestie analizowane w pracy.

Prezentacji historycznych poglądów doktryny nie uważam za cel pracy. Prezentuję je minimalistycznie, o tyle o ile mają one istotne

znaczenie dla współczesnych dylematów interpretacyjnych.[21] Można się zastanawiać czy zastąpienie Dyrektywy 95/46/WE przez RODO było potrzebne, czy było tylko niepotrzebnym paroksyzmem legislacji. RODO nie wydaje się w żaden sposób lepiej niż Dyrektywa 95/46/WE dostosowane do zjawisk w zakresie ochrony danych, które są wynikiem postępu technicznego. RODO – wbrew temu co mogłoby się wydawać – nie jest w większości poświęcone ochronie danych osobowych. Ochronie danych osobowych poświęcone jest od 3% do 5% tekstu RODO – zależnie od przyjętej metody dokonywania obliczeń. Reszta RODO to przepisy, które ustanawiają po stronie osób, których dane dotyczą, pewne uprawnienia, zaś po stronie administratorów ustanawiają odpowiadające tym uprawnieniom obowiązki. Uprawnienia te, nie dość że korelują z obowiązkami, to ich realizacja zagwarantowana jest też odpowiedzialnością administracyjną, którą ponieść może administrator, gdyby obowiązków nie zrealizował.[22]

Prezentacja i analiza poglądów doktryny umieszczone są w podrozdziałach warstwy *Uwagi*.

Polemika z poglądami doktryny

Siódmym celem pracy jest polemika z poglądami doktryny. Polemiki jakiejkolwiek, w tym polemiki prowadzonej w niniejszej pracy, nie uważam za cel istotny – w żadnym wypadku nie widzę wartości w samej polemice. Nie unikam jej ale i nie szukam. Polemikę prowadzę jedynie wtedy, kiedy uważam, że jest ona konieczna, ponieważ poglądy doktryny są mylne lub co najmniej dyskusyjne. Polemikę z mylnymi poglądami doktryny uważam za realizację pewnej misji nauki czy też naukowca, którą to misją jest, jak wierzę, poszukiwanie prawdy. Zaniechanie polemiki z poglądami uważanymi przez danego naukowca za mylne, uważam za głęboko niewłaściwe. Należy mieć świadomość, że publikacje takie jak niniejsza bywają czytane. Bywają czytane nie tylko przez osoby, które posiadają własne wyrobione poglądy na sprawy w publikacji poruszane, ale bywają czytane również przez osoby, które

[21] Pojęcie dylematu interpretacyjnego przejąłem od prof. P. Chmielnickiego, któremu z tego miejsca dziękuję.

[22] Podobnie i inspirująco: M. Błachucki, T. Górzyńska, G. Sibiga, *Słowo wstępne* w *Analiza i ocena zmian Kodeksu Postępowania Administracyjnego w latach 2010-2011*, pod. red. M. Błachuckiego, T. Górzyńskiej, G. Sibigi, Warszawa 2012, s. 7.

w publikacjach takich poszukują wiedzy.[23] Wiedzy samej w sobie, ale też wiedzy, która może im zapewnić częściowe przynajmniej bezpieczeństwo prawne. Między innymi właśnie ze względu na dobro takich osób, za niezwykle doniosłe uważam polemiki z błędnymi poglądami doktryny. Polemika z poglądami doktryny prowadzona jest w podrozdziałach warstwy *Uwagi* – aczkolwiek nie jest ich jedyną ani główną treścią.

Ustalenie i wskazanie jakie prawa i wolności wskazane są w RODO jako istniejące

Ósmym celem pracy jest ustalenie i wskazanie jakie prawa i wolności wskazane są w RODO jako istniejące. Nie chcę w tym miejscu wdawać się w rozważania nad tym czy owe prawa i wolności są w RODO ustanowione, czy RODO jedynie je opisuje. Faktem jest, że prawa i wolności zapisane w RODO są trzeba tylko umieć je znaleźć. W tym celu należy odnaleźć klucz, z użyciem którego prawodawca te prawa i wolności w RODO zakodował, po czym je po prostu odkodować. Ustalenia dotyczące praw i wolności, głównie jednak praw, prezentowane są w podrozdziałach warstwy *Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa*. Na marginesie należy tu zauważyć, że Prawa i wolności skonkretyzowane w RODO są częścią mającego europejski rodowód systemu ochrony praw jednostki, który jest częścią systemu ochrony praw człowieka.[24]

Patrząc na omawiany cel jako na **wskazanie praw jakie wynikają z RODO** widzimy, że na cel ten składają się dwa cele, a to:
- wskazanie praw jakie wynikają z art. 5 RODO,
- wskazanie praw, jakie wynikają z przepisów szczegółowych RODO.

Jako narzędzia do wskazania tych praw użyłem własnej teorii obowiązywania i wykładni prawa, którą nazwałem zrazu konceptualizmem prawniczym, którą to nazwę prof. Zdzisław Brodecki uzupeł-

[23] Por. S. Wronkowska, *op. cit.* s. 77.

[24] Por. J. Zajadło w *Ochrona praw jednostki*, pod red. Z. Brodeckiego, s. 27. Prawa i wolności skonkretyzowane w RODO są częścią mającego europejski rodowód systemu ochrony praw jednostki, który jest częścią systemu ochrony praw człowieka.

nił stwierdzając, że jest to ogólna teoria prawa[25], co przyjąłem jako drugi człon nazwy.

Prawa te omawiane są również w kolejnych, powstających równolegle z niniejszą publikacjach, uznałem jednak, że dobrze by pierwsza książka z cyklu zawierała katalog praw. Katalog ten znajduje się w pozycji: *3.5. Art. 1. Uwaga 5. Jakie prawa i wolności można wskazać na gruncie RODO*. W uwadze: *3.5.3. Art. 1. Uwaga 5.3. Prawa i wolności o charakterze zasadniczym*. zamieściłem katalog praw, które zapisano w art. 5 ust. 1 RODO. W uwadze tej zamieściłem też rozumowanie, w którym wyjaśniam dlaczego uważam, że zasady z art. 5 ust. 1 RODO to w istocie prawa osób, których dane dotyczą. Spostrzeżenia, że zasady z art. art. 5 ust. 1 RODO to w istocie obowiązki i jednocześnie prawa, dokonałem wcześniej, jeszcze na etapie pisania książki o dokumentacji, kiedy niniejsza książka znajdowała się na bardzo wczesnym etapie rozwoju. Spostrzeżeniem tym podzieliłem się pierwszy raz w formie książkowej, właśnie w książce: *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*, Kraków 2019. Spostrzeżenie przedstawione w postaci rozumowania zatytułowałem tam: *Jakie konkretnie prawa lub wolności oceniać pod kątem oceny naruszenia*. We wskazanej książce nie zamieściłem katalogu praw, a jedynie rozumowanie. W pozycji niniejszej zamieściłem katalog praw.

W pozycji niniejszej oprócz katalogu praw jakie wynikają z art. 5 RODO, nazwanych przez mnie prawami o charakterze zasadniczym, zamieściłem katalog praw jakie wynikają z przepisów szczegółowych RODO. Katalog ten znajduje się w uwadze: *3.5.7. Art. 1. Uwaga 5.7. Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe*. Prawa te nazwałem prawami szczegółowymi.

Prawa są ściśle związane z obowiązkami, zaś jedne i drugie związane są ściśle z wolnościami. Z tych względów katalog praw, które wynikają z przepisów szczegółowych RODO, rozwinąłem o obowiązki, które wynikają z tych przepisów i o wolności związane ze wskazanymi prawami i obowiązkami. W RODO mowa jest kilkakrotnie o prawach i wolnościach, jednak prawodawca nie zachował konsekwentnego reżimu przy tworzeniu aktu prawnego. Miejscami prawodawca sformułował przepisy w taki sposób, że w sposób

[25] Nie jestem w stanie wskazać źródła, rzecz miała miejsce podczas rozmowy z profesorem Zdzisławem Brodeckim.

oczywisty wynikają z nich obowiązki. Pominięcie praw i wolności wynikających z takich przepisów byłoby błędem interpretacji przepisu i jednocześnie w praktyce groziłoby co najmniej odpowiedzialnością administracyjną. Groziłoby odpowiedzialnością, ponieważ RODO zmusza administratora wielokrotnie do oceniania czy aby jakieś zdarzenie nie skutkowało ryzykiem naruszenia praw lub wolności. Jeżeli administrator nie identyfikuje praw i wolności, to tym bardziej nie może ocenić ryzyka ich naruszenia. Jeżeli zatem prawodawca sformułował przepis tak, że wynika z niego obowiązek, to do obowiązku takiego dopisałem prawo i wolność, które – jak uważam – również z takiego przepisu wynikają.

Podobnie postąpiłem jeżeli w RODO zapisano prawo, które przysługuje osobie, której dane dotyczą. Na drodze interpretacji ustaliłem treść obowiązku i wolności i zapisałem je w katalogu.

Prezentacja autorskiej teorii obowiązywania i wykładni prawa, która nosi nazwę: Konceptualizm Prawniczy jako Ogólna Teoria Prawa

Dziewiątym celem pracy jest prezentacja mojej autorskiej teorii obowiązywania i wykładni prawa, która nosi nazwę konceptualizm prawniczy jako ogólna teoria prawa. W niniejszej pracy prezentuję głównie tę stronę konceptualizmu prawniczego, która poświęcona jest wykładni prawa lub też która pozwala na przekładanie przepisów na język uprawnień, niezależnie od tego czy uprawnienia znajdują się w językowej warstwie tych przepisów. Pozwala mi to, mam nadzieję, dowieść, że przynajmniej w tym zakresie konceptualizm prawniczy nie jest teorią pustą. Cel ten uważam za pierwszy z dwóch dodatkowych celów pracy. Cel ten realizowany jest w podrozdziałach warstwy *Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa*.

Prezentacja etapowej analizy semantycznej

Dziesiątym celem pracy jest prezentacja etapowej analizy semantycznej czyli metody, za pomocą której prowadzone są rozważania w niniejszej publikacji w warstwie *Analiza*. Cel ten uważam za drugi z dwóch dodatkowych celów pracy.

Cel ten realizowany jest przede wszystkim w podrozdziałach warstwy *Analiza*. Zastosowanie etapowej analizy semantycznej poz-

wala na sprawne skomentowanie analizowanych przepisów. Wersja ostateczna komentarzy umieszczona jest w podrozdziałach warstwy *Komentarz*. Za szerszą wersję komentarzy można uznać same rozważania umieszczone w warstwie *Analiza*. Dokładność przyjętej metody analizy przepisów pozwala na łatwą polemikę z poglądami doktryny, zwłaszcza tam gdzie mają one charakter oderwanych od przepisów uogólnień lub nieuzasadnionych interpretacji.

Rozdział pierwszy

Artykuł 1 RODO

Artykuł 1 RODO

Przedmiot i cele[26]

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

1. Art. 1. Komentarz

Przepis ustanawia zakres przedmiotowy RODO.

Przepis ustanawia również cele RODO.

Z przepisu trudno wyinterpretować konkretne obowiązki, spoczywające na konkretnych osobach, jest on raczej wskazówką dla interpretacji dalszych przepisów RODO, mimo tego pewne wnioski z analizy przepisu wypływają.

RODO chroni prawa osób fizycznych, czyli żywych ludzi. RODO chroni prawa i obowiązki osób fizycznych związane z przetwarzaniem danych osobowych – z czynnościami dotyczącymi danych osobowych. RODO reguluje przepływ danych osobowych miedzy krajami UE tak, by miał on charakter swobodny.

RODO chroni prawo osób fizycznych do ochrony dotyczących ich danych osobowych. RODO rozszerza zakres praw podstawowych Unii Europejskiej dotyczących danych osobowych, poza prawa wy-

[26] Tytuł przepisu został nadany przez prawodawcę, uważam więc za celowe skomentowanie nie tylko samej treści przepisu, ale i jego tytułu właśnie, analogicznie czynię w kontekście komentowania dalszych przepisów.

mienione w art. 8 KPP UE[27], czyli RODO ustanawia, że wynikające z RODO uprawnienia osób, których dane dotyczą, mają charakter praw podstawowych UE.

RODO dopuszcza przepływ danych osobowych w UE. Celem prawodawcy nie jest ograniczenie przepływu danych osobowych. Przepływ ma zachodzić, tyle tylko że w sposób uporządkowany, wynikający z przepisów RODO.

2. Art. 1. Analiza

Art. 1 RODO posiada tytuł: ***Przedmiot i cele***. Analiza tytułu art. 1 RODO, w kontekście jego treści prowadzi do wniosku, że w art. 1 ust. 1 RODO uregulowano przedmiot RODO, a w art. 1 ust. 2 oraz 1 ust. 3 RODO uregulowano cele RODO. Z uwagi na fakt, że między wyrazami *Przedmiot* i *cele* znajduje się funktor logiczny *i* wynika, że zarówno przedmiot RODO jak i cele RODO zostały uregulowane w art. 1 RODO.

Ze słów: „(…) **o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych** (...)" wnioskujemy, że RODO chroni prawa właśnie osób fizycznych, czyli żywych ludzi. Do definicji osoby fizycznej odnoszę się dalej, w komentarzu do art. 4 pkt 1 RODO. Wydaje się, że osoby fizyczne o których mowa w przepisie to osoby, których dane dotyczą – należy jednak pamiętać, że osoby fizyczne znajdują się też często po drugiej stronie przetwarzania danych. Osoby fizyczne bywają administratorami danych, osoby fizyczne kierują podmiotami, które są administratorami danych, osoby fizyczne bywają podmiotami przetwarzającymi, wreszcie to właśnie osobom fizycznym (na przykład swoim pracownikom) administratorzy i podmioty przetwarzające, nadają upoważnienia do przetwarzania danych osobowych, czy też w inny sposób uprawniają te osoby do przetwarzania danych osobowych. Z komentowanego przepisu wynika jednak raczej, że RODO chroni prawa osób fizycznych, których dotyczą dane osobowe, wnioskujemy o tym też z art. 1 ust. 2 RODO, ze słów: *(...) ich prawo do ochrony danych osobowych*.

[27] *KPP – Karta Praw Podstawowych Unii Europejskiej*, ogłoszona dn. 12 grudnia 2007 r. przez Parlament Europejski, Radę i Komisję, w Dz.U. U. E. C 303 z 14.12.2007, s. 1. *Dziennik Urzędowy Unii Europejskiej,* Dz. U. U. E. C 202/389 z 7.6.2016 Dalej: KPP UE.

Należy tu zwrócić uwagę na jeden jeszcze niuans. Piszę wyżej, że RODO chroni prawa osób fizycznych, co jest prawdą, co wynika z analizowanego przepisu, należy jednak zwrócić uwagę na fakt, że RODO, do pewnego stopnia, chroni również prawa administratorów. Czasem przetwarzanie danych jest obowiązkiem administratora (np. art. 6 ust. 1 lit c RODO), czasem jednak przetwarzanie danych jest prawem administratora (np. art. 6 ust. 1 lit. f RODO) i takie właśnie prawa administratora RODO również chroni. Nie ma sensu intelektualne stawianie administratora w opozycji do osoby, której dane on przetwarza. Administrator przetwarza dane ponieważ ma taki obowiązek, lub ponieważ leży to w jego interesie. Interes administratora, rozumiany abstrakcyjnie, ogólnie, w oderwaniu od konkretnych stanów faktycznych, nie wydaje się być w niczym mniej ważny niż prawa osób, których dane dotyczą.

Podkreślenia wymaga, że RODO dotyczy danych osób fizycznych, bez względu na kontekst występowania tych danych. Jeżeli jakieś informacje są danymi osobowymi, to RODO ich dotyczy. Należy zwłaszcza zwrócić uwagę na fakt, że RODO chroni miedzy innymi dane osób fizycznych prowadzących działalność gospodarczą, cieszę się bardzo, że pogląd taki znalazłem u P. Litwińskiego, P. Barty i M. Kaweckiego.[28]

Ze słów: „**W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych** (...)" wnioskujemy, że RODO dotyczy ochrony osób fizycznych, czyli w istocie ochrony ich praw i obowiązków, jednak ze słów: *w związku z przetwarzaniem danych osobowych* wnioskujemy, że o ile RODO chroni prawa i obowiązki osób fizycznych, o tyle nie wszystkie prawa i obowiązki, a te jedynie, które związane są z przetwarzaniem danych osobowych. Definicja przetwarzania (danych osobowych) zawarta jest w art. 4 pkt 2 RODO i tam też ją omawiam, tu dość stwierdzić, że przetwarzanie danych osobowych to każda czynność dotycząca danych osobowych i mająca z nimi zwią-

[28] P. Litwiński, P. Barta, M. Kawecki w P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 136.

zek w taki sposób, że czynność niejako dotyka danych. Podsumowując można stwierdzić, że RODO chroni prawa i obowiązki osób fizycznych związane z wszystkimi czynnościami dotyczącymi danych osobowych.

Ze słów: „**W niniejszym rozporządzeniu ustanowione zostają** (...) **przepisy o swobodnym przepływie danych osobowych**." wnioskujemy, że RODO reguluje swobodny przepływ danych osobowych miedzy krajami UE. Przepis ten można uznać za wskazówkę interpretacyjną, zgodnie z którą celem przepisów RODO w zakresie przepływu danych nie jest ograniczanie tego przepływu, a wręcz przeciwnie – uregulowanie przepływu danych osobowych tak, by miał on charakter swobodny, co współbrzmi z art. 1 ust 3 RODO.

Ze słów: „**Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych**" wnioskujemy, że RODO chroni *podstawowe prawa i wolności osób fizycznych*[29] i że RODO zwłaszcza chroni prawo do ochrony danych osobowych. Jeśli chodzi o to jakie konkretnie prawa i wolności osób fizycznych chroni RODO, to najprościej można stwierdzić, że te które z RODO wynikają - stwierdzenie to jednak niewiele wyjaśnia. RODO ustanawia wiele uprawnień po stronie osób, których dane dotyczą – i wiele obowiązków po stronie administratorów (danych) i po stronie podmiotów przetwarzających. Należy przy tym zauważyć, że obowiązki administratorów oraz podmiotów przetwarzających to w istocie jednocześnie uprawnienia podmiotów, których dane dotyczą.

Na prawa (uprawnienia) osób, których dane dotyczą, składają się *w szczególności prawo do ochrony danych osobowych*" czyli opisane w RODO rozmaite prawa i wolności osób fizycznych, których dane dotyczą, i wreszcie obowiązki administratorów i podmiotów przetwarzających. Ponadto z komentowanych słów wynika, że wszelkie prawa i wolności osób fizycznych chronione przez RODO mają charakter praw i wolności o charakterze podstawowym.

[29] Podobnie: M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Cz. I Zagadnienia ogólne oraz proces przetwarzania danych osobowych w jednostkach organizacyjnych pomocy społecznej*, *3. Procedura administracyjna w pomocy społecznej w świetle RODO*, Warszawa 2019, Lex.

Słowa: „**Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych** (...)" stanowią swoistą klauzulę odsyłającą do dokumentu: Karta Praw Podstawowych Unii Europejskiej.

Artykuł 8 tego aktu prawnego stanowi:

Ochrona danych osobowych

1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.

3. Przestrzeganie tych zasad podlega kontroli niezależnego organu

Należy zatem uznać, że art. 1 ust. 2 RODO rozszerza zakres Praw Podstawowych Unii Europejskiej dotyczących danych osobowych poza prawa wymienione w art. 8 KPP UE – czyli RODO ustanawia, że wynikające z RODO uprawnienia osób, których dane dotyczą, mają charakter praw podstawowych UE. W związku z tym dobrze by było, gdyby omawiany przepis wyraziście oddawał ten niuans.

Ze słów: „**Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych**." wnioskujemy, że RODO dopuszcza przepływ danych osobowych w UE, ponieważ go nie ogranicza i nie zakazuje ze względu na ochronę osób fizycznych w związku z przetwarzaniem danych osobowych. Podkreślić należy, że RODO co prawda *nie ogranicza ani nie zakazuje* przepływu danych osobowych w UE, ale nie ogranicza i nie zakazuje jedynie z opisanych w przepisie powodów, czyli dopuszcza ograniczanie a nawet zakaz swobodnego przepływu danych z innych powodów niż ochrona uprawnień osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł 1 ust. 3 RODO jest niezwykle doniosły. Należy z niego wnioskować, że celem prawodawcy nie jest ograniczenie przepływu danych osobowych. Przepływ ma zachodzić, tyle tylko że w sposób uporządkowany, wynikający z przepisów RODO. Podobnie rzecz widzą P. Litwiński, P. Barta i M. Kawecki, którzy zwracają uwagę na

fakt, że jest to jeden z dwóch głównych celów RODO.[30] Ci sami autorzy zwracają też uwagę na to, że jednym z celów RODO jest też cel integracyjny, tak by RODO nie przeszkadzało w przepływie danych osobowych między państwami UE.[31] Trafna jest uwaga M. Sakowskiej-Baryły, że z komentowanego przepisu *wywodzić można nieuchronną konieczność wyważenia i pogodzenia dwóch istotnych (...) wartości, jakimi pozostaje prawo do ochrony danych osobowych i autonomia informacyjna jednostki oraz swobodny przepływ danych osobowych w UE*.[32] Podzielam stanowisko wskazanej autorki, zwracam jednak przy tym uwagę, że o ile wskazała ona na dwie istotne wartości, o tyle wymieniła trzy.

Nad treścią omawianego przepisu zastanawia się H. Hijmans, zwracając uwagę na fakt, że przepis ten odtwarza naczelną zasadę rynku wewnętrznego UE, dodając przy tym, że prawdopodobnie przepis ten jest skierowany do państw członkowskich UE, dla zapobieżenia wprowadzaniu przez te państwa ograniczeń w swobodnym przepływie danych.[33] Ogólnie ze wskazanym poglądem się zgadzam, uważam jednak, że art. 1 ust. 3 RODO ma inną rolę, albo ma również inną rolę, ze wskazaniem na: „również". Uważam, że celem tego przepisu jest przede wszystkim wskazanie, że z RODO nie wynika zakaz transgranicznego przepływu danych osobowych wewnątrz UE. Jestem sobie w stanie wyobrazić sytuację, że gdyby art. 1 ust. 3 RODO nie było, to zakaz takiego transferu danych ktoś próbowałby wyprowadzić czy to z art. 5 ust. 1 lit c RODO, z art. 5 RODO, lub z art. 6 RODO, zwłaszcza z części wprowadzającej. Artykuł 1 ust. 3 przed takimi niemądrymi pomysłami, w znacznej mierze, zabezpiecza.

---

[30] P. Litwiński (red.) P. Barta, M. Kawecki. Rozporządzenie *UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 133.

[31] P. Litwiński, P. Barta, M. Kawecki, *loc. cit.* s. 133. Podobnie: M. Sakowska-Baryła w M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 48.

[32] M. Sakowska-Baryła, *op. cit.* s. 48.

[33] H. Hijmans. w *The EU General Data Protection Regulation (GDPR). A Commentary*, edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 57

Na ciekawe zjawisko zwraca uwagę H. Hijmans autor ten zauważa[34] rzecz pozornie oczywistą, która jednak oczywista się staje dopiero, gdy ktoś ją zauważy – a mianowicie, że w art. 5 RODO zachodzi zjawisko balansu, czy też ważenia dwóch zjawisk, a mianowicie prawa do ochrony danych i prawa do swobodnego przepływu danych. Hielkie Hijmans pisze raczej o zmianie równowagi „a shift of balance" - nie dostrzegam jednak w jego wywodach, co jest istotą owej zmiany. W każdym razie należy pamiętać, że omawiany przepis chroni oba prawa - prawa do ochrony danych i prawa do swobodnego przepływu danych.

3. Art. 1. Uwagi.

3.1. Art. 1. Uwaga 1.

Artykuł 1 RODO jako wskazówka interpretacyjna

Na marginesie warto zauważyć, że art. 1 ust. 3 RODO należy traktować, podobnie jak art. 1 ust 1 RODO, jako wskazówkę interpretacyjną dla osób dokonujących wykładni RODO, tak by dokonywały tej wykładni w taki sposób, by efektem wykładni nie było ograniczenie lub zakaz swobodnego przepływu danych.[35] Należy też zauważyć, że o ile słowa: „(...) nie zakazuje (...)" mają związek z treścią RODO, bo RODO rzeczywiście nie zakazuje swobodnego przepływu danych osobowych, o tyle słowa: „Nie ogranicza się (...)" są raczej niezrealizowanym postulatem prawodawcy, ponieważ RODO w istocie jednak ogranicza swobodny przepływ danych osobowych w UE, na przykład poprzez system przesłanek dopuszczalności przetwarzania. Również z niektórych zasad można wyinterpretować takie ograniczenia, na przykład z zasady minimalizacji, zwłaszcza interpretowanej restrykcyjnie, oraz z zasady zgodności z prawem. Nie piszę, że te ograniczenia są wyraźne – wręcz przeciwnie uważam nawet, że doszukiwać ich się nie należy – co nie zmienia faktu, że doszukanie się ich możliwe jest.

[34] H. Hijmans, *op. cit.* s. 56

[35] Podobnie: D. Lubasz w *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*, red. nacz. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 107.

3.2. Art. 1. Uwaga 2.
Dodatkowe cele RODO

Wspominani wyżej aprobatywnie P. Litwiński, P. Barta i M. Kawecki zwracają uwagę na fakt, że *Oprócz celów RODO wskazanych w komentowaniem przepisie, przy jego wykładni należy uwzględnić także cele wskazywane historycznie w procesie legislacyjnym*. Niestety tego stanowiska nie sposób zaaprobować. Interpretacja aktu prawnego powinna się ograniczać głównie do interpretacji tegoż, choć oczywiście łącznie z innymi przepisami. Branie jednak pod uwagę tego co ktoś kiedyś napisał przy okazji pisania aktu prawnego jest pomysłem niebezpiecznym. Jak daleko sięgać? Do projektu? Do materiałów roboczych? Do…? Do czego wreszcie jeszcze można sięgnąć? Jak napisałem, nie sposób tego aprobować – interpretację przepisu trzeba bardzo pieczołowicie oddzielać od rozważań ogólnych, które może i dotyczą materii regulowanej w interpretowanym przepisie, jednak z interpretacją przepisu mylone być nie powinny.

3.3. Art. 1. Uwaga 3.
Niezrealizowane postulaty z motywu 13 Preambuły RODO

Poprzedzający mnie autorzy komentarzy odnieśli się do motywu 13 Preambuły RODO, zawierającego cały katalog „pobożnych życzeń" prawodawcy. Czuję się tu w obowiązku do podjęcia pewnej polemiki. Otóż zwłaszcza D. Lubasz entuzjastycznie odnosi się[36] (odnosząc się też do motywu 13 Preambuły RODO) do celów RODO. Autor ten, we fragmencie komentarza do art. 1 RODO, streścił RODO, pisząc przy tym o nowym podejściu do prywatności. Brak mi w wypowiedzi cytowanego autora, prawdziwej analizy, z której wynikałoby, że postulaty zawarte w motywie 13 Preambuły RODO, nie zostały zrealizowane. Nie widzę sensu w powtarzaniu metody D. Lubasza i streszczaniu RODO w omówieniu art. 1 RODO, tylko dla wskazania, że założenia wynikające z motywu 13 Preambuły RODO nie zostały zrealizowane.

Dalej, w niniejszej publikacji i w innych moich publikacjach[37], znajduje się wiele moich uwag wskazujących na trudności interpre-

[36] D. Lubasz, *op. cit.* s. 109-111.

[37] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora,* Kraków 2019; również publika-

tacyjne, niespójność wewnętrzną RODO i zwykłe błędy techniki prawodawczej. Pewien ślad dystansu D. Lubasza dostrzegam w słowach: *Cel ten zamierzano osiągnąć (...)*. Znacznie mniej entuzjastyczni są P. Litwiński, P. Barta i M. Kawecki, którzy tylko cytują fragment motywu 13 Preambuły RODO i to co ważne, zwracając wcześniej uwagę na fakt, że: *Ustawodawca unijny zaakcentował potrzebę zapewnienia swobody przepływu danych jako filaru gwarantującego swobodę przepływu towarów, usług i kapitału w UE*.[38]

Ślad dystansu dostrzegam też w stanowisku M. Gumularza, który zauważa,[39] że RODO samo wskazuje konieczność jednolitego stosowania przepisów w całej Unii Europejskiej, ale zauważa też, że należy zwracać uwagę na wykładanie RODO np. przez poszczególne krajowe organy nadzorcze.

3.4. Art. 1. Uwaga 4.
Co z art. 1 RODO nie wynika

Ochrona danych osobowych (różnie ujęta) jest jednym z praw podstawowych. Szeroko piszą o tym wszyscy komentatorzy.[40] Nie sposób się z tym nie zgodzić, z jednym jedynie zastrzeżeniem – fakt ten w żaden sposób nie wynika z art. 1 RODO. Zjawiskiem praw podstawowych w RODO zajmuję się niżej, głównie w uwadze *3.8. Art. 1. Uwaga 8. Obecność w RODO praw podstawowych zapisanych w KPP UE* i w uwadze *3.8. Art. 1. Uwaga 9 Prawa podstawowe zapisane w KPP UE.*

Nieco dystansu zachowują jedynie, w Komentarzu, P. Litwiński, P. Barta i M. Kawecki, którzy tego co w przepisie zapisane nie jest, nie komentują[41].

---

cja, która powstaje równolegle z niniejszą, J. Rzymowski, *RODO – GDPR. Przetwarzanie danych osobowych. Zasady. Zgodność z prawem*, Łódź. 2021.

[38] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 135.

[39] M. Gumularz. *Ochrona danych osobowych w sektorze publicznym*, rozdział I. *INFORMACJE OGÓLNE*. 1.Czym jest RODO. Warszawa 2018. Lex.

[40] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE),* 2016/679, Warszawa 2016. s. 5., P D. Lubasz. *op. cit.* s. 105-106., M. Sakowska-Baryła, *op. cit.* s. 50.

[41] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 133-137.

3.5. Art. 1. Uwaga 5.
Jakie prawa i wolności można wskazać na gruncie RODO

Ochrona danych osobowych (różnie ujęta) jest jednym z praw, które chroni RODO. Trafnie zwraca na to uwagę D. Lubasz.[42] Autor ten wymienia ochronę danych osobowych jako jedno z praw i wolności osób fizycznych. Podobnie twierdzi[43] P. Fajgielski. Uważam za konieczne poczynić tu pewne uzupełnienia. Uzupełnienia te czynię w kolejnych uwagach poniżej.

3.5.1. Art. 1. Uwaga 5.1.
Prawo do ochrony danych osobowych

Dominik Lubasz wymienia ochronę danych osobowych wśród praw i wolności osób fizycznych. Podejście takie nie jest błędne, mówi się bowiem np. o ochronie własności, ochronie posiadania. Innymi słowy przyjęte jest, że mówi się o ochronie przedmiotu prawa. Własność, może nawet ochrona własności, jest przedmiotem prawa własności i analogicznie dane osobowe, może nawet ochrona danych osobowych jest przedmiotem prawa do ochrony danych osobowych. Ochrona danych osobowych nie jest prawem, prawem jest prawo do ochrony danych osobowych.

Paweł Fajgielski rzecz ujmuje we właściwy sobie lapidarny i trafny sposób, pisząc: *„Podstawową materią regulowaną w rozporządzeniu 2016/679, a wskazaną w ust. 1 komentowanego artykułu, jest ochrona osób fizycznych w związku z przetwarzaniem danych osobowych, określana skrótowo mianem ochrony danych osobowych.*[44]. Dalej wskazany autor wskazuje, że *(...) istotą regulacji nie jest ochrona samych danych jako dóbr chronionych, ale ochrona osób fizycznych (każdego człowieka) przed negatywnymi konsekwencjami*

[42] D. Lubasz, *op. cit.* s. 105.

[43] P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 21.

[44] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* w *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, WKP 2018 – Komentarz. Kom. do art. 1.

wynikającymi z niezgodnego z prawem przetwarzania danych.[45] Cieszę się bardzo, że P. Fajgielski zwrócił uwagę na fakt, że istotą RODO nie jest ochrona danych, ale ochrona ludzi, których te dane dotyczą. Narzędziem tej ochrony jest ochrona praw i wolności, które tym ludziom przysługują. Przysługują ludziom, czyli każdemu człowiekowi z osobna. Każdemu przysługują prawa i wolności. I wolności te są chronione.

3.5.2. Art. 1. Uwaga 5.2.
Prawa a wolności

Należy zastanowić się nad zależnością między prawem do ochrony danych osobowych a wolnościami, jakie – przynajmniej deklaratywnie w komentowanym przepisie – chroni RODO. Uważam, że sprawa jest prosta. Z prawa do ochrony danych osobowych wynika wolność od przetwarzania danych osobowych w sposób niezgodny z tym prawem. Można oczywiście rzecz ująć nieco inaczej i stwierdzić, że respektowanie prawa do ochrony danych osobowych gwarantuje poszanowanie wolności od przetwarzania danych osobowych w sposób niezgodny z tym prawem. Różnie są tu, w mojej opinii, jednie w warstwie językowej. Omówić zjawisko można różnie, jednak wygląda ono tak, że są: prawo, obowiązek i wolność. Prawo i obowiązek są ze sobą splecione jak Yin i Yang. Osobie, której dane dotyczą przysługuje prawo czyli uprawnienie, na administratorze spoczywa obowiązek, tak długo jak administrator realizuje swój obowiązek, tak długo szanowana jest odpowiednia wolność związana z danym prawem i z danym obowiązkiem.[46]

3.5.3. Art. 1. Uwaga 5.3.
Prawa i wolności o charakterze zasadniczym

Należy się zastanowić nad tym, jakie jeszcze prawa i wolności chroni RODO.

Artykuł 5 ust. 1 RODO, w części wstępnej stanowi: *Dane osobowe muszą być:*. Dalej następują kolejne punkty przepisu, z których, przy pewnym wysiłku można wyinterpretować zasady. Można zatem uznać, że w art. 5 ust. 1 RODO wskazane są zasady dotyczące prze-

[45] P. Fajgielski, *loc. cit.*

[46] Podobnie J. Rzymowski, *op. cit.* s. 281.

twarzania danych osobowych, co zresztą jest zbieżne z myślą prawodawcy, który zapewne nie bez powodu nadał artykułowi 5 RODO tytuł: *Zasady dotyczące przetwarzania danych osobowych*. Analiza treści art. 5 RODO każe sądzić, że myśl prawodawcy nieco tam grzęźnie, o czym piszę przy okazji omawiania właśnie art. 5 RODO[47], niewątpliwe jest jednak, że art. 5 RODO ustanawia zasady przetwarzania danych osobowych, a przynajmniej je wskazuje i ułomnie bo ułomnie, ale zawsze jakoś, wskazuje ich treść a przez to i znaczenie.

Skoro część wprowadzająca art. 5 ust. 1 RODO wskazuje, że dane *muszą być*, to kolejne, występujące po części wprowadzającej, zasady ustanawiają obowiązki administratora. Skoro administrator ma obowiązki, to obowiązki te korelują z uprawnieniami osób, których dane dotyczą. Uprawnienie to nic innego jak prawo – prawo w znaczeniu: „right".

Zwracam uwagę na fakt, że art. 5 RODO jest przepisem o doniosłym znaczeniu. Znajduje się na początku aktu prawnego i przede wszystkim nosi tytuł: *Zasady dotyczące przetwarzania danych osobowych*. Z powyższych rozważań wynika, że w art. 5 ust. 1 RODO zapisane są uprawnienia czyli prawa. Prawa doniosłe, ponieważ są to prawa o charakterze zasad, ale niewątpliwie prawa. Niżej zestawiam te prawa łącznie z odpowiadającymi im wolnościami: kwestie wolności wyjaśniam jeszcze niżej, w uwadze *3.5.4. Art. 1. Uwaga 5.4. Zasada, prawo, obowiązek, wolność*.

Z uwagi na tytuł przepisu, z którego wymienione niżej prawa wynikają, a to: *Zasady dotyczące przetwarzania danych osobowych*, uważam, że należy wobec nich używać nazwy: „uprawnienia zasadnicze" lub „prawa zasadnicze". Konsekwentnie dla wolności, które wynikają z art. 5 ust. 1 RODO, należy używać nazwy: „wolności zasadnicze". Oczywiście dla obowiązków, które wynikają z art. 5 ust. 1 RODO, należy używać nazwy: „obowiązki zasadnicze".

Niezwykle ciekawą uwagę, którą można odnieść do kwestii uprawnień zasadniczych, obowiązków zasadniczych i wolności zasadniczych, znajdujemy w rozważaniach Z. Brodeckiego. Autor ten pisze, że *Zasady ogólne konkretyzują idee*[48]. Zbigniew Brodecki pisze o zasadach ogólnych prawa wspólnotowego, jednak zjawisko konkre-

[47] J. Rzymowski, *RODO – GDPR. Zasady. Zgodność z prawem przetwarzania danych osobowych*, Łódź. 2021.

[48] Z. Brodecki, w: *Europa Sędziów*. Pod redakcją Z. Brodeckiego. Warszawa 2007, s. 25.

tyzacji idei w zasadach, zaobserwowane przez Z. Brodeckiego, zachodzi również – jak się wydaje – w odniesieniu do zasad z art. 5 RODO.

Prawa, obowiązki i wolności wynikające z art. 5 ust. 1 RODO wymieniam poniżej.

Artykuł 5 ust. 1 lit. a RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób zgodny z prawem,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób zgodny z prawem,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób niezgodny z prawem.

Artykuł 5 ust. 1 lit. a RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób rzetelny,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób rzetelny,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób nierzetelny.

Artykuł 5 ust. 1 lit. a RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób przejrzysty,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób przejrzysty,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób nieprzejrzysty.

Artykuł 5 ust. 1 lit. b RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób ograniczony co do celu,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób ograniczony co do celu,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób nieograniczony co do celu.

Artykuł 5 ust. 1 lit. c RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób nieograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.

Artykuł 5 ust. 1 lit. d RODO.
- **Prawo do** przetwarzania danych osobowych
  w sposób prawidłowy,
  przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych osobowych
  w sposób prawidłowy,
  leżący po stronie administratora.
- **Wolność od** przetwarzania danych osobowych
  w sposób nieprawidłowy.

Artykuł 5 ust. 1 lit. e RODO.
- Prawo do przetwarzania danych osobowych
w sposób ograniczony co do przechowywania,
przysługujące osobie, której dane dotyczą.
- Obowiązek przetwarzania danych osobowych
w sposób ograniczony co do przechowywania,
leżący po stronie administratora.
- Wolność od przetwarzania danych osobowych
w sposób nieintegralny.

Artykuł 5 ust. 1 lit. f RODO.
- Prawo do przetwarzania danych osobowych
w sposób integralny,
przysługujące osobie, której dane dotyczą.
- Obowiązek przetwarzania danych osobowych
w sposób integralny,
leżący po stronie administratora.
- Wolność od przetwarzania danych osobowych
w sposób nieintegralny.

Artykuł 5 ust. 1 lit. f RODO.
- Prawo do przetwarzania danych osobowych
w sposób poufny,
przysługujące osobie, której dane dotyczą.
- Obowiązek przetwarzania danych osobowych
w sposób poufny,
leżący po stronie administratora.
- Wolność od przetwarzania danych osobowych
w sposób niepoufny - jawny.

3.5.4. Art. 1. Uwaga 5.4.
Zasada, prawo, obowiązek, wolność

Należy się zastanowić czy zasady, czyli (w pewnym uproszczeniu) prawa i wolności zawarte w art. 5 ust. 1 RODO to wszystkie prawa i wolności jakie chroni RODO. Uważam, że nie. Są jeszcze inne prawa i wolności, na które wskazuję niżej.

Prawo czyli uprawnienie daje osobie, której ono przysługuje, pewne oczekiwanie – oczekiwanie, że ktoś wykona jakąś czynność lub powstrzyma się od wykonania jakiejś czynności. Właśnie to oczekiwanie nazywamy prawem. (Jest to oczywiście nieco uproszczona definicja prawa czyli uprawnienia, ale tu wystarczająca.)

Jednocześnie z danym prawem koreluje obowiązek, który jest nałożony na osobę zobowiązaną, tu administratora danych. Obowiązek ten powoduje, że administrator musi koniecznie wykonać jakąś czynność lub musi powstrzymać się od wykonania jakiejś czynności.

Jednocześnie z faktu, że na kimś spoczywa obowiązek (tu na administratorze), wynika, że ten stan, w którym podmiot zobowiązany (tu administrator danych) musi koniecznie wykonać jakąś czynność lub musi się powstrzymać od wykonania jakiejś czynność. Chroni osobę, której przysługuje uprawnienie (tu osobę, której dane dotyczą) przed tym, by podmiot zobowiązany (tu administrator) nie zachował się w sposób inny niż oczekiwany. Jest to wolność, wolność od czyjegoś zachowania się w ten czy inny sposób lub wolność od stanu, jaki takie zachowanie mogłoby wywołać. Wyżej, w uwadze *3.5.3. Art. 1. Uwaga 5.3. Prawa i wolności o charakterze zasadniczym*, łącznie z prawami zestawiam te wolności w takim zakresie, w jakim wynikają z obowiązków i uprawnień zapisanych w art. 5 ust. 1 RODO.

Jak widać zachodzi pewne wynikanie[49] czyli:

- wpierw jest **zasada**,
- z zasady wynika **prawo**,
- z prawa wynika **obowiązek**,
- obowiązek **służy ochronie wolności** – dzięki obowiązkowi chroniona jest wolność.

[49] Wynikanie to opisałem wcześniej w J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora,* Kraków 2019, s. 356.

Można jeszcze dodać, że dzięki wolności chronione jest uprawnienie czyli prawo. Oczywiście wynikanie to można przedstawić również nieco inaczej, a mianowicie, że najpierw jest uprawnienie (prawo), z prawa wynika obowiązek, obowiązek i prawo chronią wolność. Różnica nie jest tu jedynie językowa, różnica leży w tym, czy interpretujący uważa, że charakter pierwotny mają obowiązki (powinności), czy uprawnienia. Uważam, że uprawnienia mają charakter pierwotny. Obowiązek bez osoby, której przysługuje uprawnienie z tym obowiązkiem związane, wydaje się nie mieć sensu. Najprościej wytłumaczyć to na przykładzie. Otóż wiemy, że na administratorze spoczywają pewne obowiązki, jeżeli jednak nie ma osób, których dane ten administrator by przetwarzał, bowiem nie przetwarza on żadnych danych osobowych, to trudno mówić o jego obowiązkach. Można się ich oczywiście dopatrzeć na gruncie niektórych przepisów szczegółowych RODO, jeżeli jednak administrator nie przetwarza danych (zaliczam tu również przetwarzanie przez podmiot przetwarzający), to obowiązki wynikające z RODO nabierają poważnie iluzorycznego charakteru. Co więcej widać tu element realny, który wprowadza samo przetwarzanie danych osobowych. Wydaje się, że otwiera się tu ciekawe pole badawcze. Administrator *(...) ustala cele i sposoby przetwarzania danych osobowych (...)*, czyli zacytowana tu część definicji administratora łączy go z danymi osobowymi, ale jeżeli przetwarzanie danych osobowych nie ma miejsca, jeżeli administrator ustala cele i sposoby, lecz przetwarzanie nie dochodzi do skutku, to należy się poważnie zastanowić, czy jest on administratorem.

Zwracam uwagę, że prawa wynikające z zasad z art. 5 ust. 1 RODO to nie wszystkie prawa jakie RODO chroni, niżej wskazuję jakie jeszcze prawa RODO chroni, zaznaczam przy tym, że nie są to wszystkie takie prawa. Z RODO wynikają lub w RODO wskazane są również inne prawa, z tymi prawami związane są kolejne wolności.

3.5.5. Art. 1. Uwaga 5.5.
Rozliczalność

Z art. 5 ust. 2 RODO wynika, że administrator musi być w stanie wykazać przestrzeganie zasad. Jest to zasada rozliczalności. Administrator ma zatem obowiązek wykazać przestrzeganie zasad z art. 5 ust. 1 RODO, z czego wynika obowiązek wykazania przestrzegania przepisów szczególnych RODO. Można to nazwać obowiązkiem

realizacji przepisów RODO w sposób rozliczalny. Z obowiązkiem tym związane jest, leżące po stronie osoby, której dane dotyczą, prawo do oczekiwania, że administrator wykaże przestrzeganie zasad z art. 5 ust. 1 RODO czyli wykaże przestrzeganie przepisów szczególnych RODO, czyli prawo do tego, by przepisy RODO realizowane były w sposób rozliczalny. Wspomniany *obowiązek wykazania przestrzegania przepisów szczególnych RODO* wynika z faktu, że zasad z art. 5 ust. 1 RODO nie da się realizować inaczej, jak tylko przez realizację odpowiednich przepisów szczegółowych RODO.

Przez przepisy szczególne RODO rozumiem tu przepisy od art. 6 RODO, czyli art. 6 RODO, art. 7 RODO itd., przy czym przepisy, które konkretyzują konkretne zasady, kończą się, jak uważam, na art. 49 RODO. Ewentualnie można uznać, że przepisy dotyczące odpowiedzialności administracyjnej i odpowiedzialności cywilnej, czyli art. 83 RODO i art. 82 RODO również należą do przepisów konkretyzujących zasady, acz mam tu daleko idące wątpliwości, trudno bowiem byłoby mi wskazać zasady z art. 5 ust. 1 RODO, które są konkretyzowane przez art. 82 RODO lub przez art. 83 RODO.

Jeżeli zatem zasady są konkretyzowane przez odpowiadające im przepisy szczegółowe RODO i jeżeli aby zrealizować zasadę, należy zrealizować odpowiednie przepisy szczegółowe RODO, to aby wykazać realizację zasady, trzeba wykazać realizację odpowiadających danej zasadzie przepisów szczegółowych RODO.

Dostosowując wypowiedź do konwencji przyjętej wyżej, wskazuję niżej jakie prawo i jaka wolność wynikają z art. 5 ust. 2 RODO.

- **Prawo do** tego by administrator był w stanie wykazać **przestrzeganie przepisów art. 5 ust. 1 RODO,** czyli **prawo do tego by administrator realizował zasadę rozliczalności**, przysługujące osobie, której dane dotyczą.

- **Wolność od** przetwarzania danych osobowych **w warunkach, w których administrator nie jest w stanie wykazać przestrzegania przepisów RODO** czyli **w warunkach, w których administrator nie realizuje zasady rozliczalności**.

3.5.6. Art. 1. Uwaga 5.6.
Odesłanie do KPP UE w RODO

Motyw 4 Preambuły RODO stanowi m.in. *Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.* Cytuję te słowa, nie uważam jednak, że RODO chroni prawa wymienione w cytowanej części motywu. Przepis stanowi, że RODO wskazanych w nim praw nie narusza, nie znaczy to jednak, że je chroni. Można dostrzec związki między prawem do ochrony danych osobowych a prawami wskazanymi w cytacie jednak stwierdzenie, że RODO chroni te prawa, byłoby nadużyciem, którego nie chcę popełniać.

Z drugiej strony trzeba przyznać, że w przepisach RODO, w których znajdują się odwołania do praw i wolności, nie znajdują się odwołania jedynie do praw i wolności wymienionych w RODO. O przepisach tych piszę niżej, w uwadze *3.6. Art. 1. Uwaga 6. Konieczność identyfikacji i zdefiniowania praw i wolności na gruncie RODO.* Można zatem jednak postawić tezę, że RODO chroni również prawa zapisane w KPP UE. Część tych praw wymieniam niżej w uwadze *3.8. Art. 1. Uwaga 9. Prawa podstawowe zapisane w KPP UE*.

Nie uważam, że do tych praw koniecznie należy sięgać przy okazji interpretacji RODO, uważam bowiem, że w RODO zapisano prawa, które ściśle związane są z przetwarzaniem danych osobowych, nie ma zatem powodu, by innych praw poszukiwać w innych aktach prawnych. Uważam, że wynika to z samej treści RODO, do takiego samego wniosku skłaniają mnie zasady wykładni prawa, zwłaszcza: dyrektywa języka potocznego, dyrektywa języka prawnego oraz dyrektywa języka specjalnego, oczywiście stosowane zgodnie z kolejnością stosowania dyrektyw językowych.[50] Nie widzę sensu w wyjaśnianiu spraw oczywistych, ograniczając się jedynie do pewnej konkluzji, która po przeprowadzeniu rozumowania na temat praw,

[50] L. Morawski, *Zasady wykładni prawa.* Toruń 2006, s. 89-102.

jakie należy oceniać na gruncie RODO na podstawie wskazanych dyrektyw interpretacyjnych, brzmieć musi, że skoro prawodawca odsyła w kilku miejscach RODO do praw i wolności i skoro ten sam prawodawca takowe prawa i wolności w RODO umieszcza, to nie ma sensu i nie powinno sięgać się do innych aktów prawnych, w poszukiwaniu innych praw lub wolności. Konkluzję tę można uzupełnić jeszcze jedną konkluzją, że jeżeli nawet sięgnie się w poszukiwaniu innych praw lub wolności do innych niż RODO aktów prawnych (i do innych niż te wskazane w RODO), to o ile można to zrobić, o tyle niedopuszczalne jest pomijanie praw i wolności wskazanych w RODO na rzecz praw i wolności wskazanych gdziekolwiek indziej.

3.5.7. Art. 1. Uwaga 5.7.
Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe

Wiele przepisów RODO ustanawia jakieś prawa. Czy prawa te są racjonalnymi przejawami tego co dobre i sprawiedliwe[51], czy wydumanymi pseudouprawnieniami, których celem jest stworzenie wśród administratorów atmosfery strachu, to temat na osobną dyskusję, od udziału w której się nie uchylam, a nawet którą staram się swoimi publikacjami wywoływać. Kiedy czytam przepis o prawie do ograniczenia przetwarzania lub o prawie do bycia zapomnianym, które u praworządnego administratora jest praktycznie nierealizowalne, ponieważ dawno usunął on już dane, których mieć nie powinien, to mam poczucie, że balon ochrony danych przybrał nie tylko ogromne rozmiary, ale zwłaszcza że jego kształty mają postać wyjątkowo dziwnych hybryd.

Jakkolwiek by nie oceniać jakości legislacji, nie sposób zignorować faktu, że RODO jest oraz że wynikające z niego prawa również są. „Są" w sensie obowiązywania w systemie prawa, „są" w sensie ontologicznym czyli istnieją, tak jak byt w ujęciu Parmenidesa.[52] Rozdział III RODO zatytułowany jest: „Prawa osoby, której dane dotyczą".

[51] Pisząc to wspominam zajęcia z prawa rzymskiego, a to: wykłady profesora Jana Kodrębskiego i ćwiczenia doktora Jakuba Skomiała, w których jako student miałem zaszczyt uczestniczyć i mam poczucie, że prawo zostało zepchnięte na dziwną bocznicę, na której nie rządzą duchy Celsusa i Ulpiana. Wspominam wykłady profesora Zygfryda Rymaszewskiego i myślę, że przegnano niestety duchy Baldusa i Bartolusa.

[52] L. Kołakowski, *O co nas pytają wielcy filozofowie*, *seria I*, Kraków 2008, s. 20.

Z tytułu rozdziału wynika, że zapisane jest w nim nic innego jak właśnie prawa osób, których dane dotyczą. Prawa osób, zatem również obowiązki administratorów, zatem również wolności z nich wynikające. Również przepisy innych rozdziałów, o ile tylko nakładają na administratora obowiązki, o tyle kształtują również uprawnienia i wolności.

Zgodnie z powyższym rozumowaniem, zestawiam poniżej prawa, obowiązki i wolności.

Z uwagi na fakt, że prawa wymienione poniżej wynikają z przepisów szczegółowych RODO uważam, że należy wobec nich używać nazwy: „uprawnienia szczegółowe" lub „prawa szczegółowe". Konsekwentnie dla wolności, które są poniżej wymienione, należy używać nazwy: „wolności szczegółowe.". Równie konsekwentnie dla obowiązków, które są poniżej wymienione należy używać nazwy: „obowiązki szczegółowe.".

Art. 6 ust. 1 RODO

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z prawem.
- **Obowiązek** przetwarzania danych osobowych w sposób zgodny z prawem.
- **Wolność** od przetwarzania danych osobowych w sposób niezgodny z prawem.

Art. 6 RODO w zw. z art. 9 RODO

- **Prawo** do przetwarzania szczególnych kategorii danych osobowych, wymienionych w art., 9 ust. 1 RODO w sposób zgodny z prawem i przy spełnieniu jednego z warunków wymienionych w art. 9 ust. 2 RODO.
- **Obowiązek** przetwarzania szczególnych kategorii danych osobowych, wymienionych w art., 9 ust. 1 RODO w sposób zgodny z prawem i przy spełnieniu jednego z warunków wymienionych w art. 9 ust. 2 RODO.
- **Wolność** od przetwarzania szczególnych kategorii danych osobowych, wymienionych w art., 9 ust. 1 RODO w sposób niezgodny z prawem i bez spełnienia jednego z warunków wymienionych w art. 9 ust. 2 RODO.

Art. 6 RODO w zw. z art. 10 RODO

- **Prawo** do przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO w sposób zgodny z prawem i przy spełnieniu warunków wymienionych w art. 10 RODO.
- **Obowiązek** przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO w sposób zgodny z prawem i przy spełnieniu warunków wymienionych w art. 10 RODO.
- **Wolność** od przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO w sposób niezgodny z prawem i bez spełnienia warunków wymienionych w art. 10 RODO.

Art. 13 ust. 1 RODO i art. 13 ust. 2 RODO

- **Prawo** do bycia poinformowanym o informacjach zawartych w art. 13 ust. 1 RODO i w art. 13 ust. 2 RODO w przypadku zbierania danych od osoby, której dane dotyczą, przysługujące osobie, której dane dotyczą.
- **Obowiązek** poinformowania o informacjach zawartych w art. 13 ust. 1 RODO i w art. 13 ust. 2 RODO w przypadku zbierania danych od osoby, której dane dotyczą, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osoba której dane dotyczą nie jest poinformowana o informacjach zawartych w art. 13 ust. 1 RODO i w art. 13 ust. 2 RODO w przypadku zbierania danych od osoby, której dane dotyczą.

Art. 13 ust. 3 RODO

- **Prawo** do bycia poinformowanym o celu przetwarzania innym niż cel, w którym dane osobowe zostały zebrane, przysługujące osobie, której dane dotyczą.
- **Obowiązek** poinformowania o celu przetwarzania innym niż cel, w którym dane osobowe zostały zebrane, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osoba której dane dotyczą nie jest poinformowana o celu przetwarzania innym niż cel, w którym dane osobowe zostały zebrane.

Art. 14 RODO

- **Prawo** do bycia poinformowanym o informacjach zawartych w art. 14 ust. 1 RODO i w art. 14 ust. 2 RODO w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, przysługujące osobie, której dane dotyczą.
- **Obowiązek** poinformowania o informacjach zawartych w art. 14 ust. 1 RODO i w art. 14 ust. 2 RODO w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osoba której dane dotyczą nie jest poinformowana o informacjach zawartych w art. 14 ust. 1 RODO i w art. 14 ust. 2 RODO w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą.

Art. 15 RODO

- **Prawo** do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe osoby, której dane dotyczą, przysługujące osobie, której dane dotyczą.
- **Obowiązek** poinformowania osoby, której dane dotyczą czy przetwarzane są dane osobowe jej dotyczące, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osoba której dane dotyczą nie jest poinformowana czy przetwarzane są dane osobowe jej dotyczące.

Art. 15 RODO

- **Prawo** dostępu do danych osobowych przysługujące osobie, której dane dotyczą, jeżeli dane te są przetwarzane, przysługujące osobie, której dane dotyczą.
- **Obowiązek** udzielenia osobie, której dane dotyczą, dostępu do danych osobowych jeżeli są one przetwarzane.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osobie której dane dotyczą nie udzielono dostępu do danych osobowych jeżeli są one przetwarzane.

Art. 15 ust. 2 RODO

- **Prawo** do zostania poinformowanym o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej, przysługujące osobie, której dane dotyczą.
- **Obowiązek** poinformowania o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej leżący po stronie administratora, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których osoba, której dane dotyczą, nie jest poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Art. 15 ust. 3 RODO

- **Prawo** do uzyskania kopii danych osobowych podlegających przetwarzaniu, przysługujące osobie, której dane dotyczą.
- **Obowiązek** udostępnienia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu, leżący po stronie administratora.
- **Wolność** od przetwarzania w warunkach, w których osobie – której dane dotyczą – nie udostępniono kopii danych osobowych podlegających przetwarzaniu.

Artykuł 16 RODO

- **Prawo** do sprostowania danych osobowych, które są nieprawidłowe, przysługujące osobie, której dane dotyczą.
- **Obowiązek** sprostowania danych osobowych, które są nieprawidłowe, leżący po stronie administratora.
- **Wolność** od przetwarzania nieprawidłowych danych osobowych przez administratora.

Artykuł 17 RODO

- **Prawo** do usunięcia danych osobowych, jeżeli mają miejsce okoliczności wskazane w art. 17 RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** usunięcia danych osobowych na żądanie osoby, której dane dotyczą, jeżeli mają miejsce okoliczności wskazane w art. 17 RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych, jeżeli mają miejsce okoliczności wskazane w art. 17 RODO.

Artykuł 18 RODO

- **Prawo** do żądania ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** przyjęcia żądania ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie przyjął żądania ograniczenia przetwarzania.

Artykuł 18 RODO

- **Prawo** do ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie ograniczył przetwarzania.

Artykuł 19 RODO

- **Prawo** do oczekiwania, że administrator powiadomi każdego odbiorcę, któremu ujawniono dane osobowe o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16 RODO lub zgodnie z art. 17 ust. 1 RODO lub zgodnie z art. 18 RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** powiadomienia każdego odbiorcy, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania, których administrator dokonał

zgodnie z art. 16 RODO lub zgodnie z art. 17 ust. 1 RODO, lub zgodnie z art. 18 RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie powiadomił każdego odbiorcy, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania, których administrator dokonał zgodnie z art. 16 RODO lub zgodnie z art. 17 ust. 1 RODO, lub zgodnie z art. 18 RODO.

Artykuł 20 RODO
- **Prawo** do przenoszenia danych przysługujące osobie, której dane dotyczą.
- **Obowiązek** przeniesienia danych, leżący po stronie administratora.
- **Wolność** od przetwarzania danych w warunkach, w których dane nie zostały przeniesione.

Artykuł 21 RODO
- **Prawo** do wniesienia sprzeciwu wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania, przysługujące osobie, której dane dotyczą.
- **Obowiązek** przyjęcia sprzeciwu wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie przyjął sprzeciwu wniesionego przez osobę, której dane dotyczą.

Artykuł 21 RODO
- **Prawo** do sprzeciwu wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania, przysługujące osobie, której dane dotyczą.
- **Obowiązek** zaprzestania przetwarzania danych osobowych, jeżeli osoba której dane dotyczą wniosła sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania. Obowiązek ten ulega ograniczeniu, jeżeli administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw

i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie uwzględnił sprzeciwu wniesionego przez osobę, której dane dotyczą, mimo że powinien był go uwzględnić.

Artykuł 22 RODO
- **Prawo** do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływa, przysługujące osobie, której dane dotyczą.
- **Obowiązek** dbałości o to by osoba, której dane dotyczą nie podlegała decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywoływałaby wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływała, leżący po stronie administratora.
- **Wolność** od przetwarzania danych w warunkach, w których osoba, której dane dotyczą podlegałaby decyzji, która opierałaby się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywoływałaby wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływała.

3.5.8. Art. 1. Uwaga 5.8.
Dalsze prawa, wolności i obowiązki o charakterze szczegółowym

Artykuł 24 RODO nie leży już w Rozdziale III RODO. Przepis ten, leży w Rozdziale IV RODO, zatytułowanym: *Administrator i podmiot przetwarzający*, jednak art. 24 RODO oraz przepisy następne, do art. 31 RODO włącznie, leżą w sekcji 1 tego rozdziału, zatytułowanej *Obowiązki ogólne*. Wynika z tego, że przepisy od art. 24 RODO do art. 31 RODO opisują obowiązki odpowiednio administratorów lub podmiotów przetwarzających. Z obowiązkami tymi powiązane są prawa osób, których dane dotyczą jak również odpowiednie wolności.

Dla uproszczenia wywodu, zestawiam poniżej prawa, obowiązki i wolności.

Artykuł 24 RODO

- **Prawo** do tego by przetwarzanie odbywało się zgodnie z RODO dzięki wdrożeniu przez administratora odpowiednich środków technicznych i organizacyjnych, przysługujące osobie, której dane dotyczą.
- **Obowiązek** wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania niezgodnego z RODO, zapewniona przez wdrożenie przez administratora odpowiednich środków technicznych i organizacyjnych.

Artykuł 24 RODO

- **Prawo** do tego, by administrator wykazał, że przetwarzanie odbywa się zgodnie z RODO dzięki wdrożeniu przez niego odpowiednich środków technicznych i organizacyjnych, przysługujące osobie, której dane dotyczą.
- **Obowiązek** wykazania, że administrator dokonał wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO, leżący po stronie administratora.
- **Wolność** od przetwarzania w warunkach, w których administrator nie wykazuje, że przetwarzanie odbywa się zgodnie z RODO dzięki temu, że administrator wdrożył odpowiednie środki techniczne i organizacyjne.

Artykuł 25 RODO

- **Prawo** do przetwarzania danych osobowych przy uwzględnieniu ochrony danych w fazie projektowania, przysługujące osobie, której dane dotyczą.
- **Obowiązek** uwzględnienia ochrony danych w fazie projektowania, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych bez uwzględnienia ochrony danych w fazie projektowania.

Artykuł 25 RODO

- **Prawo** do przetwarzania danych osobowych przy uwzględnieniu ochrony danych w ustawieniach domyślnych, przysługujące osobie, której dane dotyczą.
- **Obowiązek** uwzględnienia ochrony danych w ustawieniach domyślnych, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych bez uwzględnienia ochrony danych w ustawieniach domyślnych.

Artykuł 26 RODO

- **Prawo** do określenia przez współadministratorów zakresów odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** określenia przez współadministratorów zakresów odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, leżący po stronie współadministratorów.
- **Wolność** od przetwarzania danych osobowych przez współadministratorów, którzy nie określili zakresów odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

Artykuł 27 RODO

- **Prawo** do przetwarzania danych osobowych wiążącego się z oferowaniem w Unii towarów lub usług osobom, których dane dotyczą lub z monitorowaniem mającego miejsce w Unii Europejskiej zachowania osób, których dane dotyczą przez przedstawiciela wyznaczonego w Unii Europejskiej przez administratora lub podmiot przetwarzający nie mającego jednostek w Unii Europejskiej, przysługujące osobie, której dane dotyczą.
- **Obowiązek** wyznaczenia przedstawiciela w Unii Europejskiej przez administratora lub podmiot przetwarzający nie mającego jednostek w Unii Europejskiej, jeżeli przetwarzanie wiąże się z oferowaniem w Unii towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem mającego miejsce w Unii Europejskiej zachowania osób, których dane dotyczą, leżący po stronie administratora lub podmiotu przetwarzającego
- **Wolność** od przetwarzania danych wiążącego się z oferowaniem w Unii towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem mającego miejsce w Unii Europejskiej zachowania osób, których dane dotyczą, jeżeli administrator lub podmiot

przetwarzający nie mający jednostek organizacyjnych w Unii nie wyznaczył przedstawiciela w Unii Europejskiej.

Art. 28 RODO.

- **Prawo** do przetwarzania na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, jeżeli przetwarzanie odbywa się przez podmiot przetwarzający w imieniu administratora, przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora jeżeli przetwarzanie odbywa się przez podmiot przetwarzający w imieniu administratora, leżący po stronie administratora i podmiotu przetwarzającego.
- **Wolność** od przetwarzania przez podmiot przetwarzający w imieniu administratora, jeżeli przetwarzanie to nie odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.

Artykuł 29 RODO

- **Prawo** do przetwarzania danych wyłącznie na polecenie administratora przez podmiot przetwarzający oraz każdą osobę działającą z upoważnienia administratora lub podmiotu przetwarzającego i mającą dostęp do danych osobowych, przysługujące osobie, której dane dotyczą.
- **Obowiązek** przetwarzania danych wyłącznie na polecenie administratora przez podmiot przetwarzający oraz każdą osobę działającą z upoważnienia administratora lub podmiotu przetwarzającego i mającą dostęp do danych osobowych, leżący po stronie administratora lub podmiotu przetwarzającego.
- **Wolność** od przetwarzania bez polecenia administratora przez podmiot przetwarzający oraz każdą osobę działającą z upoważnienia administratora lub podmiotu przetwarzającego i mającą dostęp do danych osobowych.

Artykuł 30 ust. 1 RODO w zw. z art. 30 ust. 5 RODO

- **Prawo** do tego by administrator przetwarzający dane prowadził rejestr czynności przetwarzania danych osobowych przez administratora, jeżeli zachodzą warunki z art. 32 ust. 5 RODO, przysługujące osobie, której dane dotyczą.
- **Obowiązek** prowadzenia rejestru czynności przetwarzania danych osobowych przez administratora, jeżeli zachodzą warunki z art. 32 ust. 5 RODO.
- **Wolność** od przetwarzania danych osobowych jeżeli administrator nie prowadzi rejestru czynności przetwarzania danych osobowych przez administratora, mimo że zachodzą warunki z art. 32 ust. 5 RODO.

Artykuł 30 ust. 2 RODO w zw. z art. 30 ust. 5 RODO

- **Prawo** do tego by każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadził rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, jeżeli zachodzą warunki z art. 32 ust. 5 RODO – przysługujące osobie, której dane dotyczą.
- **Obowiązek** prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, jeżeli zachodzą warunki z art. 32 ust. 5 RODO.
- **Wolność** od przetwarzania danych osobowych jeżeli każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego nie prowadzi rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, mimo, że zachodzą warunki z art. 32 ust. 5 RODO.

Artykuł 31 RODO

- **Prawo** oczekiwania, że dane osobowe są przetwarzane przez administratora, który współpracuje z organem nadzorczym - przysługujące osobie, której dane dotyczą.
- **Obowiązek** współpracy z organem nadzorczym – leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych przez administratora, który nie współpracuje z organem nadzorczym.

Artykuł 32 RODO

- **Prawo** do przetwarzania danych osobowych w warunkach, w których wdrożono odpowiednie środki techniczne i organizacyjne dla zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, przysługujące osobie, której dane dotyczą.
- **Obowiązek** wdrożenia odpowiednich środków technicznych i organizacyjnych dla zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których nie wdrożono odpowiednich środków technicznych i organizacyjnych dla zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Artykuł 33 RODO

- **Prawo** do tego by administrator zgłosił organowi nadzorczemu naruszenie ochrony danych osobowych jeżeli nie jest mało prawdopodobne, że naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – przysługujące osobie, której dane dotyczą.
- **Obowiązek** zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych jeżeli nie jest mało prawdopodobne, że naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych spoczywających na administratorze.
- **Wolność** od przetwarzania danych osobowych w warunkach kiedy administrator nie zgłosił organowi nadzorczemu naruszenia ochrony danych osobowych, mimo że jest prawdopodobne, że naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Artykuł 34 RODO

- **Prawo** do bycia poinformowanym o naruszeniu ochrony danych osobowych jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – przysługujące osobie, której dane dotyczą.
- **Obowiązek** zawiadomienia osoby której dane dotyczą o naruszeniu ochrony danych osobowych jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – spoczywający na administratorze.
- **Wolność** od przetwarzania danych osobowych w warunkach kiedy administrator nie poinformował osoby, której dane dotyczą o naruszeniu ochrony danych osobowych mimo, że naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Artykuł 35 RODO

- **Prawo** do tego by dane osobowe przetwarzane były w warunkach, w których administrator zrealizował obowiązek dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – przysługujące osobie, której dane dotyczą.
- **Obowiązek** dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – leżący po stronie administratora.
- **Wolność** od przetwarzania danych w warunkach, w których administrator nie zrealizował obowiązku dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, mimo, że dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Artykuł 36 RODO

- **Prawo** do przetwarzania danych osobowych w warunkach, w których administrator zrealizował obowiązek konsultacji z organem nadzorczym (PUODO) jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskazała, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka – przysługujące osobie, której dane dotyczą.
- **Obowiązek** konsultacji z organem nadzorczym (PUODO) jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskazała, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka - leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w warunkach, w których administrator nie zrealizował obowiązku konsultacji z organem nadzorczym (PUODO) mimo, że ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskazała, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka.

Artykuł 37 RODO

- **Prawo** do oczekiwania, że administrator wyznaczy inspektora ochrony danych, jeżeli zachodzą warunki wskazane w art. 37 ust. 1 RODO – przysługujące osobie, której dane dotyczą.
- **Obowiązek** wyznaczenia ochrony danych w warunkach wskazanych w art. 37 ust. 1 RODO – leżący po stronie administratora.
- **Wolność** od przetwarzania danych osobowych w sytuacji kiedy administrator nie wyznaczył inspektora ochrony danych, mimo że zachodzą warunki wskazane w art. 37 ust. 1 RODO.

Wydaje się, że ślad podobnego podejścia widać u R. Kani.[53] Autor ten napisał artykuł poświęcony zjawisku rozsądku w RODO. Pomijając tematykę artykułu, zwracam uwagę, że autor zawarł w nim podrozdział *Wykonywanie praw podmiotu danych*, którego treść może wskazywać właśnie na ślad podejścia analogicznego do tego, które proponuję wyżej.

[53] R. Kania, *O kosztach i rozsądku w RODO*, ABI Expert, Nr 3 (12) s. 25-27.

Podobnie, śladu spojrzenia analogicznego do mojego dopatruję się w artykule D. Łępickiego[54], nie mogę jednak nie zauważyć, że autor ten pobłądził pisząc: *Administrator ma tutaj także pewne prawa. Nie można spełnić niemożliwych do zrealizowania żądań, bez uzyskania dodatkowych informacji, które są niezbędne do ich spełnienia.*

W takiej sytuacji administrator ma prawo odmówić wypełnienia postulatów zawartych we wniosku, w związku z brakiem możliwości udostępnienia informacji niezbędnych do jego realizacji[55]. Cieszy mnie, że D. Łępicki dostrzega uprawnienia osób, których dane dotyczą i odnosi się do ich realizacji, dlatego zresztą wskazuję jego tekst, zwracam jednak uwagę, że jeżeli administrator nie może spełnić żądań osoby, której dane dotyczą, bo na przykład nie jest pewien czy to naprawdę jest ta osoba, czy może tylko ktoś się za nią podaje, to administrator ma obowiązek tych żądań nie spełnić, a nie jak pisze D. Łępicki – administrator ma prawo tych żądań nie spełnić.

Niektóre ze wskazanych wyżej praw wskazał jako prawa L. Kępa. Zwrócił on uwagę na *prawo do uzyskania informacji czy i jakie (...) dane są przetwarzane*[56].

Autor ten wspomniał również o tym, że *Zbierając dane należy (...) przekazać informację czy podanie ich jest obowiązkowe, czy dobrowolne, przy czym należy poinformować o ewentualnych skutkach odmowy podania danych (...)*[57]. Wskazany autor nie podkreślił, że jest to prawo, jednak cytowane zdanie znajduje się w rozdziale zatytułowanym: *Prawa podmiotu danych*, więc chyba uznał, że jednak wskazana konieczność podania danych ma charakter prawa. Dlaczego nie podał pozostałych praw z art 13 RODO i z art. 14 RODO – nie mam pojęcia.

Dalej L. Kępa prowadzi rozważania[58] o obowiązku informacyjnym w ogólności i o momencie jego realizacji. Dalej jeszcze

[54] D. Łępicki, *Monitoring wizyjny – dobrowolność i obowiązki*, ABIEXPERT nr 4(9) 2018. s. 30-33.

[55] D. Łępicki, *Monitoring wizyjny – dobrowolność i obowiązki*, ABIEXPERT nr 4(9) 2018. s. 30-33.

[56] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2014. s. 326.

[57] L. Kępa, *op. cit.* s. 327.

[58] L. Kępa, *loc. cit.*

L. Kępa wspomina[59] o prawie do bycia zapomnianym, prawie do przenoszenia danych i prawie sprzeciwu. Rozdział *Prawa podmiotu danych*, L. Kępa kończy krótkim wywodem o profilowaniu.[60]

Zwracam uwagę na niedoskonałe stanowisko L. Kępy, jest ono bowiem symptomatyczne. Autor ten nazywa prawem tylko to, co w RODO prawem nazwano oraz to, co ktoś prawem nazwał. W tym kontekście jednak, podkreślenia wymaga, że do katalogu praw należą również prawa, których prawodawca ani nikt inny bezpośrednio prawami nie nazwał. Prawa te współtworzą katalog praw, który zaproponowałem wyżej w niniejszej uwadze 3.5.7. Art. 1. Uwaga 5.7. Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe.

3.5.9. Art. 1. Uwaga 5.9.
Wybrane prawa wynikające z Preambuły RODO

Jak piszę wyżej, wiele przepisów RODO ustanawia jakieś prawa. Dokładna lektura RODO wskazuje, że również poszczególne motywy *Preambuły RODO* ustanawiają pewne prawa. Istnienia *Preambuły RODO* nie sposób zignorować. W znacznej mierze powtarza ona regulacje zawarte w artykułach RODO. Językowa analiza poszczególnych motywów *Preambuły RODO* prowadzi do wniosku, że nie tylko powtarza ona regulacje zawarte w artykułach RODO, ale je zapowiada. Niezależnie od tego jak to widzimy, faktem jest, że w przepisach szczegółowych RODO i w motywach *Preambuły RODO* zapisane są w znacznej mierze te same uprawnienia. Widać to kiedy czyta się artykuły RODO i *Preambułę RODO*, oraz widać to też np. kiedy czyta się komentarz pod redakcją Ch. Kunera, L. A. Bygravea i Ch. Docksey,[61] w którym po tekście prawnym każdego przepisu RODO umieszczone są odpowiadające mu motywy *Preambuły*, określone jako *Relevant Recitals* co – jak się wydaje – najlepiej tłumaczy się na „odpowiadające motywy Preambuły".

Tak jak nie sposób zignorować istnienia RODO, tak nie sposób zignorować faktu, że RODO ma *Preambułę*.

---

[59] L. Kępa, *loc. cit.*

[60] L. Kępa, *op. cit.* s. 328.

[61] *The EU General Data Protection Regulation (GDPR). A Commentary*, edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020.

Kontynuując poczynione powyżej zestawienia, zestawiam poniżej prawa zapisane w *Preambule*. Ograniczam się do części praw, nie chcę bowiem nadmiernie obciążać wywodu monstrualnym wyliczeniem praw, tym bardziej, że znaczna cześć tych praw jest wymieniona w uwadze *3.5. Art. 1. Uwaga 5.* Jakie prawa i wolności można wskazać na gruncie RODO, w podrozdziałach warstwy *Uwagi*, a to: *3.5.3. Art. 1. Uwaga 5.3. Prawa i wolności o charakterze zasadniczym* oraz *3.5.7. Art. 1. Uwaga 5.7. Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe*.

Zestawiam poniżej prawa wskazane w Preambule RODO.

- **Prawo** do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 1 Preambuły RODO.)

- **Prawo** do ochrony danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (art. 8 ust. 1 KPP i art. 16 ust. 1 TFUE w zw. z mot. 1 Preambuły RODO).

Przepisy KPP UE wspomniane są w motywie 1 Preambuły RODO. Przepis ten odsyła do art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej i do art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Motyw 1 *Preambuły RODO* wskazuje, że: *Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej Kartą praw podstawowych) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących*.
Lektura art. 8 ust. 1 *Karty praw podstawowych Unii Europejskie*j wskazuje, że przepis ten brzmi: *Każdy ma prawo do ochrony danych osobowych, które go dotyczą*.
Lektura art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej wskazuje, że przepis ten brzmi: *Każda osoba ma prawo do ochrony danych osobowych jej dotyczących*.

Na pewne kuriozum zakrawa fakt, że już w motywie 1 Preambuły RODO znajduje się coś, co z braku lepszego określenia wypada zwać błędem. Wyżej zestawiam treść przepisów, czynię tak, ponieważ

poczynienie przez prawodawcę błędu na samym początku RODO wydaje się wręcz nieprawdopodobne. Niestety, mimo pewnego zaskoczenia, muszę zwrócić uwagę na fakt, że w motywie 1 Preambuły RODO wspomniano ochronę osób fizycznych w związku z przetwarzaniem danych osobowych i stwierdzono, że ochrona ta jest jednym z praw podstawowych. Nie byłoby w tym nic złego, gdyby w drugim zdaniu motywu 1 Preambuły RODO nie odesłano do art. 8 ust. 1 KPP i do art. 16 ust. 1 TFUE. Co widać z cytatów przepisy te, niemal jednobrzmiąco stanowią o „prawie do ochrony danych osobowych" osoby fizycznej. Zwracam uwagę, że o ile prawo wymienione w art. 8 ust. 1 KPP i prawo wymienione w art. 16 ust. 1 TFUE są tym samym prawem, czyli prawem do ochrony danych osobowych osoby fizycznej, o tyle prawo, o którym mowa w motywie 1 Preambuły RODO to inne prawo, a mianowicie prawo do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Prawa te różnią się nie tylko w warstwie językowej, co byłoby pomijalne, jednak odmienny jest w nich przedmiot ochrony. W art. 8 ust. 1 KPP i w art. 16 ust. 1 TFUE przedmiotem ochrony są dane osobowe, w motywie 1 Preambuły RODO przedmiotem ochrony (jakkolwiek dziwnie to brzmi) są osoby fizyczne. Kiedy analizujemy jakie prawa, w związku z danymi osobowymi są chronione, to nie pozostaje nic innego jak postawić obok siebie dwa prawa, a to: prawo do ochrony danych osobowych, które przysługuje osobie, której dane dotyczą (czyli osobie fizycznej) i prawo do ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych, które przysługuje osobom fizycznym. Publikacja moja ogranicza się do analizy artykułów RODO, Preambuły RODO nie analizuję, odnoszę się do niej jedynie tam, gdzie jest to absolutnie konieczne. Z uwagi na to odniesienie nie pozostaje mi nic innego jak postawienie postulatu de lege ferenda. Stawiam go niżej, w podrozdziale.

- **Prawo** do poszanowania życia prywatnego. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 4 Preambuły RODO w zw. z art. 7 KPP UE.)

- **Prawo** do poszanowania życia rodzinnego. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 7 KPP UE.)

- **Prawo** do poszanowania domu. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 7 KPP UE.)

- **Prawo** do komunikowania się. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 7 KPP UE.)

- **Prawo** do wolności myśli. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 10 KPP UE.)

- **Prawo** do wolności sumienia. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 10 KPP UE.)

- **Prawo** do wolności religii. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 10 KPP UE.)

- **Prawo** do wolności wypowiedzi. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 11 KPP UE.)

- **Prawo** do wolności informacji. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw* 4 *Preambuły RODO* w zw. z art. 11 KPP UE.)

- **Prawo** do wolności prowadzenia działalności gospodarczej. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 4 Preambuły RODO w zw. z art. 16 KPP UE.)

- **Prawo** do skutecznego środka prawnego. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 47 KPP UE.)

- **Prawo** do różnorodności kulturowej. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 22 KPP UE.)

- **Prawo** do różnorodności religijnej. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 22 KPP UE.)

- **Prawo** do różnorodności językowej. (Prawo to przysługuje osobom, których dane dotyczą.) (*Motyw 4 Preambuły RODO* w zw. z art. 22 KPP UE)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje przedsiębiorstwom prywatnym. (Motyw 6 Preambuły RODO.)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje organom publicznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do kontroli nad danymi osobowymi, które przysługuje osobom fizycznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje przedsiębiorstwom prywatnym. (Motyw 6 Preambuły RODO.)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje organom publicznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do kontroli nad danymi osobowymi, które przysługuje osobom fizycznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do ochrony danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 9 Preambuły RODO.)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje przedsiębiorstwom prywatnym. (Motyw 6 Preambuły RODO.)

- **Prawo** do wykorzystywania w swej działalności danych osobowych, które przysługuje organom publicznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do kontroli nad danymi osobowymi, które przysługuje osobom fizycznym. (Motyw 6 Preambuły RODO.)

- **Prawo** do ochrony danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 9 Preambuły RODO.)

- **Prawo** do ochrony danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 9 Preambuły RODO.)

Motyw 10 Preambuły RODO stanowi miedzy innymi, że: *Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych*. Przepis ten można uznać za odesłanie do KPP UE jednak sygnalizuję moje wątpliwości doty czące tego czy prawa i wolności zapisane w KPP UE powinny być oceniane na gruncie RODO, jeżeli nie są również zapisane w RODO.

W motywie 11 Preambuły RODO zapisano m. in., że: *Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu (...)*. Wydaje się, że postulat, wynikający z cytowanego fragmentu przepisu, nie został zrealizowany. Ustalenie jakie uprawnienia są chronione na gruncie RODO, jakie uprawnienia wynikają z RODO, jakich uprawnień RODO dotyka – wymaga głębokiego namysłu i długiej pracy.

- **Prawo** do swobodnego przepływu danych osobowych w UE. (Prawo to przysługuje głównie administratorom, ale po stronie osoby, której dane dotyczą można również dostrzec elementy tego prawa, na przykład w prawie do przenoszenia danych.) (Motyw 9 Preambuły RODO.)

W motywie 15 Preambuły RODO poruszono problem zakresu przedmiotowego RODO. Zwrócono tam uwagę na fakt, że *Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych i do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych*.

- **Prawo** do przetwarzania danych osobowych zgodnie z RODO, w kontekście działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 22 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych osób, których dane dotyczą, znajdujących się w Unii, przez administratora lub podmiot przetwarzający, którzy nie posiadają jednostki organizacyjnej w Unii, zgodnie z RODO jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego czy pociąga to za sobą płatność. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 23 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, zgodnie z RODO gdy wiąże się z monitorowaniem zachowania takich osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 24 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii także w przypadkach, gdy na mocy prawa międzynarodowego publicznego stosuje się prawo państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej państwa członkowskiego zgodnie z RODO. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 25 Preambuły RODO.)

- **Prawo** do stosowania zasad ochrony danych osobowych do danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 26 Preambuły RODO.)

- **Prawo** do stosowania zasad ochrony danych osobowych do danych osobowych spseudonimizowanych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 26 Preambuły RODO.)

- **Prawo** do ochrony danych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 28 Preambuły RODO.)

- **Prawo** do tego by administrator przetwarzający dane osobowe wskazał osoby uprawnione do przetwarzania danych osobowych, które przysługuje osobie, której dane dotyczą. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 29 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych przy przestrzeganiu zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania przez organy publiczne, które przysługuje osobom, których dane dotyczą. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 31 Preambuły RODO.)

- **Prawo** do wyrażenia zgody na przetwarzanie danych osobowych w niektórych obszarach badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych, jeżeli w momencie zbierania danych nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 33 Preambuły RODO.)

- **Prawo** do wyrażenia zgody na przetwarzanie danych tylko w niektórych obszarach badań lub elementach projektów badawczych, o ile umożliwia to zamierzony cel. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 33 Preambuły RODO.)

- **Prawo** do szczególnej ochrony danych osobowych dzieci, które przysługuje osobom, których dane dotyczą, czyli dzieciom, których dane dotyczą. (Motyw 38 Preambuły RODO.)

- **Prawo** do przetwarzania, bez zgody osoby sprawującej władzę rodzicielską lub opiekę, danych osobowych dziecka w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku, które przysługuje osobie, której dane dotyczą, czyli dziecku, którego dane dotyczą. Prawo to przysługuje administratorowi, można też dostrzec tu element prawa przysługującego dziecku, z pominięciem udziału osób sprawujących władze rodzicielską lub opiekę. (Motyw 38 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z prawem. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób rzetelny. (Prawo to przysługuje osobom, których dane dotyczą) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie zbierania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie wykorzystywania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie przeglądania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie przetwarzania w inny sposób niż zbieranie, wykorzystywanie, przeglądanie. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie w zakresie tego w jakim stopniu te dane osobowe są przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie w zakresie tego w jakim stopniu te dane osobowe będą przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób przejrzysty w zakresie w zakresie tego w jakim stopniu te dane osobowe są i będą przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości czyli w taki sposób by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości czyli w szczególności prawo do informowania osób, których dane dotyczą o tożsamości administratora. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości czyli w szczególności prawo do informowania osób, których dane dotyczą o celach przetwarzania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości, która dotyczy innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy. (Innych informacji czyli informacji innych niż prawo do informowania osób, których dane dotyczą o celach przetwarzania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości, która dotyczy prawa osób fizycznych do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do uświadomienia osobom fizycznym ryzyka związanego z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do uświadomienia osobom fizycznym zasad związanych z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do uświadomienia osobom fizycznym zabezpieczeń związanych z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do uświadomienia osobom fizycznym praw związanych z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do uświadomienia osobom fizycznym sposobów wykonywania praw przysługujących osobom fizycznym z przetwarzaniem danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do by konkretne cele przetwarzania danych osobowych były wyraźne w momencie ich zbierania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by konkretne cele przetwarzania danych osobowych były uzasadnione w momencie ich zbierania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by konkretne cele przetwarzania danych osobowych były określone w momencie ich zbierania. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by dane osobowe były adekwatne do celów dla których są one przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by dane osobowe były stosowne do celów dla których są one przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by dane osobowe były ograniczone do tego, co niezbędne do celów dla których są one przetwarzane. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by dane osobowe były przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do zapobieżenia przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne realizowane dzięki temu, że administrator ustala termin usuwania danych osobowych. Prawo to przysługuje osobom, których dane dotyczą. (Motyw 39 Preambuły RODO.)

- **Prawo** do zapobieżenia przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne realizowane dzięki temu, że administrator ustala termin okresowego przeglądu danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do zapobieżenia przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne realizowane dzięki temu, że administrator ustala termin usuwania danych osobowych i termin okresowego przeglądu danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by administrator podjął wszelkie rozsądne działania zapewniające sprostowanie danych osobowych, które są nieprawidłowe. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by administrator podjął wszelkie rozsądne działania zapewniające usunięcie danych osobowych, które są nieprawidłowe. (Prawo to przysługuje osobom, których dane dotyczą) (Motyw 39 Preambuły RODO.)

- **Prawo** do tego by administrator podjął wszelkie rozsądne działania zapewniające sprostowanie i usunięcie danych osobowych, które są nieprawidłowe. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania danych osobowych w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 39 Preambuły RODO.)

- **Prawo** do przetwarzania na podstawie zgody. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 40 Preambuły RODO.)

- **Prawo** do przetwarzania na podstawie innej niż zgoda uzasadnionej podstawy przewidzianej prawem. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 40 Preambuły RODO.)

- **Prawo** do przetwarzania na podstawie innej niż zgoda uzasadnionej podstawy przewidzianej prawem, w tym musi się ono odbywać z poszanowaniem obowiązku prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 40 Preambuły RODO.)

- **Prawo** do tego by administrator był w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania, jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 42 Preambuły RODO.)

- **Prawo** do tego by administrator był w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania, jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą w tym prawo do tego by w pisemnym oświadczeniu składanym w innej sprawie niż wyrażanie zgody, istniały gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 42 Preambuły RODO.)

- **Prawo** do tego by oświadczenie o wyrażeniu zgody miało zrozumiałą i łatwo dostępną formę, było sformułowane jasnym i prostym językiem i nie zawierało nieuczciwych warunków. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 42 Preambuły RODO.)

- **Prawo** do tego by oświadczenie o wyrażeniu zgody było świadome dzięki temu, że osoba – której dane dotyczą – zna przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 42 Preambuły RODO.)

- **Prawo** do dobrowolnego wyrażenia zgody. Prawo to jest realizowane dzięki temu, że osoba – której dane dotyczą – ma rzeczywisty i wolny wybór oraz może odmówić i wycofać zgodę bez niekorzystnych konsekwencji. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 42 Preambuły RODO.)

- **Prawo** do tego by zgoda nie stanowiła ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. (Prawo to przysługuje osobom, których dane dotyczą.) (Motyw 43 Preambuły RODO.)

- **Prawo** do tego by zgoda nie była uważana za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna. (Prawo to przysługuje osobom, których dane dotyczą.)

3.6. Art. 1. Uwaga 6. Konieczność identyfikacji i zdefiniowania praw i wolności na gruncie RODO

Namysł nad tym jakie prawa i wolności chronione są na gruncie RODO jest istotny co najmniej z dwóch względów.

Po pierwsze dobrze jest po prostu wiedzieć jakie prawa i wolności są przedmiotem ochrony.

Po drugie być może bardziej istotne, a na pewno niezwykle istotne z praktycznego punktu widzenia wskazanie praw lub wolności na gruncie RODO jest istotne dla interpretacji kilku przepisów RODO, które właśnie do praw i wolności odsyłają.

Z artykułu 24 RODO wynika, że administrator ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne tak by przetwarzanie odbywało się zgodnie z RODO. Administrator ma wdrożyć te środki, uwzględniając przy tym *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia*. Przepis ten, łącznie z art. 32 RODO, stanowi podstawę do wykonywania tak zwanych ocen ryzyka. O samym wykonywaniu takowych ocen i ich wątpliwej wartości piszę gdzie indziej[62], tu zwracam jedynie uwagę na fakt, że oceniając ryzyko należy ocenić właśnie *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia*. Prawa i wolności wskazuję wyżej, tu podkreślam, że dokonując oceny ryzyka nie wystarczy ocenić ryzyka zaistnienia zagrożeń technicznych.

Moja obserwacja praktyki – nie poparta, przyznam, metodycznymi badaniami, jednak czyniona od co najmniej kilku lat w sposób świadomy – wskazuje, że oceny ryzyka są nader często wykonywane

[62] W książce o bezpieczeństwie i ocenach na gruncie RODO, która powstaje równolegle z niniejszą.

niewłaściwie. Oceniane jest prawdopodobieństwo zaistnienia zagrożeń o charakterze technicznym i/ lub organizacyjnym. Ocenia się prawdopodobieństwo uszkodzenia danych, zniszczenia danych, zalania serwerowni, pożaru w archiwum itd. Katalog zagrożeń technicznych, fizycznych, organizacyjnych, co bywa zapominane, wynika z art. 32 ust. 2 RODO, o czym niżej, należy jednak pamiętać, że ocenienie zagrożeń z art. 32 ust. 2 RODO czy nawet mnóstwa innych, analogicznych, jest niewystarczające i błędne – błędne jeżeli ocena do tego się sprowadza. Oceniać należy *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia*. Ocenianie zagrożeń technicznych i/lub organizacyjnych jest, co najwyżej, etapem, który należy wykonać po to, by móc następnie na podstawie tego etapu, wykonać ocenę ryzyka *naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia*.

Podobną wymowę do art. 24 ust. 1 RODO ma art. 32 ust. 1 RODO. Przepis ten wskazuje przykładowe, możliwe metody zabezpieczenia danych. Z przepisu wynika, że te lub inne metody zabezpieczenia należy zastosować uwzględniwszy *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia*, czyli to samo ryzyko, o którym mowa w art. 24 ust. 1 RODO. Artykuł 32 ust 2 RODO wskazuje jakie ryzyka techniczno-organizacyjne należy uwzględniać, przy ocenie stopnia bezpieczeństwa. Podkreślam jednak, że ocena ryzyk z art. 32 ust. 2 RODO może stanowić jedynie etap we właściwej ocenie a mianowicie ocenie ryzyka *naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia*.

Kolejny przepis, dla zrozumienia, a tym samym zastosowania którego, konieczne jest zrozumienie czym są prawa i wolności osób fizycznych, to art. 33 RODO. Z przepisu tego wynika obowiązek zgłaszania do RODO naruszeń ochrony danych osobowych. Naruszenie ochrony danych osobowych zdefiniowano w art. 4 pkt 12 RODO. Zaistnienie takiego naruszenia jest warunkiem koniecznym dla zgłoszenia go do RODO jednak nie jest warunkiem jedynym ani wystarczającym. Naruszenie ochrony danych osobowych podlega zgłoszeniu organowi nadzorczemu (w Polsce: Prezesowi Urzędu Ochrony Danych Osobowych, w skrócie: PUODO) jeżeli nie jest to *mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych*, co wynika z art. 33 RODO. Żeby zatem

wiedzieć czy dane zdarzenie, o charakterze naruszenia, trzeba zgłosić do PUODO, trzeba wiedzieć czy i w jakim stopniu naruszenie to skutkowało ryzykiem, ale znowu podobnie jak w przypadku art. 24 RODO i art. 32 RODO, nie ryzykiem technicznym (na przykład jednym z ryzyk wskazanych w art. 32 ust. 2 RODO) ale *ryzykiem naruszenia praw lub wolności osób fizycznych*.

Truizmem jest, stwierdzenie, że dla oceny ryzyka naruszenia jakichkolwiek praw, należy te prawa zidentyfikować.

Jeszcze jeden przepis, dla interpretacji i zastosowania którego, konieczne jest zidentyfikowanie praw i wolności, o których w przepisie mowa to art. 34 ust. 1 RODO. Z przepisu tego wynika obowiązek zawiadamiania osób których dane dotyczą o naruszeniu ochrony danych osobowych. Również w tym przepisie, zaistnienie obowiązku, tu obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, uzależniono od ryzyka *naruszenia praw lub wolności osób fizycznych*. By nie zostawiać kwestii niedopowiedzianej, przypominam, że administrator ma obowiązek poinformować osobę, której dane dotyczą o naruszeniu ochrony danych osobowych jeżeli naruszenie to *może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych*.

Truizmem również jest stwierdzenie, że dla oceny i tego ryzyka naruszenia praw, konieczne jest tych praw zidentyfikowanie.

Kolejny przepis, dla zastosowania którego konieczna jest ocena praw i wolności to art. 35 RODO. Z przepisu tego wynika nakaz dokonania *oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych* w sytuacji, w której dany (planowany) rodzaj przetwarzania *może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych*. Jak widać i tu ocena zagrożeń technicznych, jakkolwiek przeprowadzona, może być jedynie etapem prowadzącym do oceny ryzyka *naruszenia praw lub wolności osób fizycznych*.

Z art. 35 RODO ściśle związany jest art. 36 RODO. Przepis ten opisuje jakie czynności podejmuje organ nadzoru (PUODO), kiedy administrator skonsultuje się z nim, ponieważ ocena skutków wskazała, że *przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka*. Z faktu, że art. 36 ust. 1 RODO odsyła do art. 35 RODO wynika, że w art. 36 ust. 1 RODO mowa jest, oczywiście, o ryzyku naruszenia praw i wolności. Organ nadzoru, z którym konsultuje się administrator

danych, ma obowiązek zbadać czy administrator dostatecznie zidentyfikował ryzyko i czy administrator ryzyko to dostatecznie zminimalizował. Artykuł 36 ust. 2 RODO odsyła do art. 36 ust 1 RODO, ten z kolei do art. 35 RODO, nie ma zatem wątpliwości, że ryzyko nad którym zastanawia się PUODO to również ryzyko naruszenia praw i wolności.

Jak widać z rozważań prowadzonych w niniejszej „uwadze", identyfikacja i wskazanie praw i wolności są konieczne dla zastosowania kilku przepisów RODO. Co więcej są to przepisy, których niezastosowanie lub niewłaściwe zrozumienie może po stronie administratora skutkować odpowiedzialnością administracyjną lub cywilną.

Propozycję katalogu praw przedstawił L. Kępa. Mimo historycznego już dziś wymiaru jego rozważań, uważam, że nawet sam fakt ich pojawienia się jest godny odnotowania. Zestawienie praw poczynione przez L. Kępę cytuję poniżej, głównie dlatego, że jak widzę, myśl L. Kępy szła tą samą drogą, którą idzie moja – a mianowicie: że prawa osób, których dane dotyczą, wynikają z poszczególnych przepisów. Leszek Kępa zestawił prawa na gruncie UODO97[63], jednak pomijając pewne różnice w regulacji, dla samej koncepcji praw nie ma znaczenia kiedy ona powstała.

Wraz z przyjęciem ustawy wszyscy obywatele otrzymali potwierdzenie szerokiego katalogu praw:
- dane o osobie „należą" do osoby i może ona decydować o ich losie, w szczególności o tym czy zechce je ujawnić;
- dane o osobie można przetwarzać wyłącznie na podstawie obowiązującego prawa;
- osoba, której dane dotyczą ma prawo sprawować kontrolę nad tym, kto i jakie jej dane dotyczące przetwarza;
- zebrane dane nie są dostępne dla wszystkich;
- można je przetwarzać wyłącznie w ograniczonym czasie i celu.

Prawo osoby do kontroli nad tym, kto przetwarza dane jej dotyczące oraz jaki jest ich zakres, a więc z jej punktu widzenia najważniejsze prawo, wyraża się przez:
- obowiązek informowania jej o tym, kto te dane przetwarza;
- prawo do informacji o tym, jakie jej dane są przetwarzane;

[63] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.* Dz.U. 1997 nr 133 poz. 883. ze zm. t.j. Dz.U. 2016 poz. 922. ze zm. (Dalej: UODO97.)

- możliwość sprostowania danych, ich aktualizacji, bądź usunięcia gdy są niepełne lub nieprawdziwe;
- możliwość sprzeciwienia się przetwarzaniu danych.[64]

3.7. Art. 1. Uwaga 7.
Prywatność w RODO

Błędem jest doszukiwanie się w RODO aktu prawnego, którego jedynym celem jest ochrona prawa do prywatności. O samej prywatności w samym tekście RODO nie ma mowy wcale, wydaje się to niewiarygodne, ale słowo „prywatność" w tekście RODO, traktowanym od art. 1 RODO w górę do art. 99 RODO, nie występuje.

Upór w poszukiwaniach słowa „prywatność" w tekście RODO może owocować sukcesem, jednak sukces ten jest niewielki, słowo to występuje 2 razy w przypisie do motywu 173 Preambuły RODO, jednak lektura przypisu rozczaruje tego, kto szuka prywatności w tekście prawnym RODO, z którego wynikają konkretne obowiązki, i prawa, ponieważ treścią przypisu jest tytuł dyrektywy, w której treści słowo „prywatność" się znajduje.[65] W Preambule RODO, poza wskazanym przypisem, słowo „prywatność" również nie występuje. Życie prywatne i rodzinne to inne zjawisko niż prywatność, nie chcąc wdawać się w poboczne rozważania definicyjne zaznaczam, że prywatność jest, jak się wydaje, czymś szerszym niż życie prywatne i rodzinne. Jakkolwiek by na zjawisko prywatności nie patrzeć – prawodawca na gruncie RODO zjawisko to pominął. Skoro zjawisko (a przynajmniej pojęcie) to zostało pominięte, to błędem byłoby doszukiwanie się w RODO aktu prawnego, który chroni głównie, czy może wręcz jedynie, prawo do prywatności. Podejście takie niezgodne byłoby z RODO w warstwie dogmatycznej, zaś w warstwie teoretycznej godziłoby w koncepcję racjonalnego prawodawcy.

Można spojrzeć też inaczej, a mianowicie: że błędem jest zakładanie, że prawo do prywatności jest jedynym prawem, jakie jest chronione na gruncie RODO.

---

[64] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2014, s. 20-21.

[65] Przypis ten, by nie obciążać wywodu głównego zamieszczam jedynie tutaj: „*Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej – dyrektywa o prywatności i łączności elektronicznej*, *Dz.U*. L 201 z 31.7.2002, s. 37)".

Na związek ochrony danych osobowych z ochroną prywatności zwraca uwagę P. Fajgielski, ten sam autor podkreśla jednak, że *można już mówić o wyodrębnieniu ochrony danych osobowych jako osobnej dziedziny prawa i ukształtowaniu regulacji prawnych, które mają na celu ochronę osób fizycznych przed negatywnymi konsekwencjami bezprawnego przetwarzania danych*.[66] Zgadzam się z P. Fajgielskim z tym, że uważam, iż osobną dziedziną prawa o wyodrębnieniu której można mówić, nie jest ochrona danych osobowych, bo ta jest zjawiskiem, ale prawo ochrony danych osobowych. Co ciekawe, stronę wcześniej[67] P. Fajgielski rozróżnia ochronę danych osobowych i prawo ochrony danych osobowych.

Na gruncie wypowiedzi P. Fajgielskiego można zatem mówić o dwóch prawach, są to:
- prawo do ochrony danych osobowych; oraz
- prawo do prywatności.

Co ciekawe złudzeniu, że RODO głównie chroni prywatność ulegli też np. L. A. Bygrave i L. Tosoni, którzy w komentarzu do definicji danych osobowych napisali, że: The focus of data protection law on personal data reflects its basic aim of safeguarding the privacy and related interests of individual natural/physical persons, particularly within the informational sphere.[68], co tłumaczy się na język polski jako: Skupienie prawa ochrony danych osobowych na danych osobowych odzwierciedla jego podstawowy cel jaki jest ochrona prywatności i związanych z nią interesów osób fizycznych, zwłaszcza w sferze informacyjnej69.

Prawo (right) do ochrony danych osobowych przysługuje każdemu człowiekowi i jest elementem ogólnego prawa (right) do ochrony danych osobowych uregulowanego prawem (law) ochrony danych osobowych.

Cieszy, że różnicę tę zauważył P. Fajgielski, pisząc: *Prawo ochrony danych osobowych (przepisy) warto odróżnić od ogólnego prawa*

[66] P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 20.

[67] P. Fajgielski, *op. cit.* s. 18.

[68] L. A. Bygrave, L. Tosoni *w The EU General Data Protection Regulation (GDPR). A Commentary*, edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020. s. 106.

[69] Tłumaczenie: J. Rzymowski.

do ochrony danych osobowych w znaczeniu podmiotowym, rozumianego jako prawo przysługujące osobie, której dane dotyczą, w związku z przetwarzaniem jej danych, na które składa się szereg uprawnień (...).

Wskazany autor zauważa zatem, że na prawo do ochrony danych osobowych składają się uprawnienia. W znacznej mierze odpowiada to mojej koncepcji wielu uprawnień wynikających z RODO, którą przedstawiłem w *Uwadze 3.5. Art. 1. Uwaga 5. Jakie prawa i wolności można wskazać na gruncie RODO*, a wcześniej w książce o dokumentacji[70], którą administrator ma obowiązek sporządzić, na gruncie RODO.

3.8. Art. 1. Uwaga 8
Obecność w RODO praw podstawowych zapisanych w KPP UE

Motyw 10 Preambuły RODO stanowi miedzy innymi, że: (…) Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. (…). Przepis ten należy uznać za odesłanie do KPP UE. Analiza KPP UE wskazuje, że ten akt prawny zawiera dziesiątki praw. Z praw tych wynikają obowiązki, realizacja praw i obowiązków gwarantuje odpowiadające im wolności. Poniżej zestawiam część praw wynikających z KPP UE. Niżej jeszcze, w uwadze, prowadzę rozważania nad tym jakie prawa, które wynikają z KPP UE chroni również RODO. Na gruncie KPP UE chronione jest wiele praw, trzeba zadać jednak jedno pytanie, a mianowicie czy RODO chroni wszystkie prawa podstawowe z KPP UE, czy tylko niektóre. Możliwe są tu dwa poglądy.

Pogląd pierwszy, a mianowicie, że RODO chroni tylko te prawa z KPP UE, które wymienione są w KPP UE i w RODO.

Pogląd drugi, a mianowicie, że RODO chroni wszystkie prawa, które są chronione na gruncie KPP UE.

Pierwszy pogląd jest bardziej kuszący, po oznaczeniu i nazwaniu praw na gruncie RODO wystarczy odnaleźć niektóre z nich w KPP UE i podsumować, że tylko te prawa z KPP UE są chronione na gruncie RODO. Uważam, że ten pogląd należy odrzucić. Uważam tak, ponieważ pogląd ten grozi nieochronieniem w praktyce, wię-

[70] J. Rzymowski, *RODO – GDPR*, *op. cit.* s. 356.

kszości praw wynikających z KPP UE. Faktem jest, że większość tych praw nie ma związku z ochroną danych, odnoszę się do tego w następnym akapicie.

Pogląd drugi uważam za trafny. RODO chroni prawa podstawowe. Nie do końca wiadomo które. W KPP UE zapisano wiele praw podstawowych. Prawa te wymieniam niżej w Uwadze *3.8. Art. 1. Uwaga 9. Prawa podstawowe zapisane w KPP UE*. Prawa podstawowe, które wynikają z KPP UE to jednocześnie uprawnienia osób fizycznych, czy też, jeśli patrzymy na to nieco inaczej – z praw podstawowych wynikają uprawnienia osób fizycznych. Ja podzielam jeszcze inny, choć analogiczny, pogląd, a mianowicie: że prawa podstawowe zapisane w KPP UE składają się z miliardów uprawnień poszczególnych osób fizycznych. KPP UE jest fizykalnym zapisem tych uprawnień, ale uprawnienia przysługują poszczególnym osobom. Każdej osobie przysługują jej własne uprawnienia, które wymienione w sposób zagregowany są na gruncie KPP UE (patrz: konceptualizm prawniczy jako ogólna teoria prawa).

W każdym razie, z KPP UE, wynika wiele uprawnień. Uprawnienia te przysługują osobom fizycznym niezależnie od tego czy RODO tak stanowi czy nie. Pozostaje pytanie, czy uprawnienia te chronione są na gruncie RODO. Uważam, że najuczciwszy jest pogląd ostrożnościowy. Nie wiadomo czy uprawnienia z KPP UE są chronione na gruncie RODO i skoro tego nie wiadomo, to z ostrożności administrator powinien działać tak jakby uprawnienia z KPP UE były na gruncie RODO chronione. Ostrożność ma tu niejako dwa skrzydła.

Jednym ochrania osobę której dane dotyczą, skoro bowiem nie wiadomo czy administrator powinien jej prawa chronić, chronić po to, aby pominąwszy któreś z praw nie obniżyć poziomu ochrony, to administrator musi chronić wszystkie prawa wynikające z KPP UE.

Drugie skrzydło ostrożności chroni administratora, do pewnego stopnia, przed PUODO i przed ewentualną odpowiedzialnością cywilną. Jestem niestety w stanie wyobrazić sobie sytuację, w której PUODO ściga administratora dlatego, że ten, nie dokonał oceny ryzyka naruszenia któregoś z praw z KPP UE, zwłaszcza w realiach kontroli po naruszeniu ochrony danych osobowych.

Niestety gotowość do wojny jako względna gwarancja pokoju, w tym wypadku: spokoju, administratora, jest podejściem może smutnym ale najlepszym.

Z uwagi na poczynione wyżej uwagi, zamieszczam niżej listę uprawnień wynikających z KPP UE. Dla porządku, umieszczam ją w osobnej uwadze.

Zastanowienie się nad tym czy przy ocenianiu ryzyka naruszenia praw i wolności na gruncie RODO oceniać również prawa wynikające z KPP UE zdaje się prowadzić do wniosku, że przynajmniej niektóre z tych praw należy brać pod uwagę. RODO odsyła do praw podstawowych w *Motywie 10 Preambuły RODO. Jednocześnie art. 52 KPP UE* stanowi m. in., że *Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. (...)*. Nie wydaje się, by takowa ustawa, ustawa z której wynikałoby, że nie należy brać pod uwagę ryzyka naruszenia tych praw, przy ocenianiu ryzyka naruszenia praw i wolności na gruncie RODO, była do odnalezienia. Innymi słowy, prawa i wolności wynikające z KPP UE, należy brać pod uwagę na gruncie ocen naruszenia praw lub wolności dokonywanych na podstawie RODO. Nie można ukrywać, że za ustawę taką, choć RODO ustawą, w sensie dosłownym, nie jest, można uznać RODO. Przyjęcie takiej koncepcji prowadzi, z kolei do wniosku, że przy ocenie ryzyka należy brać pod uwagę jedynie prawa i wolności, o których mowa jest w RODO, i o który piszę wyżej w podrozdziałach warstwy uwagi: *3.5.8. Art. 1. Uwaga 5.8. Wybrane prawa wynikające z Preambuły RODO*, *3.5.3. Art. 1. Uwaga 5.3. Prawa i wolności o charakterze zasadniczym* i *3.5.7. Art. 1. Uwaga 5.7. Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe*.

3.8. Art. 1. Uwaga 9
Prawa podstawowe zapisane w KPP UE

Wymieniam poniżej prawa podstawowe, które udało mi się wypisać z KPP UE. Przy każdym z praw wskazuję w jakim przepisie zostało ono zapisane.

Świadomie nie wskazuję jaki obowiązek i jaka wolność są z danym prawem związane, czy też z niego wynikają. W celu ustalenia jakie obowiązki spoczywają na administratorach, wskutek funkcjonowania wskazanych praw i jakie wolności są chronione dzięki poszanowaniu wskazanych praw, należy zastosować metodę, jaka zastosowana jest wyżej w uwadze *3.5. Art. 1. Uwaga 5. Jakie prawa i wolności można wskazać na gruncie RODO*. W uwadze tej w podroz-

dziale *3.5.3. Art. 1. Uwaga 5.3. Prawa i wolności o charakterze zasadniczym* wskazuję jak kształtują się prawa i wolności na gruncie art. 5 ust. 1 RODO. W tej samej uwadze, w podrozdziale *3.5.7. Art. 1. Uwaga 5.7. Prawa szczegółowe, wolności szczegółowe, obowiązki szczegółowe* wskazuję jak kształtują się prawa, wolności i obowiązki, na gruncie przepisów szczegółowych RODO.

Prawa te zajmują kilka stron niniejszej książki. Administrator może zadać sobie pytanie o to, czy jest sens oceniać ryzyko naruszenia każdego z tych praw, przy każdej okazji, kiedy należy oceniać ryzyko naruszenia praw. Wydaje się, że niektóre z praw mogą, w niektórych sytuacjach, nie znaleźć zastosowania, z uwagi na specyfikę stanu faktycznego. Jeżeli nauczyciel ujawni w sposób niezgodny z prawem, na przykład oceny ze sprawdzianu w szkole podstawowej, czy nawet jeżeli wykładowca lub uczelnia ujawni w sposób nieuprawniony wyniki z egzaminu, to pewnym absurdem wydaje się ocenianie prawdopodobieństwa naruszenia wszystkich wskazanych praw, wydaje się jednak, że administrator powinien być ich świadom i tam gdzie to adekwatne – tam powinien oceniać ryzyko ich naruszenia, zaś w stosunku do tych, których ocenianie byłoby bezsensowne – odnotowywać, że oceny ryzyka naruszenia danego prawa się, w danej sytuacji, nie dokonuje.

- **Prawo** człowieka do godności. (Art. 1 KPP UE)

- **Prawo** człowieka do szanowania i ochrony jego godności. (Art. 1 KPP UE)

- **Prawo** człowieka do życia. (Art. 2 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia skazanym na karę śmierci i do nie bycia poddanym wykonaniu kary śmierci. (Art. 2 ust. 2 KPP UE)

- **Prawo** człowieka do poszanowania jego integralności fizycznej i psychicznej. (Art. 3 ust. 1 KPP UE)

- **Prawo** człowieka do tego by w dziedzinie medycyny i biologii szanowana była jego swobodna i świadoma zgoda jako osoby zainteresowanej, wyrażona zgodnie z procedurami określonymi przez ustawę. (Art. 3 ust. 2 lit. a KPP UE)

- **Prawo** człowieka do tego by w dziedzinie medycyny i biologii szanowany był zakaz praktyk eugenicznych, w szczególności tych, których celem jest selekcja osób. (Art. 3 ust. 2 lit b KPP UE)

- **Prawo** człowieka do tego by w dziedzinie medycyny i biologii szanowany był zakaz wykorzystywania ciała ludzkiego i jego poszczególnych części jako źródła zysku. (Art. 3 ust. 2 lit. c KPP UE)

- **Prawo** człowieka do tego by w dziedzinie medycyny i biologii szanowany był zakaz reprodukcyjnego klonowania istot ludzkich. (Art. 3 ust. 2 lit. d KPP UE)

- **Prawo** człowieka do nie bycia poddanym torturom ani nieludzkiemu lub poniżającemu traktowaniu albo karaniu. (Art. 4 KPP UE)

- **Prawo** człowieka do nie bycia trzymanym w niewoli lub w poddaństwie. (Art. 5 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia zmuszonym do świadczenia pracy przymusowej lub obowiązkowej. (Art. 5 ust. 2 KPP UE)

- **Prawo** człowieka do nie bycia przedmiotem handlu. (Art. 5 ust. 3 KPP UE)

- **Prawo** człowieka do wolności i bezpieczeństwa osobistego. (Art. 6 ust. 3 KPP UE)

- **Prawo** człowieka do poszanowania życia prywatnego i rodzinnego. (Art. 7 KPP UE)

- **Prawo** człowieka do poszanowania domu. (Art. 7 KPP UE)

- **Prawo** człowieka do poszanowania komunikowania się. (Art. 7 KPP UE)

- **Prawo** człowieka do ochrony danych osobowych które go dotyczą. (Art. 8 ust. 1 KPP UE)

- **Prawo** człowieka do przetwarzania danych osobowych w sposób rzetelny. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do przetwarzania danych osobowych w określonych celach. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do przetwarzania danych osobowych za zgodą osoby której dane dotyczą. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do przetwarzania danych osobowych w oparciu o inną niż zgoda uzasadnioną podstawę prawną przewidzianą ustawą. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do dostępu do zebranych danych osobowych które go dotyczą. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do dokonania sprostowania danych osobowych które go dotyczą. (Art. 8 ust. 2 KPP UE)

- **Prawo** człowieka do zawarcia małżeństwa zgodnie z ustawami krajowymi regulującymi korzystanie z tego prawa.
  (Art. 9 ust. 2 KPP UE)

- **Prawo** człowieka do założenia rodziny zgodnie z ustawami krajowymi regulującymi korzystanie z tego prawa. (Art. 9 ust. 2 KPP UE)

- **Prawo** człowieka do wolności myśli. (Art. 10 ust. 1 KPP UE)

- **Prawo** człowieka do wolności myśli, sumienia i religii.
  (Art. 10 ust. 1 KPP UE)

- **Prawo** człowieka do wolności myśli, sumienia i religii obejmujące wolność zmiany religii lub przekonań oraz obejmujące wolność uzewnętrzniania indywidualnie lub wspólnie z innymi, publicznie lub prywatnie, swej religii lub przekonań poprzez uprawianie kultu, nauczanie, praktykowanie i uczestniczenie w obrzędach.
  (Art. 10 ust. 1 KPP UE)

- **Prawo** człowieka do odmowy działania sprzecznego z własnym sumieniem, zgodnie z ustawami krajowymi regulującymi korzystanie z tego prawa. (Art. 10 ust. 2 KPP UE)

- **Prawo** człowieka do wolności wypowiedzi. (Art. 11 ust. 1 KPP UE)

- **Prawo** człowieka do wolności wypowiedzi obejmujące wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. (Art. 11 ust. 1 KPP UE)

- **Prawo** człowieka do wolności i pluralizmu mediów. (Art. 11 ust. 2 KPP UE)

- **Prawo** człowieka do swobodnego, pokojowego zgromadzania się oraz do swobodnego stowarzyszania się na wszystkich poziomach, zwłaszcza w sprawach politycznych, związkowych i obywatelskich. (Art. 12 ust. 1 KPP UE)

- **Prawo** człowieka do tworzenia związków zawodowych i przystępowania do nich dla obrony swoich interesów. (Art. 12 ust. 1 KPP UE)

- **Prawo** człowieka do wyrażania woli politycznej za pośrednictwem partii politycznych. (Art. 12 ust. 2 KPP UE)

- **Prawo** człowieka do uprawiania sztuki w sposób wolny od ograniczeń. (Art. 13 KPP UE)

- **Prawo** człowieka do prowadzenia badań naukowych w sposób wolny od ograniczeń. (Art. 13 KPP UE)

- **Prawo** człowieka do poszanowania wolności akademickiej. (Art. 13 KPP UE)

- **Prawo** człowieka do nauki. (Art. 14 KPP UE)

- **Prawo** człowieka do dostępu do kształcenia zawodowego. (Art. 14 KPP UE)

- **Prawo** człowieka do dostępu do kształcenia ustawicznego. (Art. 14 KPP UE)

- **Prawo** człowieka do podejmowania pracy. (Art. 15 ust. 1 KPP UE)

- **Prawo** człowieka do wykonywania swobodnie wybranego zawodu. (Art. 15 ust. 1 KPP UE)

- **Prawo** człowieka do wykonywania swobodnie zaakceptowanego zawodu. (Art. 15 ust. 1 KPP UE)

- **Prawo** człowieka do swobodnego poszukiwania zatrudnienia w każdym Państwie Członkowskim. (Art. 15 ust. 2 KPP UE)

- **Prawo** człowieka do swobodnego wykonywania pracy w każdym Państwie Członkowskim. (Art. 15 ust. 2 KPP UE)

- **Prawo** człowieka do swobodnego Korzystania z prawa przedsiębiorczości w każdym Państwie Członkowskim. (Art. 15 ust. 2 KPP UE)

- **Prawo** człowieka do swobodnego korzystania z prawa świadczenia usług w każdym Państwie Członkowskim. (Art. 15 ust. 2 KPP UE)

- **Prawo** człowieka będącego obywatelem państwa trzeciego, który posiada zezwolenie na pracę na terytorium Państw Członkowskich do takich samych warunków pracy, z jakich korzystają obywatele Unii. (Art. 15 ust. 3 KPP UE)

- **Prawo** człowieka do wolności prowadzenia działalności gospodarczej zgodnie z prawem Unii oraz ustawodawstwami i praktykami krajowymi. (Art. 16 KPP UE)

- **Prawo** człowieka do władania, używania, rozporządzania i przekazania w drodze spadku mienia nabytego zgodnie z prawem. (Art. 17 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia pozbawionym swojej własności, chyba że w interesie publicznym, w przypadkach i na warunkach przewidzianych w ustawie, za słusznym odszkodowaniem za jej utratę wypłaconym we właściwym terminie. (Art. 17 ust. 1 KPP UE)

- **Prawo** człowieka do tego wykorzystanie mienia podlegało regulacji ustawowej w zakresie, w jakim jest to konieczne ze względu na interes ogólny. (Art. 17 ust. 1 KPP UE)

- **Prawo** człowieka do ochrony własności intelektualnej. (Art. 17 ust. 2 KPP UE)

- **Prawo** człowieka do azylu z poszanowaniem zasad Konwencji genewskiej z 28 lipca 1951 roku i Protokołu z 31 stycznia 1967 roku dotyczących statusu uchodźców oraz zgodnie z Traktatem o Unii Europejskiej i Traktatem o funkcjonowaniu Unii Europejskiej (zwanych dalej „Traktatami"). (Art. 18 KPP UE)

- **Prawo** człowieka do nie bycia wydalonym w ramach wydalenia zbiorowego. (Art. 19 KPP UE)

- **Prawo** człowieka do niebycia usuniętym z terytorium państwa, wydalonym lub wydanym w drodze ekstradycji do państwa, w którym istnieje poważne ryzyko, iż może być poddany karze śmierci, torturom lub innemu nieludzkiemu lub poniżającemu traktowaniu albo karaniu. (Art. 19 KPP UE)

- **Prawo** człowieka do bycia równym wobec prawa. (Art. 20 KPP UE)

- **Prawo** człowieka do niebycia dyskryminowanych ze względu na posiadanie jakichkolwiek cech. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na płeć. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na rasę. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na kolor skóry. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na pochodzenie etniczne lub społeczne. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na cechy genetyczne. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na język. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na religię. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na przekonania. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na poglądy polityczne lub wszelkie inne poglądy. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na przynależność do mniejszości narodowej. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na majątek. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na urodzenie. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na niepełnosprawność. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na wiek. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do nie bycia dyskryminowanym ze względu na orientację seksualną. (Art. 21 ust. 1 KPP UE)

- **Prawo** człowieka do różnorodności kulturowej. (Art. 22 KPP UE)

- **Prawo** człowieka do różnorodności religijnej (Art. 22 KPP UE)

- **Prawo** człowieka do równości kobiet i mężczyzn we wszystkich dziedzinach, w tym w zakresie zatrudnienia, pracy i wynagrodzenia. (Art. 23 KPP UE)

- **Prawo** człowieka do utrzymywania lub przyjmowania środków zapewniających specyficzne korzyści dla osób płci niedostatecznie reprezentowanej. (Art. 23 KPP UE)

- **Prawo** człowieka będącego dzieckiem do takiej ochrony i opieki, jaka jest konieczna dla jego dobra. (Art. 24 ust. 1 KPP UE)

- **Prawo** człowieka będącego dzieckiem do swobodnego wyrażania swoich poglądów. (Art. 24 ust. 1 KPP UE)

- **Prawo** człowieka będącego dzieckiem do tego by jego poglądy były brane pod uwagę w sprawach, które go dotyczą, stosownie do jego wieku I stopnia dojrzałości. (Art. 24 ust. 1 KPP UE)

- **Prawo** człowieka do tego by we wszystkich działaniach dotyczących dzieci, zarówno podejmowanych przez władze publiczne, jak i instytucja prywatne, Uwzględnia no przede wszystkim najlepszy interes dziecka. (Art. 24 ust. 2 KPP UE)

- **Prawo** człowieka będącego dzieckiem do utrzymywania stałego osobistego związku z obojgiem rodziców chyba że jest to sprzeczne z jego interesami. (Art. 24 ust. 3 KPP UE)

- **Prawo** człowieka będącego dzieckiem do utrzymywania bezpośredniego kontaktu z obojgiem rodziców chyba że jest to sprzeczne z jego interesami. (Art. 24 ust. 3 KPP UE)

- **Prawo** człowieka będącego osobą w podeszłym wieku do godnego i niezależnego życia. (Art. 25 KPP UE)

- **Prawo** człowieka będącego osobą w podeszłym wieku do uczestniczenia w życiu społecznym i kulturalnym. (Art. 25 KPP UE)

- **Prawo** człowieka będącego osobą niepełnosprawną do korzystania ze środków mających zapewnić mu samodzielność, integrację społeczną i zawodową oraz udział w życiu społeczności. (Art. 26 KPP UE)

- **Prawo** człowieka będącego pracownikiem do tego by zagwarantowano mu, na właściwych poziomach, informacji i konsultacji we właściwym czasie, w przypadkach i na warunkach przewidzianych w prawie Unii oraz ustawodawstwach i praktykach krajowych. (Art. 27 KPP UE)

- **Prawo** człowieka będącego przedstawicielem pracowników do tego by zagwarantowano mu, na właściwych poziomach, informacji i konsultacji we właściwym czasie, w przypadkach i na warunkach przewidzianych w prawie Unii oraz ustawodawstwach i praktykach krajowych. (Art. 27 KPP UE)

- **Prawo** pracowników lub ich organizacji do negocjowania i zawierania układów zbiorowych pracy na odpowiednich poziomach oraz do podejmowania, w przypadkach konfliktu interesów, działań zbiorowych, w tym strajku, w obronie swoich interesów, zgodnie z prawem Unii oraz ustawodawstwami i praktykami krajowymi. (Art. 28 KPP UE)

- **Prawo** pracodawców lub ich organizacji do negocjowania i zawierania układów zbiorowych pracy na odpowiednich poziomach oraz do podejmowania, w przypadkach konfliktu interesów, działań zbiorowych, w tym strajku, w obronie swoich interesów, zgodnie z prawem Unii oraz ustawodawstwami i praktykami krajowymi. (Art. 28 KPP UE)

- **Prawo** człowieka do dostępu do bezpłatnego pośrednictwa pracy. (Art. 29 KPP UE)

- **Prawo** człowieka będącego pracownikiem do ochrony w przypadku nieuzasadnionego zwolnienia z pracy, zgodnie z prawem Unii oraz ustawodawstwami i praktykami krajowymi. (Art. 30 KPP UE)

- **Prawo** człowieka będącego pracownikiem do warunków pracy szanujących jego zdrowie, bezpieczeństwo i godność. (Art. 31 ust. 1 KPP UE)

- **Prawo** człowieka będącego pracownikiem do ograniczenia maksymalnego wymiaru czasu pracy, do okresów dziennego i tygodniowego odpoczynku oraz do corocznego płatnego urlopu. (Art. 31 ust. 2 KPP UE)

- **Prawo** człowieka będącego dzieckiem do tego by jego praca była zakazana. (Art. 32 KPP UE)

- **Prawo** człowieka do tego by minimalny wiek dopuszczenia do pracy nie był niższy niż minimalny wiek zakończenia obowiązku szkolnego, bez uszczerbku dla uregulowań bardziej korzystnych dla młodocianych i z wyjątkiem ograniczonych odstępstw. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by mieć zapewnione warunki pracy odpowiednie dla jego wieku. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed wyzyskiem ekonomicznym. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego bezpieczeństwu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego zdrowiu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego rozwojowi fizycznemu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego rozwojowi psychicznemu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego rozwojowi moralnemu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby szkodzić jego rozwojowi społecznemu. (Art. 32 KPP UE)

- **Prawo** człowieka będącego młodocianym dopuszczonym do pracy do tego by być chronionym przed jakąkolwiek pracą która mogłaby utrudniać mu edukację. (Art. 32 KPP UE)

- **Prawo** człowieka do tego by jego rodzina korzystała z ochrony prawnej. (Art. 33 ust. 1 KPP UE)

- **Prawo** człowieka do tego by jego rodzina korzystała z ochrony ekonomicznej i społecznej. (Art. 33 ust. 1 KPP UE)

- **Prawo** człowieka do ochrony przed zwolnieniem z pracy w celu pogodzenia życia rodzinnego z zawodowym, z powodów związanych z macierzyństwem. (Art. 33 ust. 2 KPP UE)

- **Prawo** człowieka do płatnego urlopu macierzyńskiego oraz do urlopu wychowawczego po urodzeniu lub przysposobieniu dziecka w celu pogodzenia życia rodzinnego z zawodowym. (Art. 33 ust. 2 KPP UE)

- **Prawo** człowieka do świadczeń z zabezpieczenia społecznego oraz do usług społecznych, zapewniających ochronę w takich przypadkach, jak: macierzyństwo, choroba, wypadki przy pracy, zależność lub podeszły wiek oraz w przypadku utraty zatrudnienia, zgodnie z zasadami ustanowionymi w prawie Unii oraz ustawodawstwach i praktykach krajowych. (Art. 34 ust. 1 KPP UE)

- **Prawo** każdego człowieka mającego miejsce zamieszkania i przemieszczającego się legalnie w obrębie Unii Europejskiej do świadczeń z zabezpieczenia społecznego i przywilejów socjalnych zgodnie z prawem Unii oraz ustawodawstwami i praktykami krajowymi. (Art. 34 ust. 2 KPP UE)

- **Prawo** człowieka do pomocy społecznej i mieszkaniowej dla zapewnienia, zgodnie z zasadami ustanowionymi w prawie Unii oraz ustawodawstwach i praktykach krajowych, godnej egzystencji wszystkim osobom pozbawionym wystarczających środków. Celem tego prawa jest zwalczanie wykluczenia społecznego i ubóstwa.
(Art. 34 ust. 3 KPP UE)

- **Prawo** człowieka do dostępu do profilaktycznej opieki zdrowotnej. (Art. 35 KPP UE)

- **Prawo** człowieka do korzystania z leczenia na warunkach ustanowionych w ustawodawstwach i praktykach krajowych.
(Art. 35 KPP UE)

- **Prawo** człowieka do tego, by przy określaniu i realizowaniu wszystkich polityk i działań Unii zapewniony był wysoki poziom ochrony zdrowia ludzkiego. (Art. 35 KPP UE)

- **Prawo** człowieka do uznania i poszanowania przez UE dostępu do usług świadczonych w ogólnym interesie gospodarczym, przewidzianego w ustawodawstwach i praktykach krajowych, zgodnie z Traktatami, w celu wspierania spójności społecznej i terytorialnej Unii. (Art. 36 KPP UE)

- **Prawo** człowieka do dostępu do usług świadczonych w ogólnym interesie gospodarczym, przewidzianego w ustawodawstwach i praktykach krajowych, zgodnie z Traktatami, w celu wspierania spójności społecznej i terytorialnej Unii. (Art. 36 KPP UE)

- **Prawo** człowieka do tego by wysoki poziom ochrony środowiska i poprawa jego jakości były zintegrowane z politykami Unii i zapewnione zgodnie z zasadą zrównoważonego rozwoju.
(Art. 37 KPP UE)

- **Prawo** człowieka do wysokiego poziomu ochrony środowiska i poprawy jego jakości. (Art. 37 KPP UE)

- **Prawo** człowieka do tego, by w politykach UE zapewniony był wysoki poziom ochrony konsumentów. (Art. 38 KPP UE)

- **Prawo** człowieka wysokiego poziomu ochrony konsumentów. (Art. 38 KPP UE)

- **Prawo** człowieka, który jest obywatelem UE do głosowania i kandydowania w wyborach do Parlamentu Europejskiego w Państwie Członkowskim, w którym ma miejsce zamieszkania, na takich samych warunkach jak obywatele tego państwa. (Art. 39 ust. 1 KPP UE)

- **Prawo** człowieka do tego by członkowie Parlamentu Europejskiego byli wybierani w powszechnych wyborach bezpośrednich, w głosowaniu wolnym i tajnym. (Art. 39 ust. 2 KPP UE)

- **Prawo** człowieka, który jest obywatelem UE do głosowania i kandydowania w wyborach do władz lokalnych w Państwie Członkowskim, w którym ma miejsce zamieszkania, na takich samych warunkach jak obywatele tego państwa. (Art. 40 KPP UE)

- **Prawo** człowieka do bezstronnego i sprawiedliwego rozpatrzenia swojej sprawy w rozsądnym terminie przez instytucje, organy i jednostki organizacyjne Unii. (Art. 41 ust. 1 KPP UE)

- **Prawo** człowieka do bezstronnego i sprawiedliwego rozpatrzenia swojej sprawy w rozsądnym terminie przez instytucje, organy i jednostki organizacyjne Unii, w tym prawo każdego do bycia wysłuchanym, zanim zostaną podjęte indywidualne środki mogące negatywnie wpłynąć na jego sytuację. (Art. 41 ust. 1 KPP UE w zw. z art. 41 ust. 2 KPP UE)

- **Prawo** człowieka do bezstronnego i sprawiedliwego rozpatrzenia swojej sprawy w rozsądnym terminie przez instytucje, organy i jednostki organizacyjne Unii w tym prawo każdego do dostępu do akt jego sprawy, przy poszanowaniu uprawnionych interesów poufności oraz tajemnicy zawodowej i handlowej. (Art. 41 ust. 1 KPP UE w zw. z art. 41 ust. 2 KPP UE)

- **Prawo** człowieka do bezstronnego i sprawiedliwego rozpatrzenia swojej sprawy w rozsądnym terminie przez instytucje, organy i jednostki organizacyjne Unii w tym prawo do tego by administracja uzasadniała swe decyzje.
  (Art. 41 ust. 1 KPP UE w zw. z art. 41 ust. 2 KPP UE)

- **Prawo** człowieka do domagania się od Unii naprawienia, zgodnie z zasadami ogólnymi wspólnymi dla praw Państw Członkowskich, szkody wyrządzonej przez instytucje lub ich pracowników przy wykonywaniu ich funkcji. (Art. 41 ust. 3 KPP UE)

- **Prawo** człowieka do naprawienia, zgodnie z zasadami ogólnymi wspólnymi dla praw Państw Członkowskich, szkody wyrządzonej przez instytucje lub ich pracowników przy wykonywaniu ich funkcji. (Art. 41 ust. 3 KPP UE)

- **Prawo** człowieka do tego by mógł zwrócić się pisemnie do instytucji Unii w jednym z języków Traktatów i by otrzymał odpowiedź w tym samym języku. (Art. 41 ust. 4 KPP UE)

- **Prawo** człowieka będącego obywatelem UE do dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy. (Art. 42 KPP UE)

- **Prawo** człowieka będącego osobą fizyczną, mająca miejsce zamieszkania lub statutową siedzibę w Państwie Członkowskim do dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy. (Art. 42 KPP UE)

- **Prawo** człowieka do tego by każda osoba prawna mająca statutową siedzibę w Państwie Członkowskim miała prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy. (Art. 42 KPP UE)

- **Prawo** człowieka będącego obywatelem UE do zwrócenia się do Europejskiego Rzecznika Praw Obywatelskich w przypadkach niewłaściwego administrowania w działaniach instytucji, organów i jednostek organizacyjnych Unii, z wyłączeniem Trybunału Sprawiedliwości Unii Europejskiej wykonującego swoje funkcje sądowe. (Art. 43 KPP UE)

- **Prawo** człowieka będącego osobą fizyczną, mająca miejsce zamieszkania w Państwie Członkowskim do zwrócenia się do Europejskiego Rzecznika Praw Obywatelskich w przypadkach niewłaściwego administrowania w działaniach instytucji, organów i jednostek organizacyjnych Unii, z wyłączeniem Trybunału Sprawiedliwości Unii Europejskiej wykonującego swoje funkcje sądowe. (Art. 43 KPP UE)

- **Prawo** człowieka do tego by każda osoba prawna mająca statutową siedzibę w Państwie Członkowskim mogła zwrócić się do Europejskiego Rzecznika Praw Obywatelskich w przypadkach niewłaściwego administrowania w działaniach instytucji, organów i jednostek organizacyjnych Unii, z wyłączeniem Trybunału Sprawiedliwości Unii Europejskiej wykonującego swoje funkcje sądowe. (Art. 43 KPP UE)

- **Prawo** człowieka będącego obywatelem UE do petycji do Parlamentu Europejskiego. (Art. 44 KPP UE)

- **Prawo** człowieka będącego osobą fizyczną, mająca miejsce zamieszkania lub statutową siedzibę w Państwie Członkowskim do petycji do Parlamentu Europejskiego. (Art. 44 KPP UE)

- **Prawo** człowieka do tego by każda osoba prawna mająca statutową siedzibę w Państwie Członkowskim miała prawo do petycji do Parlamentu Europejskiego. (Art. 44 KPP UE)

- **Prawo** człowieka, będącego obywatelem UE do swobodnego przemieszczania się i przebywania na terytorium Państw Członkowskich. (Art. 45 ust. 1 KPP UE)

- **Prawo** do tego by swoboda przemieszczania się i pobytu została przyznana, zgodnie z Traktatami, obywatelom państw trzecich przebywającym legalnie na terytorium Państwa Członkowskiego. (Art. 45 ust. 2 KPP UE)

- **Prawo** człowieka, będącego obywatelem UE do korzystania na terytorium państwa trzeciego, w którym Państwo Członkowskie, którego jest obywatelem, nie ma swojego przedstawicielstwa, z ochrony dyplomatycznej i konsularnej każdego z pozostałych Państw Członkowskich na takich samych warunkach jak obywatele tego państwa. (Art. 46 KPP UE)

- **Prawo** człowieka, którego prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w art. 47 KPP UE. (Art. 47 KPP UE)

- **Prawo** człowieka do sprawiedliwego i jawnego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy. (Art. 47 KPP UE)

- **Prawo** człowieka do uzyskania porady prawnej. (Art. 47 KPP UE)

- **Prawo** człowieka do skorzystania z pomocy obrońcy i przedstawiciela. (Art. 47 KPP UE)

- **Prawo** człowieka będącego oskarżonym do tego by był uważany za niewinnego, dopóki jego wina nie zostanie stwierdzona zgodnie z prawem. (Art. 48 KPP ust. 1 UE)

- **Prawo** człowieka będącego oskarżonym do tego by poszanowane było jego prawo do obrony. (Art. 48 ust. 2 KPP UE)

- **Prawo** człowieka będącego oskarżonym do obrony.
(Art. 48 ust. 2 KPP UE)

- **Prawo** człowieka do tego by nie zostać skazanym za popełnienie czynu polegającego na działaniu lub zaniechaniu, który według prawa krajowego lub prawa międzynarodowego nie stanowił czynu zabronionego pod groźbą kary w czasie jego popełnienia. (Art. 49 ust. 1 KPP UE)

- **Prawo** człowieka do tego by nie wymierzono kary surowszej od tej, którą można było wymierzyć w czasie, gdy czyn zabroniony pod groźbą kary został popełniony. (Art. 49 ust. 1 KPP UE)

- **Prawo** człowieka do tego by zastosowanie miała zastosowanie kara łagodniejsza, jeśli ustawa, która weszła w życie po popełnieniu czynu zabronionego pod groźbą kary, przewiduje karę łagodniejszą. (Art. 49 ust. 1 KPP UE)

- **Prawo** człowieka do tego by kary nie były nieproporcjonalnie surowe w stosunku do czynu zabronionego pod groźbą kary. (Art. 49 ust. 3 KPP UE)

- **Prawo** człowieka do tego by nie być ponownie sądzonym lub ukaranym w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary, w odniesieniu do którego zgodnie z ustawą został już uprzednio uniewinniony lub za który został już uprzednio skazany prawomocnym wyrokiem na terytorium Unii. (Art. 49 KPP UE)

4. Art. 1. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 1 RODO nie nakłada na administratora żadnych konkretnych obowiązków z punktu widzenia Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, komentowany przepis jedynie informuje, że w RODO ustanowione są obowiązki mające na celu ochronę osób fizycznych i ochronę uprawnień osób fizycznych.

5. Art. 1. Konkretyzacja zasad

Artykuł 1 RODO nie konkretyzuje zasad z art. 5 RODO. Związek jaki można dostrzec między art. 1 RODO a zasadami z art. 5 RODO jest taki, że art. 1 RODO, zwłaszcza jeżeli uznamy go za przepis kierunkujący interpretację przepisów RODO, kierunkuje interpretację art. 5 RODO. Można zatem stwierdzić, że zasady z art. 5 RODO należy interpretować w duchu art. 1 RODO, czyli tak by stosowanie zasad jednocześnie: chroniło osoby fizyczne i zapewniało

swobodny przepływ danych osobowych, chroniło prawa i wolności osób fizycznych w szczególności ich prawo do ochrony danych osobowych, nie ograniczało swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Podejście takie ma pewne znaczenie dla interpretacji zasad, zwłaszcza zasady minimalizacji i skłania do łagodnego rozumienia tej zasady, o czym dokładniej mowa w uwagach do art. 5 ust. 1 lit c RODO, zamieszczonych w równolegle przygotowywanej pozycji.[71]

6. Art. 1. Postulaty de lege ferenda

6.1. Art. 1. Wstęp.

Jakie prawa chroni RODO

Ze słów: „Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych." wnioskujemy, jak napisałem wyżej, że RODO chroni „podstawowe prawa i wolności osób fizycznych", zwłaszcza chroni prawo do ochrony danych osobowych. Czai się tu pewna pułapka. Prawo do ochrony danych osobowych występuje w art. 8 Karty Praw Podstawowych Unii Europejskiej. Powstaje zatem sytuacja, w której prawo do ochrony danych osobowych wymienione jest w KPP UE i w RODO. Prawo do ochrony danych osobowych jest prawem podstawowym ponieważ jest o nim mowa w KPP UE, to samo prawo do ochrony danych osobowych występuje w art. 1 ust. 2 RODO. Prawo do ochrony danych osobowych, występujące w art. 1 ust. 2 RODO jest prawem podstawowym z dwóch powodów. Ponieważ występuje w KPP UE, jako prawo podstawowe i ponieważ w art. 1 ust. 2 RODO jest ono nazwane prawem podstawowym. Należy tu zwrócić uwagę, że i w KPP UE i w art. 1 ust. 2 RODO mowa jest o tym samym, jednym prawie, a mianowicie o prawie do ochrony danych osobowych. i tu właśnie pojawia się problem, ponieważ w art. 1 ust. 2 RODO napisano, że RODO „chroni podstawowe prawa i wolności osób fizycznych" i jako przykład takich praw i wolności podano „prawo do ochrony danych osobowych". Wydaje się, że prawo do ochrony danych osobowych jest raczej prawem niż wolnością, ale to

[71] J. Rzymowski, *RODO – GDPR. Przetwarzanie danych osobowych. Zasady. Zgodność z prawem*, Łódź. 2021. (3.3. Art. 5 ust. 1 lit. c. Uwaga 3. Treść zasady, podejście łagodne.) (Publikacja powstająca równolegle z niniejszą.)

niewielki problem, nad którym można przejść do porządku. Można uznać, że RODO chroni podstawowe prawa i wolności i, że przykładowym, podstawowym prawem, jakie chroni RODO jest prawo do ochrony danych osobowych. Świadomie wróciłem w rozważaniach, po raz kolejny do tego samego, do prawa do ochrony danych osobowych. i tu właśnie widzę problem. Skoro prawo do ochrony danych osobowych jest przykładowych prawem jakie jest chronione przez RODO, to trzeba zadać pytanie o to jakie to jeszcze podstawowe prawa i wolności osób fizycznych chroni RODO. Droga najbezpieczniejsza wyjaśnienia jest taka, że RODO chroni te same prawa i wolności, które chroni KPP UE. Nie jest to niestety dobra droga. RODO pełne jest praw, które w KPP UE nie występują, na przykład, by daleko nie szukać, prawo do bycia zapomnianym, prawo do żądania ograniczenia przetwarzania, uprawnienia informacyjne itd. W RODO jest wiele uprawnień, których nie ma w KPP UE. Można oczywiście usiłować poszczególne prawa wynikające z RODO uznać za odpowiadające poszczególnym prawom wynikającym z KPP UE. Jest to jakaś droga, jednak jest to, moim zdaniem, droga uzasadniania poglądów prawodawcy, poza tym zestawienie praw wynikających z RODO z prawami wynikającymi z KPP UE wskazuje, że z RODO wynika wiele praw, których w KPP UE nie znajdziemy.

Uważam, że właściwsza jest inna droga. Na przepis trzeba popatrzeć bez złudzeń i szczerze powiedzieć, że nie do końca wiadomo o jakich to „podstawowych prawach i wolnościach" osób fizycznych stanowi RODO. Że nie wiadomo które prawa i wolności są podstawowe a które nie. Oczywiście dalszy wniosek może być tylko jeden. Skoro przepis jest niejasny to należy go poprawić, jeśli nie jest niezbędny to usunąć.

6.2. Art. 1. Postulat 2.
Doprecyzowanie czyje prawa chroni RODO

Z rozważań prowadzonych w analizie (2. Art. 1. Analiza) wynika, że z uwagi na pewną niejasność analizowanego przepisu, można mieć wątpliwość w kwestii tego, prawa jakich osób fizycznych RODO chroni. Czy RODO chroni prawa osób fizycznych, których dane dotyczą, czy też innych osób fizycznych, zwłaszcza osób fizycznych występujących po stronie administratora danych. Wydaje się, że RODO chroni prawa osób, których dane dotyczą, jednak,

szczerze powiedziawszy, z przepisu to nie wynika a dobrze by wynikało. W związku z powyższym postuluję nowelizację art. 4 pkt 1 RODO w następujący sposób:
„W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem **dotyczących ich** danych osobowych oraz przepisy o swobodnym przepływie danych osobowych."
(Czcionką wytłuszczoną zaznaczyłem słowa dodane.)

6.3. Art. 1. Postulat 3.
Potrzeba poprawienia nie zaś usunięcia przepisu

Przede wszystkim należy odpowiedzieć na pytanie, czy przepis jest niezbędny. Uważam, że tak. Dobrze, że jest na początku RODO przepis, który wyjaśnia, co jest celem RODO. Oczywiście powinien czynić to w sposób zrozumiały i stąd stawiam niżej postulat (6.3. Art. 1. Postulat 2. Doprecyzowanie treści przepisu.). W sytuacji dylematu interpretacyjnego[72] na gruncie RODO, interpretator powinien mieć jakąś wskazówkę, wskazówkę, która pomogłaby mu w podjęciu decyzji w sytuacji skrajnego braku danych koniecznych do podjęcia decyzji lub w sytuacji zbiegu argumentów za podjęciem decyzji na tak i na nie – za ochroną danych i przeciw tej ochronie. Postulat jest zatem taki, by przepisu nie usuwać a tylko go poprawić. Wydaje się, że najlepiej by było gdyby treść przepisu odpowiadała jego tytułowi. Tytuł przepisu brzmi: „przedmiot i cele".

Przepis był niewątpliwie pisany przez ekspertów, wydaje się więc właściwe dopasowanie formy przepisu do tytułu, przy jednoczesnym pozostawieniu możliwie niezmienionej treści przepisu.

W związku z powyższym postuluję nowelizację art. 1 ust. 1 RODO i art. 1 ust. 2 RODO we wskazany poniżej sposób, przy czym w proponowanej treści przepisu ujmuję również postulat (6.2. Art. 1. Postulat 2. Doprecyzowanie czyje prawa chroni RODO.)
„1. **przedmiotem rozporządzenia są:**
~~W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie~~

[72] Pojęcie „dylematu interpretacyjnego" zawdzięczam prof. P. Chmielnickiemu, dziękuję Panie Profesorze.

ochrona osób fizycznych w związku z przetwarzaniem **ich** danych osobowych i o~~raz przepisy o~~ swobodny~~m~~ przepływ~~ie~~ danych osobowych.
2. **Celem rozporządzenia jest ochrona** ~~Niniejsze rozporządzenie chroni~~ podstawowe**ych** praw~~a~~ i wolności osób fizycznych, w szczególności **dotyczącego** ich praw~~o~~**a** do ochrony danych osobowych." (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Przepis po nowelizacji miałby postać:
„1. przedmiotem rozporządzenia są:
ochrona osób fizycznych w związku z przetwarzaniem danych osobowych i
swobodny przepływ danych osobowych"
2. celem rozporządzenia jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności dotyczącego ich prawa do ochrony danych osobowych"

Uważam, że dobrze, by po zaproponowanej części przepisu, umieszczono jego obecny ustęp 3.

6.4. Art. 1. Postulat 4.
Doprecyzowanie treści przepisu

Przepis stanowi: „**Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych**.". Z zamieszczonych powyżej rozważań wynika, że nie do końca wiadomo jakie to prawa przepis chroni. Z rozważań skonsolidowanych w (6.1. Art. 1 postulaty de lege ferenda. Wstęp.) wynika, że dobrze by przepis zawierał wskazówkę na wypadek dylematu interpretacyjnego. Postuluję zatem by art. 1 ust. 2 RODO miał następującą postać: „Niniejsze rozporządzenie chroni prawo do ochrony danych osobowych.".

6.5. Art. 1. Postulat 5.
Dalsze doprecyzowanie treści przepisu

W pozycji „6.1. Art. 1 postulaty de lege ferenda. Wstęp." wyjaśniłem, że, jeżeli się spojrzy bez złudzeń, to nie wiadomo o jakich prawach osób fizycznych stanowi przepis, stanowiąc, że je chroni. Wyżej (6.4. Postulat 4. Doprecyzowanie treści przepisu.) postuluję, by

jako prawo chronione wskazać prawo do ochrony danych osobowych. Przepis stanowi: *Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.* Z zamieszczonych powyżej rozważań wynika, że nie do końca wiadomo jakie to prawa. W art. 5 ust. 1 RODO zapisano *Zasady dotyczące przetwarzania danych osobowych*. Dalej, część wstępna art. 5 ust. 1 RODO stanowi: *Dane osobowe muszą być:*. I dalej wymienione są kolejne zasady. Są one wymienione w przepisie i nieco, dość ułomnie, zdefiniowane. Piszę o tym dalej przy okazji omawiania art. 5 RODO.[73] Tu zwracam uwagę na pewien szczegół. Zasady te są to zasady w znaczeniu dyrektywalnym,[74] czy też „zasady systemu prawa" [75]. Z treści art. 5 ust. 1 RODO, a zwłaszcza słów wprowadzających, wynika, że zasady wymienione w art. 5 RODO to obowiązki administratora. Obowiązki administratora stanowią jednocześnie uprawnienia osób, których dane dotyczą. Piszę o zasadach, zasadach zapisanych w przepisie, zasadach w znaczeniu dyrektywalnym, zasadach systemu prawa, czyli niewątpliwie, zasady te, czyli obowiązki administratora, czyli uprawnienia osób, których dane dotyczą mają charakter istotny.[76] Skoro są to istotne uprawnienia, czyli prawa, to nic nie stoi na przeszkodzie by nie wskazać na nie już w art. 1 RODO. Postuluję zatem, by art. 1 ust. 3 RODO miał następującą postać:

„Niniejsze rozporządzenie chroni:

prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą zgodności z prawem;

prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą rzetelności;

---

[73] J. Rzymowski, *RODO – GDPR. Przetwarzanie danych osobowych. Zasady. Zgodność z prawem*, Łódź. 2021. (Publikacja powstająca równolegle z niniejszą.)

[74] S. Wronkowska, M. Zieliński, Z. Ziembiński. Zasady prawa. Zagadnienia podstawowe. Warszawa 1974. s. 14-15.

[75] K. Opałek, J. Wróblewski. Zagadnienia teorii prawa. Warszawa 1969. s. 92.

[76] W wywodzie głównym, dla uproszczenia zrównuję zasady z obowiązkami i z uprawnieniami, mam jednak świadomość, że godzi to w zasadę niesprzeczności, zaznaczam więc, że o ile zasady to obowiązki, tylko inaczej nazwane, to uprawnienia z obowiązków tych wynikają a nie są z nimi tożsame. Uprawnienie i obowiązek są zjawiskami o tym samym charakterze ontologicznym, jednak w zakresie znaczenia, treści, zawartości ontologicznej, nie należy ich utożsamiać.

prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą przejrzystości.;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą ograniczenia celu;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z minimalizacji danych;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą prawidłowości;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą ograniczenia przechowywania;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą integralności;
prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z zasadą poufności".

Przyznam, że postulat ten stawiam niejako wbrew sobie. Zasadom poświęcony jest art. 5 RODO. Powtarzanie ich w art. 1 RODO nie wydaje się roztropne. Z drugiej jednak strony lepiej wbić do głowy adresatom RODO, że zasady dotyczące przetwarzania danych są istotne, niż tego nie czynić lub tak jak teraz jest to w komentowanym przepisie napisane, pisać w mętny sposób, że „(…) chroni podstawowe prawa i wolności osób fizycznych (…)".

Wobec zaproponowanego postulatu, można postawić pewien zarzut. Zasady z art. 5 ust. 1 RODO to obowiązki administratora, innymi słowy, zasady z art. 5 ust. 1 RODO są obowiązkami administratora. Obowiązki administratora to uprawnienia osób, których dane dotyczą, innymi słowy obowiązki administratora są uprawnieniami osób, których dane dotyczą. Poprawniej mówiąc, obowiązki administratora są związane z uprawnieniami osób, których dane dotyczą. I tu może pojawić się pewien zgrzyt. Można powiedzieć o prawie do przetwarzania danych w sposób zgodny z prawem, jednak stwierdzenie: „prawo do przetwarzania danych osobowych w sposób zgodny z prawem do przetwarzania w sposób rzetelny" wydaje się horrendalne. Pewien merytoryczny sens to ma bowiem pierwsze prawo - „prawo do przetwarzania danych osobowych" to prawo leżące po stronie osoby, której dane dotyczą, drugie prawo: „w sposób zgodny z prawem do przetwarzania w sposób rzetelny" to w istocie obowiązek ADO, jednak można to wszystko wyrazić prościej, tak też poniżej postuluję.

6.5. Art. 1. Postulat 6.
Ostateczne doprecyzowanie treści przepisu

Konsolidując postulaty postawione powyżej postuluję by art. 1 RODO miał treść wskazaną poniżej.

„Przepis po nowelizacji miałby postać:

„1. przedmiotem rozporządzenia są:

ochrona osób fizycznych w związku z przetwarzaniem danych osobowych i

swobodny przepływ danych osobowych"

2. celem rozporządzenia jest ochrona prawa osób fizycznych do ochrony dotyczących ich danych osobowych

Celem rozporządzenia jest ochrona:

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób zgodny z prawem;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób rzetelny;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób przejrzysty;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób ograniczony co do celu;

prawo osób, których dane dotyczą, do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób prawidłowy;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób ograniczony co do przechowywania;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób integralny;

prawa osób, których dane dotyczą, do przetwarzania danych osobowych w sposób poufny".

3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych."

6.6. Art. 1. Postulat 7.
Poprawka motywu 1 Preambuły RODO

W motywie 1 Preambuły RODO napisano, że: *Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.* Jednocześnie w art. 8 ust. 1 KPP UE napisano: *Każdy ma prawo do ochrony danych osobowych, które go dotyczą.*

W KPP UE jest zatem chronione prawo do ochrony danych osobowych, nie zaś, jak wynika z motywu 1 Preambuły RODO – osoby fizyczne w związku z przetwarzaniem danych osobowych. Wygada to obecnie tak, jakby autorzy RODO zajrzeli do KPP UE, jednak zaniedbali przy tym dokładnej lektury tego aktu prawnego.

W związku z powyższym, postuluję by motyw 1 RODO miał treść następującą:
„Ochrona ~~osób fizycznych w związku z przetwarzaniem~~ danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. (Czcionką przekreśloną zaznaczam słowa usunięte.)"

6.7. Art. 1. Postulat 8.
Rozszerzenie zakresu przedmiotowego RODO na poziomie art. 2 ust. 2 RODO

Wyżej w analizie *2. Art. 1. Analiza*, przy okazji analizy słów: *(...) o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych (...)*, piszę, że *Interes administratora, rozumiany abstrakcyjnie, ogólnie, w oderwaniu od konkretnych stanów faktycznych, nie wydaje się być w niczym mniej ważny niż prawa osób, których dane dotyczą.* Tu mogę dodać, że analiza przepisów RODO wskazuje na fakt, że prawodawca dba w RODO nie tylko o prawa i wolności osób, których dane dotyczą, ale również o interesy administratora. Wynika to np. z art. 21 RODO, w którym opisane jest prawo do sprzeciwu. Osoba, której dane dotyczą może złożyć, w pewnych sytuacjach

sprzeciw wobec przetwarzania dotyczących jej danych, jednak administrator, również w pewnych sytuacjach, może po rozpatrzeniu sprzeciwu osoby której dane dotyczą, nadal dotyczące jej dane przetwarzać.

Podobnie rzecz się ma z art. 17 RODO, który osobie, której dane dotyczą, daje w pewnych sytuacjach, prawo do żądania usunięcia danych, której jej dotyczą. Osoba, której dane dotyczą ma prawo zażądać ich usunięcia (nieco upraszczam), zaś administrator ma obowiązek to żądanie rozpatrzyć, co jednak nie oznacza, że zawsze administrator ma obowiązek te dane usunąć. W pewnych sytuacjach administrator dane usuwa, bo ma taki obowiązek, w innych sytuacjach administrator danych nie usuwa, tylko dalej je przetwarza bo ma taki obowiązek.

Jak zatem widać, RODO chroni nie tylko prawa osób, których dane dotyczą, ale również prawa administratorów. Można też na sprawę spojrzeć tak, że RODO chroni nie tylko prawa osób fizycznych, ale również prawa innych podmiotów, jeżeli podmioty te są administratorami (danych).

Widać to też na przykładzie art. 6 ust. 1 lit. f RODO. Z przepisu tego wynika konieczność ważenia „prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią" z podstawowymi prawami i wolnościami osoby fizycznej. Jeżeli uświadomimy sobie, że administrator może być osobą fizyczną, to okazuje się, że słowa o prawnie uzasadnionych interesach mogą być rozumiane jako mówiące o prawach i wolnościach administratora. Uważam, że różnica jest tu głównie w warstwie językowej. Analogicznych przykładów w RODO jest więcej, ograniczam się tu do wyżej wskazanych, uważam bowiem, że nawet one wskazują, że RODO chroni nie tylko prawa osób fizycznych, zwłaszcza osób, których dane dotyczą, ale również prawa i wolności administratorów.

W związku z powyższym postuluję nowelizację art. 1 ust. 2 RODO we wskazany poniżej sposób.

„2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych **oraz prawa i wolności administratorów**" (Czcionką wytłuszczoną zaznaczam słowa dodane.)

7. Art. 1. Rozważania historyczne.
7.1. Art. 1 Rozważanie 1.
Odpowiedniki w dawnej legislacji

Odpowiednikiem art. 1 RODO jest art. 1 Dyrektywy 95/46/WE i art. 1 UODO97.

Hielke Hijmans pisze wręcz, że *Article 1 is the sequel of Article 1 DPD (...)*.[77] Różnice między przepisami wynikają z ich nieco innego kontekstu historycznego, tudzież z faktu, że RODO i Dyrektywa 95/46/WE to akty inaczej działające, do innych kategorii podmiotów skierowane. RODO, jak wiadomo, działa wprost, Dyrektywa 95/46/WE działała przez krajowe akty prawne.

[77] H. Hijmans w: *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 51

Rozdział drugi

Artykuł 2 RODO

Artykuł 2 RODO

Materialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.
4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad

odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.

7. Art. 2. Rozważania historyczne.[78]

7.1. Art. 2 Rozważanie 1.

Odpowiedniki w dawnej legislacji

Odpowiednikiem art. 2 RODO jest art. 3 Dyrektywy 95/46/WE i art. 2 UODO97 i art. 3a UODO97. Tematyka zbliżona poruszana jest również w art. 3 UODO97.

[78] Numer „7" nie jest tu błędem, a dostosowaniem do konwencji publikacji.

Artykuł 2 ust. 1 RODO

Materialny zakres stosowania

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. (…)

1. Art. 2 ust. 1. Komentarz

Przepis precyzuje zakres przedmiotowy RODO.

Zakres przedmiotowy RODO odwołuje się do przetwarzania danych osobowych. RODO stosuje się do przetwarzania danych osobowych w sposób opisany w przepisie. Samo przetwarzanie zdefiniowane jest w art. 4 pkt 2 RODO.

Przetwarzanie danych, które skutkuje stosowaniem RODO to przetwarzanie w sposób zautomatyzowany. Zautomatyzowanie przetwarzania danych osobowych może być całkowite lub częściowe.

Dzięki użyciu funktora *lub*, dane osobowe mogą być przetwarzane tylko w sposób całkowicie zautomatyzowany, lub tylko w sposób częściowo zautomatyzowany, lub w sposób zautomatyzowany jednocześnie całkowicie i częściowo.

Wydaje się, że możliwe jest przetwarzanie, które jest jednocześnie zautomatyzowane całkowicie i częściowo – po prostu na różnych etapach danej czynności jest ona wykonywana to tak to tak.

Przetwarzanie danych, które skutkuje stosowaniem RODO to również przetwarzanie w sposób niezautomatyzowany

Dzięki użyciu słowa: *oraz*, czyli odpowiednika słowa: „i”, RODO dotyczy zarówno przetwarzania danych w sposób zautomatyzowany, jak i przetwarzania danych w sposób niezautomatyzowany.

Jeśli chodzi o przetwarzanie danych osobowych w sposób niezautomatyzowany, to RODO obejmuje swym zakresem przetwarzanie danych w sposób niezautomatyzowany, o ile dane tak przetwarzane stanowią część zbioru danych.

Również, jeśli chodzi o przetwarzanie danych osobowych w sposób niezautomatyzowany, to RODO obejmuje swym zakresem przetwa-

rzanie danych w sposób niezautomatyzowany, o ile dane tak przetwarzane mają stanowić część zbioru danych. Angielska wersja przepisu każe sądzić, że mowa tu o danych co do których zamiarowane jest (ADO zamiaruje) włączenie do zbioru danych.

Dzięki użyciu funktora *lub*, dane osobowe, których dotyczy przepis mogą stanowić cześć zbioru danych lub mogą go nie stanowić, oczywiście przy zachowaniu pozostałych warunków, wynikających z przepisu.

Podsumowując poczynione powyżej ustalenia można stwierdzić jak poniżej.

RODO ma zastosowanie do przetwarzania danych osobowych
- jedynie w sposób całkowicie zautomatyzowany.

I jednocześnie

RODO ma zastosowanie do przetwarzania danych osobowych
- jedynie w sposób częściowo zautomatyzowany.

I jednocześnie

RODO ma zastosowanie do przetwarzania danych osobowych
- w sposób częściowo zautomatyzowany i w sposób całkowicie zautomatyzowany.

Wskazane wyżej trzy sposoby przetwarzania są niezależne od tego czy dane przetwarzane na jeden z tych sposobów stanowią cześć zbioru danych albo mają stanowić część zbioru danych albo stanowią cześć zbioru danych i mają stanowić cześć zbioru danych (na przykład innego zbioru danych niż ten, którego część obecnie stanowią).[79]

Wskazane wyżej trzy sposoby przetwarzania są również niezależne od tego czy dane przetwarzane na jeden z tych sposobów są zapisane czy nie są zapisane.

Jeśli chodzi o przetwarzanie danych w sposób inny niż zautomatyzowany, to RODO ma zastosowanie do przetwarzania danych osobowych:
- stanowiących część zbioru danych.

I jednocześnie

[79] Por. M. Gumularz *Ochrona danych osobowych w sektorze publicznym. Rozdział II. POJĘCIE DANYCH OSOBOWYCH. 2.Podziały danych osobowych i ich praktyczne konsekwencje. 2.3.Dane uporządkowane oraz nieuporządkowane. 2.3.1. Ogólne informacje.* Warszawa 2018, Lex.

RODO ma zastosowanie do przetwarzania danych osobowych
- mających stanowić część zbioru danych.
I jednocześnie
RODO ma zastosowanie do przetwarzania danych osobowych
- stanowiących część zbioru danych i mających stanowić część zbioru danych.

2. Art. 2 ust. 1. Analiza

Słowa: „**Materialny zakres stosowania**" stanową tytuł art. 2 RODO. Analiza przepisu w kontekście jego treści prowadzi do wniosku, że w art. 2 RODO uregulowano czego RODO dotyczy a czego nie. Również w art. 2 RODO napisane jest czego RODO dotyczy, tyle, że w art. 2 RODO napisano to znacznie szczegółowiej. Sam tytuł to tylko nazwa, istotne jest znaczenie tytułu a przez to znaczenie przepisu. Uważam, że można stwierdzić, że o ile w art. 1 RODO uregulowano przedmiot RODO, to w art. 2 RODO, przedmiot ten doprecyzowano.

Ze słów: „**Niniejsze rozporządzenie ma zastosowanie do** (…)" należy wnosić, że przepis statuuje zakres przedmiotowy RODO. Artykuł 2 ust. 1 RODO statuuje zakres przedmiotowy RODO w sposób pozytywny – wskazując jakie czynności objęte są zakresem RODO, przepis kolejny - art. 2 ust. 2 RODO statuuje zakres przedmiotowy RODO w sposób negatywny – wskazując jakie czynności nie są objęte zakresem RODO.

Ze słów: „(…) **zastosowanie do przetwarzania danych osobowych** (…)" należy wnosić, że zakres przedmiotowy RODO odwołuje się do przetwarzania danych osobowych. RODO stosuje się do przetwarzania danych osobowych w sposób opisany w przepisie. Samo przetwarzanie zdefiniowane jest w art. 4 pkt 2 RODO.

Ze słów wytłuszczonych: „(…) **przetwarzania danych osobowych w sposób** całkowicie lub częściowo **zautomatyzowany** (…)" należy wnosić, że przetwarzanie danych, które skutkuje stosowaniem RODO to przetwarzanie w sposób zautomatyzowany. Zautomatyzowane przetwarzanie danych jest utożsamiane z przetwarzaniem danych z wykorzystaniem komputerów.

Twierdzi tak P. Fajgielski, który za czynności zautomatyzowane uważa czynności dokonywane w komputerowej bazie danych ale też czynności wykonywane z użyciem programów biurowych, takich jak edytory tekstu i arkusze kalkulacyjne.[80]

Twierdzi tak D. Lubasz: *W konsekwencji objęte rozporządzeniem będzie nie tylko przetwarzanie w systemach teleinformatycznych, lecz także inne sposoby automatycznego przetwarzania na innych urządzeniach, np. wideorejestratorach samochodowych, bodycamach czy kamerach zainstalowanych na dronach, utrwalających zapis*.[81] Wartościowe jest zwrócenie uwagi na wideorejestratory i pozostałe urządzenia, ale co do systemów informatycznych, zachowuję daleko idący dystans.

W podobnym kierunku idzie wywód K. Wygody,[82] który zautomatyzowane przetwarzanie danych osobowych dostrzega w przetwarzaniu danych osobowych przez sztuczną inteligencję (z tym stanowiskiem się zgadzam), w przetwarzaniu danych osobowych przez *pojedyncze urządzenia „inteligentne" (np. liczniki, zamki, klucze) (...)*. Wywód K. Wygody nie jest do końca jasny, w zakresie dotyczącym przetwarzania danych osobowych w komputerze, rozumianego jako przetwarzanie w sposób zautomatyzowany.

Naukowe sumienie nie pozwala mi przyłączyć się do powyższego chóru. Uważam, że nietrafne jest utożsamienie przetwarzania danych osobowych z użyciem komputerów z przetwarzaniem w sposób zautomatyzowany. Szczególnie uderza mnie przykład przetwarzania z wykorzystaniem edytora tekstu jako przetwarzania w sposób zautomatyzowany. Wyobraźmy sobie, że ktoś zapisuje dane osobowe w pliku stworzonym w edytorze tekstu i dokonuje tego naduszając od-

[80] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* w: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* WKP 2018 – Komentarz. Kom. do art. 2.

[81] D. Lubasz w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 126.

[82] K. Wygoda w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Warszawa 2018, s. 56.

powiednie klawisz klawiatury. Czy to jest czynność zautomatyzowana? Uważam, że nie. Program zwykle automatycznie zapisuje stan pliku, co czynnością zautomatyzowaną się wydaje, jednak już czynność zamknięcia pliku, jego zapisania na zewnętrznym nośniku i włożenia nośnika do szuflady nie są czynnościami zautomatyzowanymi. Czynności wykonywane w komputerze można zatem próbować uważać za czynności zautomatyzowane, ale to z uwagi na pogląd P. Fajgielskiego, do którego odnoszę się w uwadze *3.3. Art. 2 ust. 1. Uwaga 2. Czynności częściowo zautomatyzowane*, należy jednak otwarcie powiedzieć, że nie każda czynność na danych osobowych wykonana z użyciem komputerów jest czynnością zautomatyzowaną. Jednocześnie należy pamiętać, że uznanie, że dana czynność nie jest czynnością zautomatyzowaną może prowadzić do niestosowania RODO wobec takiej czynności, co z kolei z jednej strony godzi w prawa osoby, której dane dotyczą, z drugiej strony może zagrozić bezpieczeństwu prawnemu administratora.

Na marginesie powyższych rozważań należy zwrócić uwagę na fakt, że zautomatyzowane przetwarzanie danych nie odnosi się jedynie do danych zapisanych. Możliwe jest zautomatyzowane przetwarzanie danych, które nie są zapisane.

Ze słów: „(…) **całkowicie lub częściowo** (…)" należy wnosić, że samo zautomatyzowanie przetwarzania danych osobowych może być całkowite lub częściowe. W świetle rozważań prowadzonych powyżej, ciekawa jest możliwość przetwarzania w sposób *częściowo zautomatyzowany*. Być może właśnie w takim przetwarzaniu, przetwarzaniu częściowo zautomatyzowanym jest klucz do uznania czynności wykonywanych z wykorzystaniem komputera za czynności zautomatyzowane, bo nawet jeśli pewne czynności wykonywane z wykorzystaniem komputera nie są zautomatyzowane to pewne są i wtedy, kiedy jedne i drugie potraktujemy razem, to są to czynności częściowo zautomatyzowane. Nie jestem przekonany czy pogląd ten nie jest znajdywaniem sensu w przepisie nieco „na siłę", jednak zwracam uwagę, że rozszerzające rozumienie zakresu pojęcia czynności zautomatyzowanych prowadzi do lepszej ochrony praw osób, których dane dotyczą, co wydaje się pożądane.

Zużycia wyrazu wytłuszczonego: „(…) do przetwarzania danych osobowych w sposób całkowicie **lub** częściowo zautomatyzowany oraz

do przetwarzania w sposób inny niż zautomatyzowany (…)" należy wnosić, że dzięki użyciu funktora *lub*, dane osobowe mogą być przetwarzane tylko w sposób całkowicie zautomatyzowany, albo tylko w sposób częściowo zautomatyzowany, albo w sposób zautomatyzowany jednocześnie całkowicie i częściowo.

Wydaje się, że możliwe jest przetwarzanie, które jest jednocześnie zautomatyzowane całkowicie i częściowo – po prostu na różnych etapach danej czynności jest ona wykonywana to tak to tak.

Ze słów: „(…) **do przetwarzania w sposób inny niż zautomatyzowany** (…)" należy wnosić, że przetwarzanie danych, które skutkuje stosowaniem RODO to również przetwarzanie w sposób niezautomatyzowany

Ze słów: „(…) do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany **oraz** do przetwarzania w sposób inny niż zautomatyzowany (…)" należy wnosić, że dzięki użyciu słowa „oraz", czyli odpowiednika słowa: *i* RODO dotyczy zarówno przetwarzania danych w sposób zautomatyzowany, jak i przetwarzania danych w sposób niezautomatyzowany (inny niż zautomatyzowany).

Ze słów: „(…) **danych osobowych stanowiących część zbioru danych** (…)" należy wnosić, że jeśli chodzi o przetwarzanie danych osobowych w sposób niezautomatyzowany, to muszą to być dane osobowe stanowiące część zbioru danych, „zbiór danych" został zdefiniowany w art. 4 ust 6 RODO, jako : *uporządkowany zestaw danych osobowych (...)*.

Pojęcie zbioru danych jest tłumaczeniem słów „*filing system*". Trzeba przyznać, że nie jest to tłumaczenie szczęśliwe. „File" to plik, kartoteka, archiwum rejestr", „filing system" to zatem system porządkowania, „zbiór" jest to pewnym nadużyciem.[83] Jako czasownik, „file" znaczy „to arrange in order for preservation and reference",[84] czyli, w skrócie tłumacząc: „porządkować".

[83] Takie tłumaczenia podaje Google translator, pomijam przy tym tłumaczenia związane z piłami i pilnikami, bo o te narzędzia w przepisie nie chodzi. (dostęp: 2020.05.10. godz. 02.20).

[84] https://www.merriam-webster.com/dictionary/file (dostęp: 2020.05.10. godz. 02.22).

Ze słów: „(...) **mających stanowić część zbioru danych**.” należy wnosić, że jeśli chodzi o przetwarzanie danych osobowych w sposób niezautomatyzowany, to muszą to być dane osobowe o których przepis stanowi, że są to dane, które mają stanowić część zbioru danych. Angielska wersja przepisu każę sądzić, że mowa tu o danych co do których zamiarowane jest (ADO zamiaruje) włączenie do zbioru danych. *(...)* ***are intended to form*** *part of a filing system* – co uważam należy przetłumaczyć na: *(...) co do których planowane/zamierzane jest uczynienie ich częścią* – no i powiedzmy: *zbioru*.

Z użycia funktora „(...) **lub** (...)” należy wnosić, że dane osobowe, których dotyczy przepis mogą stanowić cześć zbioru danych bądź mogą go nie stanowić i jednocześnie mają go stanowić, o ile zachowane są pozostałe, opisane w przepisie warunki. Użycie funktora *lub* wskazuje, że możliwa jest jeszcze jedna sytuacja, otóż dane, których dotyczy przepis mogą jednocześnie i stanowić zbiór danych i go nie stanowić i jednocześnie te dane, które zbioru nie stanowią mają go stanowić. Tylko na pozór wydaje się to niemożliwe, w praktyce jest to możliwe, po prostu u jednego administratora pewne dane należą do zbioru i jednocześnie inna kopia tych samych danych u tego samego administratora nie należy do zbioru ale ma do niego należeć. W sensie fizykalnym nie są to te same dane, ale jeżeli ich treść się pokrywa, to w istocie są to te same dane.

3. Art. 2 ust. 1. Uwagi

3.1. Art. 2 ust. 1. Uwaga 1.
Przetwarzanie poza zakresem przedmiotowym RODO

Warto zauważyć, że z prowadzonych rozważań wynika, że RODO nie dotyczy przetwarzania danych w sposób niezautomatyzowany i jednocześnie nie stanowiących i nie mających stanowić części zbioru danych. Przykładem takiego przetwarzania danych osobowych jest na przykład sytuacja, w której sekretarka odbiera telefon, wysłuchuje danych osobowych osoby dzwoniącej, nie zapisuje ani nie zapamiętuje tych danych, po czym na przykład udziela osobie dzwoniącej informacji, o które ta pyta. W takim wypadku sekretarka przetwarza co prawda dane osobowe osoby dzwoniącej, jednak jest to przetwarzanie nieobjęte zakresem przedmiotowym RODO.

Dla zrozumienia zjawiska przetwarzania danych osobowych poza zakresem przedmiotowym RODO warto zastanowić się nad przetwarzaniem danych w portalach społecznościowych. Jeżeli osoba fizyczna publikuje tam informacje dotyczące innych osób fizycznych, w kontekście jej czynności o czysto osobistym lub domowym charakterze, to RODO takiej publikacji nie dotyczy. Należy jednak zwrócić uwagę na fakt, że czysto osobistego lub domowego charakteru nie można utożsamiać z charakterem niezawodowym. Nie lubię wyjaśnień kazuistycznych, uważam bowiem, że często, z uwagi na specyfikę stanów faktycznych, prowadzą one, zwłaszcza nieuważnego czytelnika, na intelektualne manowce, tym niemniej warto przypomnieć tu sprawę Lindquist. Istotą stanu faktycznego było w tej sprawie, że pani Lindquist publikowała informacje o kolegach, z którymi działała dobroczynnie w szwedzkim kościele. Pani Lindquist podnosiła, że ponieważ czynności, które łączyły ja z kolegami miały charakter religijny i dobroczynny, nie zaś ekonomiczny[85], to prawo ochrony danych (wtedy funkcjonowała Dyrektywa 95/46/WE) nie stosuje się do publikowania informacji w Internecie. ETS nie podzielił argumentów pani Lindquist.[86] Na sprawę tę zwraca uwagę H. Kranenborg, warto jednak uporządkować ustalenia.

- Publikowanie w Internecie informacji dotyczących innych osób znajduje się poza zakresem RODO, jeżeli ma to charakter czysto osobisty lub domowy.
- O czysto osobistym lub domowym charakterze przetwarzania danych osobowych nie decyduje czy relacja miedzy publikującym a osobami, których dane są publikowane ma charakter związany z jakąkolwiek pracą lub odpłatnością.
- Usługodawca, który udostępnia infrastrukturę, umożliwiającą wykonywanie na danych osobowych czynności (przetwarzanie danych) o czysto osobistym lub domowym charakterze, sam nie wykonuje na tych danych takich czynności – jego czynności nie mają charakteru czysto osobistego lub domowego. Pojawia się tu ciekawy

[85] H. Kranenborg w: *The EU General Data Protection Regulation (GDPR). A Commentary. Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler.* Oxford 2020. s. 67.

[86] Bodil Lindqvist Case C-101/01, Bodil Lindqvist, judgment of 6 November 2003 (ECLI: EU: C:2003:596).

problem, a mianowicie, te same dane są przetwarzane poza zakresem RODO i w zakresie RODO.

3.2. Art. 2 ust. 1. Uwaga 2.
Zbiór danych a zbiór danych osobowych

Należy tu zwrócić szczególną uwagę, że fakt, że zbiór danych, o którym jest mowa w przepisie, to zbiór danych a nie zbiór danych osobowych. W pierwszych słowach przepisu mowa jest o danych osobowych, więc mogłoby się wydawać, że i słowa o zbiorze dotyczą zbioru danych osobowych. Należy jednak zwrócić uwagę, na fakt, że jeżeli ograniczenie zbioru danych jedynie do zbioru danych osobowych może zawęzić zakres przedmiotowy RODO, a tym samym pozbawić część osób, które dane dotyczą, prawa do ochrony ich danych osobowych, co nie wydaje się roztropne. Jednocześnie należy zwrócić uwagę na fakt, że *zbiór danych* został zdefiniowany w art. 4 ust 6 RODO, jako: *uporządkowany zestaw danych osobowych (...)*, co znów zawęża zakres przedmiotowy RODO.

Dla poruszanych tu zagadnień ciekawe jest spostrzeżenie L. Kepy, a mianowicie, że: *Dane osobowe ze względu na ich ilość, strukturę i kryteria dostępności dzieli się na:*
- pojedyncze,
- w zestawach,
- w zbiorach.[87]

3.3. Art. 2 ust. 1. Uwaga 3.
Czynności częściowo zautomatyzowane

Przetwarzanie danych osobowych jest często bardzo złożonym procesem, który łączy w sobie czynności zautomatyzowane i czynności niezautomatyzowane. Zauważył to P. Fajgielski, który stwierdził: *Komentowany przepis nie wymaga, aby wszystkie czynności mieszczące się w zakresie przetwarzania realizowane były w sposób zautomatyzowany – wystarczy, że tylko niektóre operacje dokonywane będą w taki sposób, aby uznać, że przetwarzanie jest częściowo zautomatyzowane, co pociąga za sobą konieczność stosowania przepisów rozporządzenia*[88]. Niezwykle wartościowa jest cytowana myśl, którą

[87] L. Kępa, *Ochrona danych osobowych w praktyce.* Warszawa 2014, s. 36.

[88] P. Fajgielski, o*p. cit.*

ja rozumiem tak, że wystarczy by część czynności odbywała się w sposób zautomatyzowany, by wszystkie związane czynności znajdowały siew zakresie RODO. O ile z myślą P. Fajgielskiego się zgadzam, o tyle nie mogę się zgodzić z użyciem zwrotu: *wszystkie czynności mieszczące się w zakresie przetwarzania*, zwrot ten budzi mój sprzeciw, bowiem czynności to właśnie przetwarzanie.

3.4. Art. 2 ust. 1. Uwaga 4. Czynności częściowo zautomatyzowane, dane nieuporządkowane

Ciekawą uwagę poczynił M. Gumularz. Autor ten zwrócił uwagę na fakt, że *(...) brak w RODO przepisu, który wymagałby od administratora danych porządkowania danych osobowych według kryteriów umożliwiających dostęp do tych danych.*[89]. Rozwiniecie myśli wskazanego autora prowadzi do ciekawych wniosków. Jeżeli administrator (danych) nie przetwarza danych w sposób zautomatyzowany i nie zamierza przetwarzać danych w sposób zautomatyzowany i dane nie stanowią części zbioru i dane nie mają stanowić części zbioru danych, to takiego przetwarzania RODO nie dotyczy. Jest to oczywisty wniosek z art. 2 ust. 1 RODO, jednak dopiero takie zestawienie, sprowokowane poglądem M. Gumularza, daje pełną świadomość zjawiska, że dane przetwarzane w permanentnym nieładzie są danymi, których RODO nie dotyczy (w permanentnym nieładzie i jednocześnie poza komputerem).

Tytułem uzupełnienia myśli M. Gumularza, należy dodać, że wskazany przez niego brak obowiązku porządkowania danych osobowych wynika z faktu, że tych nieuporządkowanych danych RODO po prostu nie dotyczy, nie może zatem ustanawiać obowiązku uporządkowania, gdyby bowiem zawierało, to rozszerzałoby to zakres RODO. Rozważanie takie jest oczywiście możliwe, jednak prawodawca go nie zastosował.

[89] M. Gumularz *op. cit.*

3.4.1. Art. 2 ust. 1. Uwaga 4.1. Przetwarzanie zautomatyzowane niezapisanych danych osobowych

Na marginesie rozważań o czynnościach zautomatyzowanych warto zwrócić uwagę na jeden jeszcze problem. Należy otóż pamiętać, że czynności zautomatyzowane nie muszą być przeprowadzane wobec (na) danych osobowych zapisanych. Kuszący jest pogląd, zgodnie z którym RODO miałoby dotyczyć jedynie danych zapisanych. Niestety, mimo, że kuszący, to pogląd ten jest błędny. Nie sposób znaleźć uzasadnienia dla poglądu zgodnie z którym RODO dotyczyłoby jedynie danych zapisanych. Warto zwrócić tu uwagę na fakt, że analizowany art. 2 ust. 1 RODO stanowi o przetwarzaniu danych osobowych *w sposób całkowicie lub częściowo zautomatyzowany* i o przetwarzaniu danych osobowych *w sposób inny niż zautomatyzowany*, jednak przepis nie wskazuje, że przetwarzanie w jeden czy drugi sposób, by znajdować się w zakresie RODO, musi odbywać się na danych zapisanych.

Przykładem przetwarzania danych osobowych w sposób zautomatyzowany jest monitorowanie wizyjne, z wykorzystaniem sprzętu komputerowego, bez zapisu monitoringu i oczywiście w warunkach, w których monitoring dotyczy rozpoznawalnych osób. Podobnie sprawę widzi K. Wygoda.[90]

3.5. Art. 2 ust. 1. Uwaga 5. Przetwarzanie danych osobowych przez podmioty publiczne i podmioty prywatne

Ciekawą uwagę znaleźć można u Herke Kranenborga, autor ten pisze: *Article 2 does not differentiate between the public and private sectors, and thus covers both of them.*[91], czyli: *Artykuł 2 nie rozróżnia między sektorami publicznym i prywatnym i zatem dotyczy ich obydwu*[92]. Nie jestem zwolennikiem wskazywania czego akt prawny nie dotyczy, ponieważ to czego dotyczy zwykle wystarcza by wyjaśnić co do wyjaśnienia jest, tym niemniej rozumiem intencję wskazanego autora. Herke Kranenborg odnosi się bowiem do poglądu, zgodnie z któ-

[90] K. Wygoda, *op. cit.* s. 57.

[91] H. Kranenborg, *op. cit.* s. 63.

[92] Tłum. J. Rzymowski.

rym *(...) it would have been better to have tailor-made rules for the public sector*[93], czyli *lepiej by było mieć zasady dopasowane do sektora publicznego*[94].

Przyznam, że tak tego nigdy nie widziałem, zapewne z racji przyzwyczajenia do faktu, że i w poprzednim stanie prawnym przetwarzanie danych osobowych w sektorze publicznym i prywatnym było uregulowane jednakowo. Jednocześnie, zwłaszcza w praktyce, dostrzegałem, że przepisy (zarówno dawne jak i RODO) nie szanują specyfiki przetwarzania danych osobowych w sektorze publicznym, a szczególnie kwestii związanych z długoletnią archiwizacją i niemożnością wprowadzania poprawek do dokumentów zarchiwizowanych.

Nie stawiam postulatu rozdzielenia przepisów dotyczących ochrony danych na przepisy dotyczące sektora publicznego i przepisy dotyczące sektora prywatnego, tym bardziej, że gdyby takie rozróżnienie legislacyjne wprowadzić chciano, to w sektorze publicznym należałoby zmierzyć się z rozróżnieniem na przetwarzanie danych w sferze imperium i w sferze dominium, zaś w sektorze prywatnym należałoby zmierzyć się z przetwarzaniem danych w związku z realizacją zadań publicznych przez podmioty niepubliczne i z odróżnieniem takiego przetwarzania od przetwarzania nie w związku z realizacją zadań publicznych.

Lepiej chyba, że nikt się z tym zmierzyć nie chciał, ponieważ wprowadziłoby to zamieszanie przeokrutne.

Mając na uwadze powyższe rozważania, widzę jednak możliwość wprowadzenia w RODO wyłączeń wobec realizacji niektórych obowiązków przez niektóre kategorie podmiotów i to zdecydowanie na poziomie RODO. Kwestie te pozostawiono ustawodawcom krajowym, co godzi w koncepcje ujednolicenia ochrony danych w UE.

[93] H. Kranenborg w: *The EU General Data Protection Regulation (GDPR). A Commentary. Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler,* Oxford 2020. s. 63. Również wskazane tam: „Blume and Svanberg 2013: Blume and Svanberg, *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus*, 15 Cambridge Yearbook of European Legal Studies (2013), 27."

[94] Tłum. J. Rzymowski.

4. Art. 2 ust. 1. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 2 ust. 1 RODO pozornie nie nakłada na administratora żadnych konkretnych obowiązków. W istocie przepis ten nakłada na administratora obowiązki.
  Otóż **art. 2 ust. 1 RODO nakłada na administratora obowiązek** stosowania RODO jeżeli zachodzą pewne, opisane w przepisie warunki.

Administrator ma zatem obowiązek stosować RODO:

-- jeżeli przetwarza dane osobowe w sposób całkowicie zautomatyzowany
lub
-- jeżeli przetwarza dane osobowe w sposób częściowo zautomatyzowany
i
-- jeżeli administrator przetwarza dane osobowe w sposób niezautomatyzowany jednak dane te stanowią cześć zbioru danych osobowych lub dane te mają stanowić cześć zbioru danych osobowych.

- Jednocześnie **art. 2 ust. 1 RODO ustanawia uprawnienie**, które przysługuje każdej osobie której dotyczą dane osobowe. Uprawnienie polega na tym że osoba, której dotyczą dane osobowe ma prawo oczekiwać, że administrator stosuje RODO wobec dotyczących jej danych osobowych jeżeli zachodzą pewne, opisane w przepisie warunki.

Osoba, której dane dotyczą ma zatem prawo oczekiwać, że administrator stosuje RODO:

-- jeżeli administrator przetwarza dane osobowe w sposób całkowicie zautomatyzowany
lub
-- jeżeli administrator przetwarza dane osobowe w sposób częściowo zautomatyzowany
i
-- jeżeli administrator przetwarza dane osobowe w sposób niezautomatyzowany jednak dane te stanowią cześć zbioru danych osobowych lub dane te mają stanowić cześć zbioru danych osobowych.

5. Art. 2. ust. 1 Konkretyzacja zasad.

Artykuł 2 ust.1 RODO nie konkretyzuje zasad z art. 5 RODO. Można jednak wskazać na pewne związki miedzy art. 2 ust. 1 RODO a zasadami z art. 5 RODO.

Po pierwsze, art. 2 ust. 1 RODO warunkuje stosowanie zasad z art. 5 RODO. Jeżeli przetwarzanie danych osobowych nie spełnia warunków opisanych w art. 2 ust. 1 RODO to RODO, w danej sytuacji, nie skutkuje obowiązkami po stronie osób przetwarzających dane ani uprawnieniami po stronie osób, których dane dotyczą.

Po drugie, jeżeli przetwarzanie danych osobowych spełnia warunki opisane w art. 2 ust. 1 RODO to przepis ten, podobnie jak art. 1 RODO, uznać należy za przepis kierunkujący interpretację przepisów RODO, w tym kierunkujący interpretację art. 5 RODO.

6. Art. 2. ust. 1 Postulaty de lege ferenda

6.1 Art. 2. ust. 1 Postulat 1. Doprecyzowanie zakresu RODO

Wydaje się, że treść art. 2 ust. 1 RODO ogranicza poważnie zakres ochrony danych, ponieważ jeżeli dane nie są przetwarzane w sposób całkowicie lub częściowo zautomatyzowany i nie stanowią i nie mają stanowić części zbioru danych, to do danych tych RODO nie ma zastosowania. Zbiór danych zdefiniowany jest w art. 4 ust. 6 RODO. Możliwe jest zatem, że administrator tak skonstruuje wewnętrzne procedury przetwarzania, że mimo iż dane będzie przetwarzał, to przetwarzania tego, RODO nie będzie dotyczyło. Wystarczy wyobrazić sobie, że administrator przetwarza dane na papierze, przechowuje je w postaci nieuporządkowanej i w polityce ochrony danych zapisał, że z danych należących do konkretnych kategorii nie zamierza tworzyć zbiorów. Tak odbywającego się przetwarzania danych osobowych RODO by nie dotyczyło.

Jeżeli uważamy, że ochrona danych osobowych jest zjawiskiem dobrym i pożądanym, to dobrze by było, gdyby przepis nie umożliwiał łatwego obchodzenia go, by nie był łatwy do obejścia. Artykuł 2 ust. 1 RODO powinien raczej brzmieć np. tak: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych". Ewentualne zawężenia zakresu rozporządzenia powinny wtedy mieć postać wyjątków, na przykład takich: „Rozporządzenie nie ma zas-

tosowania do przetwarzania danych osobowych, które nie stanowią części zbioru danych i nie będą go stanowić".

6.1 Art. 2. ust. 1 Postulat 2. Dalsze doprecyzowanie zakresu RODO

Uwaga *3.2. Art. 2 ust. 1. Uwaga 2. Zbiór danych a zbiór danych osobowych* prowadzi do wniosku, że zakres przedmiotowy RODO zależy częściowo od rozumienia pojęcia „zbiór danych". Jeżeli rozumie się je szeroko, jako zbiór jakichkolwiek danych, czyli danych osobowych i danych nieosobowych, to rozszerza to zakres RODO, jeżeli rozumie się je wąsko, jako zbiór danych osobowych, to zawęża to zakres RODO. Operacje te należy prowadzić na poziomie art. 2 ust. 1 RODO, czyli przepisu o charakterze zasady, od której w art. 2 ust. 2 RODO są wyjątki, który to przepis jest też dalej uszczegóławiany przez art. 6 RODO i przez art. 9 RODO. Rozstrzygniecie konkretnego dylematu interpretacyjnego typu:

zasada>wyjątek>zasada>wyjątek,

może nie być łatwe, kiedy nie do końca wiadomo jaki jest zakres znaczenia zasady. Dla ułatwienia dokonywania wykładni przepisu należy zastąpić *zbiór danych* „zbiorem danych osobowych".

Artykuł 2 ust. 1 RODO, po wprowadzeniu Postulatu 2 miałby brzmienie:

„Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych osobowych lub mających stanowić część zbioru danych osobowych."

Artykuł 2 ust. 1 RODO, po wprowadzeniu postulatu 2 i postulatu 1 brzmiałby:

„Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych", zaś jego doprecyzowanie: „Rozporządzenie nie ma zastosowania do przetwarzania danych osobowych, które nie stanowią części zbioru danych osobowych i nie będą go stanowić".

Artykuł 2 ust. 1 RODO powinien raczej brzmieć np. tak: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych".

Ewentualne zawężenia zakresu rozporządzenia powinny wtedy mieć postać wyjątków, na przykład takich: „Rozporządzenie nie ma

zastosowania do przetwarzania danych osobowych, które nie stanowią części zbioru danych osobowych i nie będą go stanowić”

.

Artykuł 2 ust. 2 RODO

Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

1. Art. 2 ust. 2. Komentarz

Przepis statuuje zakres przedmiotowy RODO.[95]

Artykuł 2 ust. 2 RODO statuuje zakres przedmiotowy RODO w sposób negatywny – wskazując jakie czynności nie są objęte zakresem RODO.

Artykuł 2 ust. 1 RODO ma zakres szerszy niż art. 2 ust. 2 RODO. Kolejne punkty art. 2 ust. 2 RODO zawierają opis kolejnych sytuacji, w których przetwarzanie nie jest objęte zakresem RODO.

Można stwierdzić, że art. 2 ust. 1 RODO statuuje zasadę, zaś art. 2 ust. 2 RODO statuuje wyjątki wobec tej zasady. Stwierdzenie to ma daleko idące skutki, ponieważ wyjątków nie należy interpretować rozszerzająco.[96]

Trafna jest uwaga K. Wygody, który stwierdza, że „ustanowione wyłączenia nie odnoszą się do przesłanek mieszczących się w ustępie 1, ale maja charakter podmiotowy (ust. 3) lub związany z celem

[95] P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych.* Komentarz, Warszawa 2018, s. 138.

[96] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 179.

aktywności, która w sposób obiektywny może być uznana za przetwarzanie danych.[97]

RODO nie ma zastosowania do przetwarzania danych osobowych które zachodzi w ramach działalności nieobjętej zakresem prawa UE.

RODO nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdziału 2 TUE. Tytuł V rozdziału Traktatu o Unii Europejskiej brzmi: *POSTANOWIENIA OGÓLNE O DZIAŁANIACH ZEWNĘTRZNYCH UNII i POSTANOWIENIA SZCZEGÓLNE DOTYCZĄCE WSPÓLNEJ POLITYKI ZAGRANICZNEJ I BEZPIECZEŃSTWA*, rozdział drugi tego tytułu brzmi: *Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa*. Rozdział 2 tytułu V TUE stanowi o polityce zagranicznej, bezpieczeństwie UE, wspólnej polityce obronnej – sprawy te, na gruncie komentowanego przepisu wyłączono z zakresu RODO.

RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Fakt, że działalność nie ma charakteru zawodowego lub, że działalność nie ma charakteru handlowego, nie przesądza o tym, że działalność taka ma charakter czysto osobisty lub czysto domowy. Działalność czysto osobista lub domowa to działalność bez związku z działalnością zawodową lub handlową. Jeżeli działalność ma związek z działalnością zawodową lub handlową, to nie jest to działalność osobista lub domowa.

Tylko osoby fizyczne mogą mieć sprawy osobiste lub domowe. Spraw osobistych lub domowych nie może mieć na przykład spółka, urząd, szpital, stowarzyszenie czy uczelnia, podmioty takie nie mogą zatem skorzystać z wyłączeń spod zakresu RODO opartych na przetwarzanie danych osobowych w ramach czynności o czysto osobistym lub domowym charakterze.

Wyłączenie spod zakresu RODO nie jest związane z celem przetwarzania danych osobowych.

RODO nie ma zastosowania nie tylko do czynności podejmowanych przez osobę fizyczną, ale i przez organ tyle że do czynności opisanych dalej w przepisie.

[97] K. Wygoda w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 55.

RODO nie ma zastosowania do przetwarzani danych przez organy, ale jedynie wtedy, kiedy organy te przetwarzają dane osobowe do celów opisanych dalej w przepisie. Te organy, które realizują cele wskazane w przepisie.

Cele o których mowa w przepisie i które realizowane przez właściwe organy sprawiają, że do przetwarzania danych osobowych w związku z ich realizacją nie ma zastosowania RODO to:
- cele zapobiegania przestępczości.
- cele prowadzenia postepowań przygotowawczych.
- cele wykrywania i ścigania czynów zabronionych lub wykonywania kar.

Z przepisu wynika, że ze stosowania RODO zwalnia przetwarzanie danych osobowych:
- jedynie w celu wykrywania czynów zabronionych, albo
- jedynie w celu ścigania czynów zabronionych, albo
- jedynie w celu wykonywania kar , albo
- w celu wykrywania czynów zabronionych i w celu ścigania czynów zabronionych, albo
- w celu wykrywania czynów zabronionych i w celu wykonywania kar.
- Ze stosowania RODO zwalnia również przetwarzanie danych osobowych do celu, którym jest przetwarzanie danych osobowych do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

2. Art. 2 ust. 2. Analiza.

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do** (...)" należy wnosić, że przepis statuuje zakres przedmiotowy RODO.[98] Przy czym o ile art. 2 ust. 1 RODO statuuje zakres przedmiotowy RODO w sposób pozytywny – wskazując jakie czynności objęte są zakresem RODO, o tyle art. 2 ust. 2 RODO statuuje zakres przedmiotowy RODO w sposób negatywny – wskazując jakie czynności nie są objęte zakresem RODO. Artykuł 2 ust. 1 RODO ma zakres ogólniejszy, a przez to szerszy niż art. 2 ust. 2 RODO. Kolejne punkty art.

[98] P. Litwiński (red.) P. Barta, M. Kawecki, *loc. cit.*

2 ust. 2 RODO zawierają opis kolejnych sytuacji, w których może, co prawda, zachodzić przetwarzanie danych osobowych, jednak do przetwarzania tego RODO nie ma zastosowania, czyli przetwarzanie to nie jest objęte zakresem RODO. Można stwierdzić, że art. 2 ust. 1 RODO statuuje zasadę, zaś art. 2 ust. 2 RODO statuuje wyjątki wobec tej zasady. Stwierdzenie to ma daleko idące skutki. Wyjątków nie należy interpretować rozszerzająco.[99] Piszę o tym niżej w uwagach.

Niezwykle ciekawa i trafna jest uwaga K. Wygody, który stwierdza, że *ustanowione wyłączenia nie odnoszą się do przesłanek mieszczących się w ustępie 1, ale maja charakter podmiotowy (ust. 3) lub związany z celem aktywności , która w sposób obiektywny może być uznana za przetwarzanie danych*.[100].

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:**
a) w ramach działalności nieobjętej zakresem prawa Unii; (...)" należy wnosić, że RODO nie ma zastosowania do przetwarzania danych osobowych które zachodzi w ramach działalności nieobjętej zakresem prawa UE. Prawodawca w Preambule stanowi: *Niniejsze rozporządzenie nie ma zastosowania do kwestii ochrony podstawowych praw i wolności ani do swobodnego przepływu danych osobowych w związku z działalnością nieobjętą zakresem prawa Unii, taką jak działalność dotycząca bezpieczeństwa narodowego. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w związku z działaniami związanymi ze wspólną polityką zagraniczną i bezpieczeństwa Unii*, co w znacznej mierze wyjaśnia przepis.

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:** (...)
b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE; (...)" należy wnosić, że RODO nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdziału 2 TUE. Tytuł V rozdziału

[99] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 179.,

[100] K. Wygoda, *loc. cit.*

Traktatu o Unii Europejskiej brzmi: *POSTANOWIENIA OGÓLNE O DZIAŁANIACH ZEWNĘTRZNYCH UNII I POSTANOWIENIA SZCZEGÓLNE DOTYCZĄCE WSPÓLNEJ POLITYKI ZAGRANICZNEJ I BEZPIECZEŃSTWA*, rozdział drugi tego tytułu brzmi: *Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa*. Rozdział 2 tytułu V TUE stanowi o polityce zagranicznej, bezpieczeństwie UE, wspólnej polityce obronnej – sprawy te, na gruncie komentowanego przepisu wyłączono z zakresu RODO.

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:** (...)
c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze; (...)" należy wnosić, że RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach wykonywanych przez nią czynności o czysto osobistym lub domowym charakterze.

Niewątpliwie chwili zastanowienia wymaga czym są czynności o czysto osobistym charakterze i czym są czynności o czysto domowym charakterze.

Jeśli chodzi o czynności o czysto osobistym charakterze, to komentatorzy wypowiadają się w tej sprawie, jednak trudno na razie o ostateczne wnioski.

Autorzy poradnika dla radców prawnych i adwokatów piszą: *Poprzez przetwarzanie w ramach czynności o charakterze osobistym lub domowym rozumie się przetwarzanie bez związku z działalnością zawodową lub handlową.*[101]. Pozornie nie sposób nie zgodzić się z tym stanowiskiem, uważam jednak, że utożsamienie, które tu się w zasadzie odbyło, charakteru osobistego lub domowego z działalnością zawodową lub handlową jest zbyt dużym uproszczeniem, tym bardziej, że przepis nie mówi o jedynie o charakterze osobistym, ale o charakterze **czysto** osobistym, **czysto** domowym. Nie chcę wdawać się tu w kazuistykę, tym bardziej, że na razie, kiedy nie ma jeszcze ukształtowanego orzecznictwa, przykłady musiałyby być wyimaginowane, przez co mogłyby być błędne, podkreślam jednak, że fakt, że działalność nie ma charakteru zawodowego lub, że działalność nie ma

[101] *Poradnik dla radców prawnych i adwokatów. Ogólne rozporządzenie o ochronie danych (RODO).* X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka, s. 16.

charakteru handlowego, nie przesądza o tym, że działalność taka ma charakter czysto osobisty lub czysto domowy.

Trafnie na motyw 18 Preambuły RODO zwracają uwagę P. Litwiński, P. Barta i M. Kawecki [102]. Prawodawca przedkłada tam, że działalność czysto osobista lub domowa to działalność bez związku z działalnością zawodową lub handlową. Uważam, że ze wskazanego motywu wynika przede wszystkim, że jeżeli działalność ma związek z działalnością zawodową lub handlową, to nie jest to działalność osobista lub domowa.

We wskazanym motywie Preambuły zwraca się dalej uwagę na przykładowe rodzaje działalności osobistej lub domowej. Prawodawca wymienia korespondencję i przechowywanie adresów podtrzymywanie więzi społecznych oraz działalność internetową podejmowaną w ramach podtrzymywania więzi społecznych. Prawodawca zwraca jednak dalej uwagę w wskazanym motywie, że RODO ma zastosowanie *do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej* – odnoszą się do tego P. Litwiński, P. Barta i M. Kawecki, [103] pisząc, ze jeżeli podmiot korzysta z serwisu społecznościowego, to tyczy się go omawiane wyłączenie, jednak podmiotu taki serwis prowadzącego wyłączenie się nie tyczy. Zgadzam się z tym jednak konieczne jest tu poczynienie pewnych uwag. Przede wszystkim nie można mówić o „podmiocie". Uważam, że należy zdecydowanie stać na stanowisku, że tylko osoby fizyczne mogą mieć sprawy osobiste lub domowe zaś RODO dotyczy kogoś kto prowadzi serwis społecznościowy, ponieważ prowadzenie takowego trudno za takie sprawy uznać. Na podobne zjawisko zwraca uwagę K. Wygoda, który twierdzi,[104] że zakresem RODO nie jest objęte wykonywanie przez osobę fizyczną jej hobby, działalność filantropijna, działalność społeczna i działalność artystyczna, o ile działalności te nie zostaną sformalizowane. W wypowiedzi K. Wygody dostrzegalny jest jednak pewien dystans i ostrożność, które są całkiem zrozumiałe, uważam bowiem że w odniesieniu do wskazanych sfer działalności człowieka, trudno czasem powiedzieć czy dzia-

[102] P. Litwiński (red.) P. Barta, M. Kawecki *op. cit.* s. 147.

[103] P. Litwiński (red.) P. Barta, M. Kawecki *op. cit*. s. 149.

[104] K. Wygoda *op. cit*. s. 60.

łalność taka ma charakter osobisty czy już takowego charakteru nie ma. Wystarczy wyobrazić sobie wystąpienie artysty amatora, na które ten zaprasza swoich znajomych oraz znajomych tychże znajomych. Na pierwszy rzut oka zdarzenie takie wydawałoby się zdarzeniem o charakterze osobistym, jeżeli jednak do stanu faktycznego dołożymy wydanie wejściówek umożliwiających wejście do pomieszczenia w którym ów koncert się odbywa, dystrybucję tych wejściówek - choćby pocztą elektroniczną - sporządzenie listy osób którym wejściówki wydano i w oparciu o którą wpuszcza się dane osoby do pomieszczenia i tak dalej i tak dalej, to może się okazać że zdarzenie o charakterze osobistym wywołało niekorzystny skutek dla jednej lub większej ilości tych osób. Oczywiście zdarzenie o charakterze osobistym może wywołać taki skutek, wystarczy wyobrazić sobie na przykład zatrucie pokarmowe u osób zaproszonych na całkiem prywatne przyjęcie urodzinowe. Tu właśnie otwiera się pole do interpretacji, z jednej strony osoba fizyczna zaprasza znajomych na urodziny, z drugiej strony podmiot gospodarczy przetwarza dane w celu wystawienia faktury. Bogactwo potencjalnych stanów faktycznych mieszczących się między tymi skrajnościami jest ogromne, co w jakimś stopniu wyjaśnia brak skrystalizowanego stanowiska w omawianej kwestii nawet tylko u komentatorów przepisu.

Jeśli chodzi o czynności o domowym charakterze to wartościowa jest uwaga D. Lubasza, który odsyła do wersji angielskiej i do wersji niemieckiej RODO,[105] wersja angielska każe interpretować czynności o czysto domowym charakterze jako czynności związane z prowadzeniem gospodarstwa domowego, wersja niemiecka, każe interpretować czynności o czysto domowym charakterze jako czynności związane z rodziną.

Paweł Litwiński, P. Barta i M. Kawecki prowadzą dalej długie rozważania nad tym, że RODO nie dotyczy działań ***w ramach*** *czynności o czysto osobistym lub domowym charakterze* (podkr. J. Rz.), nie zaś w celach o takim charakterze. Rozważania wskazanych autorów są trafne, ich trafność dostrzegam jednak głównie w tym, że lektura tekstu wskazanych autorów zwraca uwagę na fakt że wyłączenie spod

[105] D. Lubasz w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M.Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka. Warszawa 2018. s. 138.

zakresu RODO nie jest związane z celem przetwarzania. Rozważania nad słowem „ramy" wydają się nieco jałowe, zwłaszcza jeżeli porównamy różne wersje językowe komentowanego przepisu w wersji angielskiej użyto słów *within the context* które oznaczają mniej więcej to co oznaczają polskie słowa *w kontekście*, w wersji czeskiej użyte są słowa: *v souvislosti*, co można przetłumaczyć na *kontekst* ale też na *związek* lub *odniesienie*.

Wydaje się, że jeżeli osoba fizyczna uzyska, lub uzyskuje sporadyczny przychód w związku na przykład ze sprzedażą należących do niej przedmiotów, jednak osoba ta nie prowadzi w tym zakresie działalności, to RODO nie dotyczy czynności na danych, wykonywanych przez tę osobę fizyczną, w związku z taką sprzedażą[106]. Uważam, że jest tak dlatego, że osoba ta, nie prowadzi działalności handlowej a jedynie pozbywa się niepotrzebnych przedmiotów.

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych**: (...)
d) **przez właściwe organy** (…)" należy wnosić, że RODO nie ma zastosowania do przetwarzania danych osobowych przez podmioty, określone w przepisie jako *właściwe organy*. Fakt, że RODO nie ma zastosowania do przetwarzani danych przez organy jest niezwykle istotny, z komentowanego przepisu wynika bowiem, ze RODO nie ma zastosowania nie tylko do czynności podejmowanych przez osobę fizyczną, o czym piszę wyżej, ale i przez organ tyle że do czynności opisanych dalej w przepisie.

Ze słów: „**Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych**: (...)
d) **przez właściwe organy do celów** (…)" należy wnosić, że RODO nie ma zastosowania do przetwarzani danych przez organy, ale jedynie wtedy, kiedy organy te przetwarzają dane osobowe do celów opisanych dalej w przepisie.

Jeśli chodzi o właściwe organy, to na pierwszy rzut oka przepis nie wskazuje jakie to są owe właściwe organy. Bliższe przyjrzenie się przepisów każe sądzi, że właściwe organy, to te organy, które realizują cele wskazane w przepisie.

[106] Podobnie: P. Litwiński (red.) P. Barta, M. Kawecki, *op. cit.* s. 149 - 150.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: (...)
d) przez właściwe organy **do celów zapobiegania przestępczości**, (...)" należy wnosić, że cele o których mowa w przepisie i które realizowane przez właściwe organy sprawiają, że do przetwarzania danych osobowych w związku z ich realizacją nie ma zastosowania RODO cele zapobiegania przestępczości.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: (...)
d) przez właściwe organy **do celów** (...) **prowadzenia postępowań przygotowawczych**, (...)" należy wnosić, że cele przetwarzania, które również zwalniają ze stosowania RODO to cele prowadzenia postępowań przygotowawczych.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: (...)
d) przez właściwe organy **do celów** (...), **wykrywania i ścigania czynów zabronionych lub wykonywania kar**, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.". należy wnosić, że cele przetwarzania, które również zwalniają ze stosowania RODO to cele wykrywania i ścigania czynów zabronionych lub wykonywania kar. z przepisu wynika, że ze stosowania RODO zwalnia przetwarzanie danych osobowych:
- jedynie w celu wykrywania czynów zabronionych, albo
- jedynie w celu ścigania czynów zabronionych, albo
- jedynie w celu wykonywania kar, albo
- w celu wykrywania czynów zabronionych i w celu ścigania czynów zabronionych, albo
- w celu wykrywania czynów zabronionych i w celu wykonywania kar.

Użycie funktora *i* nie jest tu trafne, należy interpretować przepis tak, jakby użyto tu przecinka albo jakby użyto tu słowa „lub", szerzej piszę o tym w uwadze *3.1. Art. 2 ust. 2. Uwaga 1. Niewłaściwe użycie funktora „i"*.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: (...)

d) **przez właściwe organy do celów** zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, **w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom**. ." należy wnosić, że ze stosowania RODO zwalnia przetwarzanie danych osobowych do celu, którym jest przetwarzanie danych osobowych do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Tu również należy uznać, że prawodawca użył *i* jedynie przypadkiem, bowiem sensowne byłoby tu użycie „lub" w miejsce *i*.

3. Art. 2 ust. 2. Uwagi

3.1. Art. 2 ust. 2. Uwaga 1. Niewłaściwe użycie funktora *i*

Artykuł 2 ust. 2 lit d RODO stanowi: *przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*.

Użycie funktora *i*, w zwrocie: *wykrywania i ścigania czynów zabronionych* nie jest najszczęśliwszym pomysłem. Z użycia funktora *i* wynika bowiem, że RODO nie ma zastosowania jeżeli właściwe organy przetwarzają dane osobowe do celów wykrywania i ścigania czynów zabronionych, czyli i do wykrywania i do ścigania. Idąc jeszcze dalej, RODO nie ma zastosowania, jeżeli właściwe organy przetwarzają dane osobowe do realizacji obydwu celów połączonych słowem *i* czyli i do wykrywania i do ścigania czynów zabronionych. Wynika z tego wniosek, że jeżeli właściwe organy przetwarzają dane osobowe do jednego z wymienionych celów, ale do drugiego nie, to do takiego przetwarzania RODO ma zastosowanie. Językowa interpretacja przepisu prowadzi do wniosku, że jeżeli właściwy organ przetwarza dane osobowe jedynie w celu wykrywania czynów zabronionych lub jedynie w celu ściągania czynów zabronionych, to do takiego przetwarzania RODO ma zastosowanie. Ułomna konstrukcja przepisu, gdyby interpretować go językowo, prowadziłaby do sytuacji, w której zachodzi opisane dalej następstwo czynności.

- Właściwy organ przetwarza dane osobowe do celów wykrywania czynów zabronionych. Organ ten nie przetwarza danych osobowych do celów ścigania czynów zabronionych, więc RODO ma zastosowanie do przetwarzania danych osobowych do celów wykrywania czynów zabronionych.
- Następnie ten sam, lub inny organ zaczyna przetwarzać dane osobowe do celów ścigania czynów zabronionych. Organ ten, lub inny, przetwarzał te same dane do celów wykrywania czynów zabronionych, więc teraz dane osobowe są przetwarzane do celów wykrywania czynów zabronionych i do celów ścigania czynów zabronionych, więc RODO nie ma zastosowania ani do wykrywania czynów zabronionych ani do ścigania czynów zabronionych. Tyle, że wcześniej miało zastosowanie, kiedy organ przetwarzał dane tylko do celów wykrywania czynów zabronionych.

Wniosek z opisanych czynności jest absurdalny,[107] najpierw RODO ma zastosowanie, potem nie ma. Nie przemawia za tym, żaden racjonalny powód a jedynie niefrasobliwe użycie słowa *i*.

Gorsza jeszcze sytuacja zachodzi jeżeli dane osobowe nie są przetwarzane w celu wykrywania czynów zabronionych a jedynie w celu ścigania czynów zabronionych. Jeżeli właściwe organy jedynie ścigają czyny zabronione, ale nie zajmują się ich wykrywaniem, to nie zachodzi zjawisko przetwarzania danych osobowych w celu wykrywania czynów zabronionych i w celu ścigania czynów zabronionych. Co więcej zajść ono nie może. Czyny zostały na przykład wykryte dawno temu, zanim pojawiło się RODO, a teraz są jedynie ścigane. Patrząc językowo – do takiego ścigania a w zasadzie do przetwarzania danych osobowych do celów ścigania czynów zabronionych, ale jedynie ścigania, RODO ma zastosowanie.

3.2. Art. 2 ust. 2. Uwaga 2.
Ponowne niewłaściwe użycie funktora *i*

Artykuł 2 ust. 2 lit d RODO stanowi: „w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.”

[107] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 150.

Użycie funktora *i*, nie jest i tu najszczęśliwszym pomysłem. Z użycia funktora *i* wynika bowiem, że RODO nie ma zastosowania jeżeli właściwe organy przetwarzają dane osobowe do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i do celów zapobiegania zagrożeniom bezpieczeństwa publicznego. Niezwykłe jest to, że ten sam błąd popełniono w jednym przepisie dwukrotnie, tak jakby jego autor, anonimowy ekspert Parlamentu Europejskiego, nie miał świadomości rzeczywistego znaczenia słowa *i*. Może nie miał.

Językowa interpretacja przepisu prowadzi i tu do wniosku, że jeżeli właściwy organ przetwarza dane osobowe jedynie w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego lub jedynie w celu zapobiegania zagrożeniom bezpieczeństwa publicznego, to do takiego przetwarzania RODO ma zastosowanie. Ułomna konstrukcja przepisu, gdyby interpretować go językowo, prowadziłaby do sytuacji, w której przetwarzanie danych osobowych w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i w celu zapobiegania zagrożeniom bezpieczeństwa publicznego zwalniałoby ze stosowania RODO, jednak przetwarzanie w jednym z tych celów nie zwalniałoby ze stosowania RODO. Piramidalna wręcz absurdalność[108] takiego wniosku sprawia, że należy go odrzucić i interpretować przepis tak jakby zamiast użyć *i*, użyto „lub". Takie też podstawienie zastosowałem przy interpretacji przepisu w komentarzu *1. Art. 2 ust. 2. Komentarz* i w analizie *2. Art. 2 ust. 2. Analiza*.

3.3. Art. 2 ust. 2. Uwaga 3. Artykuł 2 ust. 1 RODO jako zasada, art. 2 ust. 2 RODO jako wyjątek

Zwracam uwagę na pewną pułapkę, w którą może łatwo wpaść interpretator. Z art. 6 RODO i z art. 9 RODO wynika ogólny zakaz przetwarzania danych osobowych. Zakaz ten jest zasadą, zaś kolejne dopuszczenia przetwarzania wynikają z kolejnych liter art. 6 ust. 1 RODO i z kolejnych liter art. 9 ust. 2 RODO. Uprawnione jest zatem stwierdzenie, że przetwarzanie danych jest zabronione i że dopuszczone jest ono wyłącznie w zakresie objętym przesłankami zawartymi w art. 6 ust. 1 RODO lub w art. 6 ust. 2 RODO.

[108] L. Morawski, *loc. cit.*

Uprawnione jest więc stwierdzenie, że zasadą jest zakaz przetwarzania danych osobowych i że wyjątki spod zakresu tej zasady ustanowione są w art. 6 ust. 1 RODO i w art. 9 ust. 2 RODO. Nieuważny interpretator może więc zastanawiać się nad następującym problemem. Zasada wynika z art. 2 ust. 1 RODO. Wyjątki spod zakresu tej zasady wynikają z art. 2 ust. 2 RODO. Jednocześnie zasada wynika z art. 6 ust. 1 RODO i z art. 9 ust. 1 RODO. Wyjątki spod zakresu tej zasady wynikają z kolejnych liter art. 6 ust. 1 RODO i z art. 9 ust. 2 RODO. Która regulacja jest zasadą? Która jest wyjątkiem? Który przepis ma charakter prawa ogólnego? Który przepis ma charakter prawa szczególnego? Jak to poukładać? Rzecz jest wbrew pozorom prosta, wymaga jednak pewnej uwagi. Rozplątuję rzecz poniżej.

Z art. 2 ust. 1 RODO wynika ogólna zasada zgodnie z którą RODO ma zastosowanie do przetwarzania danych w pewnych warunkach, warunki te są wymienione w art. 2 ust. 1.

Z art. 2 ust. 2 wynikają wyjątki, zgodnie z którymi RODO nie ma zastosowania do przetwarzania danych osobowych w pewnych warunkach, warunki te są wymienione w kolejnych literach art. 2 ust. 2 RODO.

Warunki z art. 2 ust. 1 RODO mają charakter zasady. Z przepisu tego wynika, kiedy RODO ma zastosowanie, czyli kiedy dane osobowe są chronione. Jeżeli ochronę danych osobowych uznajemy za coś właściwego, dobrego, to należy uznać, że lepiej jest dane osobowe chronić niż ich nie chronić. Skoro tak, to lepiej by zakres ochrony danych osobowych był możliwie szeroki, niżby miał być wąski. Te pozornie naiwne rozważania prowadzę po to by uzasadnić, że jeżeli pojawiają się wątpliwości jak interpretować kolejne elementy art. 2 ust. 1 RODO, to należy interpretować je niezawężająco. Nie jest to wyjątek, więc nie ma tu miejsca zakaz wykładni rozszerzającej wyjątku[109] i jednocześnie każde zawężenie zakresu art. 2 ust. 1 RODO godzi w ochronę danych osobowych, czyli w interesy osób, których dane osobowe dotyczą.

Warunki z art. 2 ust. 1 RODO mają charakter wyjątków. z przepisu tego wynika, kiedy RODO nie ma zastosowania, czyli kiedy dane osobowe nie są chronione. Ponieważ są to wyjątki, to zgodnie z zasadą zakazu dokonywania wykładni rozszerzającej wyjątków[110] nie

[109] L. Morawski, *op. cit*. s. 179.

[110] L. Morawski, *loc. cit.*

wolno interpretować ich rozszerzająco. Należy przy tym zwrócić uwagę, że każde rozszerzenie zakresu art. 2 ust. 2 RODO godzi w ochronę danych osobowych, czyli w interesy osób, których dane osobowe dotyczą. Jak widać argument z wykładni prawa zbiega się tu z argumentem aksjologicznym. Zbiega się, jeżeli oczywiście interpretator uważa ochronę danych osobowych za dobro. Jeżeli nawet interpretator nie uważa ochrony danych osobowych za dobro, to bezpieczniej dla niego jest by przepisy interpretował wbrew sobie, ponieważ sankcje, czy to administracyjne, czy to cywilne, czy to karne (krajowe, spoza RODO ale też groźne) są zbyt poważne, by ryzykować spór z PUODO, lub z sądami, spór, w którym interpretujący w imieniu ADO przepisy interpretator podnosiłby, że ochrona danych osobowych to zło.

3.4. Art. 2 ust. 2. Uwaga 4. Artykuł 2 ust. 1 RODO jako zasada, art. 2 ust. 2 RODO jako wyjątek

Artykuł 2 ust. 1 RODO zawiera zasadę zgodnie z którą przetwarzane są dane osobowe. Artykuł 2 ust. 2 RODO zawiera wyjątki spod zasady ustanowionej w art. 2 ust. 1 RODO. Im węższy jest wyjątek, tym lepiej chronione są dane osobowe. Im szerszy jest wyjątek, tym gorzej chronione są dane osobowe. Dwukrotne użycie słowa *i* w art. 2 ust. 2 RODO, zawęża stosowanie tego przepisu, tym samym podnosi poziom ochrony danych osobowych. Zamiana słowa *i* na słowo „lub" w art. 2 ust. 2 RODO, rozszerza stosowanie tego przepisu, tym samym obniża poziom ochrony danych osobowych. Mając to na uwadze można by zaryzykować tezę, że dwukrotne użycie słowa *i*, w art., 2 ust. 2 RODO, jest zasadne, podnosi bowiem poziom ochrony danych osobowych. Obniżanie poziomu ochrony danych osobowych wydaje się być czymś złym, podnoszenie poziomu ochrony danych osobowych wydaje się być czymś dobrym. Mając, z kolei, to na uwadze można by optować za tym, by słowo *i* pozostało w przepisie i nie postulować zmiany *i* na „lub". Analiza przepisu na poziomie: zasada/wyjątek, pozwala postawić, postawiony wniosek. Drobiazgowa analiza przepisu, przeprowadzona w uwadze *3.1. Art. 2 ust. 2. Uwaga 1. Niewłaściwe użycie funktora „i"* oraz w uwadze *3.2. Art. 2 ust. 2. Uwaga 2. Ponowne niewłaściwe użycie funktora „i"*, każe jednak wniosek ten odrzucić, widać z niej bowiem, że słowa *i* użyto

może nie przypadkowo, ale na pewno nieumiejętnie, w sposób prowadzący do wykazanych we wskazanych uwagach, absurdalnych wniosków. Mając wreszcie to na uwadze, stawiam niżej postulat *6.1 Art. 2 ust. 2. Postulat 1*.

4. Art. 2 ust. 2. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Art. 2 ust. 2 RODO pozornie nie nakłada na ADO żadnych konkretnych obowiązków. W istocie przepis ten nakłada na ADO obowiązki.
  Otóż art. 2 ust. 2 RODO nakłada na ADO obowiązek stosowania RODO jeżeli zachodzą pewne, opisane w przepisie warunki.
  ADO ma zatem obowiązek stosować RODO :

-- jeżeli przetwarza dane osobowe w ramach działalności objętej zakresem prawa Unii

lub

-- jeżeli przetwarza dane osobowe jako państwo członkowskie poza ramami wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE

lub

-- jeżeli przetwarza dane osobowe jako osoba fizyczna poza czynnościami o czysto osobistym lub domowym charakterze

-- jeżeli przetwarza dane osobowe poza przetwarzaniem tych danych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

- Jednocześnie art. 2 ust. 2 RODO ustanawia uprawnienie, które przysługuje każdej osobie której dotyczą dane osobowe. Uprawnienie polega na tym że osoba, której dotyczą dane osobowe ma prawo oczekiwać, że ADO stosuje RODO wobec dotyczących jej danych osobowych jeżeli zachodzą pewne, opisane w przepisie warunki.
  Osoba, której dane dotyczą ma zatem prawo oczekiwać, że ADO stosuje RODO:

-- jeżeli administrator przetwarza dane osobowe w ramach działalności objętej zakresem prawa Unii
lub
-- jeżeli administrator przetwarza dane osobowe jako państwo członkowskie poza ramami wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE
lub
-- jeżeli administrator przetwarza dane osobowe jako osoba fizyczna poza czynnościami o czysto osobistym lub domowym charakterze
lub
-- jeżeli administrator przetwarza dane osobowe poza przetwarzaniem tych danych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Mając na uwadze powyższe rozważania, należy pamiętać, że obowiązki w zakresie przetwarzania danych osobowych pojawiają się o tyle o ile nie zachodzą okoliczności skutkujące wyłączeniem z zakresu RODO, wskazane w innych przepisach od art. 1 RODO do art. 3 RODO.

5. Art. 2. ust. 1 Konkretyzacja zasad.

Artykuł 2 ust. 2 RODO nie konkretyzuje zasad z art. 5 RODO. Można jednak wskazać na pewne związki miedzy art. 2 ust. 1 RODO a zasadami z art. 5 RODO.

Po pierwsze, art. 2 ust. 2 RODO, podobnie jak art. 2 ust. 1 RODO warunkuje stosowanie zasad z art. 5 RODO. Jeżeli przetwarzanie danych osobowych nie spełnia warunków opisanych w art. 2 ust. 2 RODO to RODO, w danej sytuacji, nie skutkuje obowiązkami po stronie osób przetwarzających dane ani uprawnieniami po stronie osób, których dane dotyczą.

Po drugie, jeżeli przetwarzanie danych osobowych spełnia warunki opisane w art. 2 ust. 2 RODO to przepis ten, podobnie jak art. 1 RODO i jak art. 2 ust. 1 RODO, uznać należy za przepis kierunkujący interpretację przepisów RODO, w tym kierunkujący interpretację art. 5 RODO.

6. Art. 2 ust. 2. Postulaty de lege ferenda

6.1 Art. 2 ust. 2. Postulat 1.
Użycie funktorów logicznych we właściwy sposób

W art. 2 ust. 2 lit d RODO dwukrotnie użyto słowa *i*. Słowo *i* ma konkretną wartość logiczną, oznacza ono, że zachodzą łącznie obydwa zjawiska połączone tą literą. W uwadze *3.1. Art. 2 ust. 2. Uwaga 1. Niewłaściwe użycie funktora „i”* oraz w uwadze *3.2. Art. 2 ust. 2. Uwaga 2. Ponowne niewłaściwe użycie funktora „i”* wyjaśniłem drobiazgowo dlaczego użycie słowa *i* w komentowanym przepisie, co więcej, dwukrotne użycie tego słowa, jest błędem oraz, że interpretacyjnie należy przyjać, że użyte w przepisie *i* oznaczają „lub“. Interpretacja interpretacją, uważam jednak, że przepis nie powinien być tak niechlujnie napisany.

Słowa takie jak „i“ czy „lub“ mają konkretne znaczenie. Posługiwanie sie tymi słowami bez poszanowania dla tego znaczenia jest okazaniem pogardy dla logiki, czyli działu filozofii ogólnej, dla stosowania logiki w prawie, wreszcie jest dowodem na rozpaczliwą niekompetencje autorów przepisu. Nie pozostaje nic innego jak zaproponować jego poprawioną wersję.

Przepis powinien zatem mieć treść:
„przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania **lub** ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego **lub** zapobiegania takim zagrożeniom.”.
(Wytłuściłem słowa „lub”, którymi zastąpiłem słowa „i”).

Artykuł 2 ust. 3 RODO

Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.

1. Art. 2 ust. 3. Komentarz

Do przetwarzania danych osobowych opisanego w przepisie ma zastosowanie rozporządzenie (WE) nr 45/2001. Tym samym przepis komentowany wskazuje że przetwarzanie danych osobowych opisane w nim, regulowane jest przez wskazany akt prawny.

Przepis dotyczy przetwarzania danych osobowych przez podmioty wskazane w przepisie.

Podmioty wskazane w przepisie i do przetwarzania danych osobowych przez które przepis się odnosi to instytucje, organy i jednostki organizacyjne Unii.

Niestety przepis jest źle napisany w wersji angielskiej i źle przetłumaczony na język polski. Odnoszę się do tego w uwadze *3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora „i" oraz przecinka* i w postulacie *6.1 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego.*

Interpretacja celowościowa, nieco poprawiona wobec językowej prowadzi do wniosku, że wskazane w przepisie rozporządzenie ma zastosowanie do przetwarzania danych osobowych:

- jedynie przez instytucje UE lub
- jedynie przez organy UE lub
- jedynie przez jednostki organizacyjne UE lub
- przez organy UE i jednocześnie przez jednostki organizacyjne UE lub
- przez instytucje UE i jednocześnie przez organy UE i jednocześnie przez jednostki organizacyjne UE.

Wersja angielska przepisu stanowi również o przetwarzaniu danych przez agencje UE. Szerzej w postulacie *6.2 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego.*

Rozporządzenie (WE) nr 45/2001 (czyli: Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych) oraz inne akty prawne wydane przez organy UE, które to akty prawne mają zastosowanie do przetwarzania danych osobowych przez podmioty wskazane w przepisie, zostają zmienione a dokładniej, dostosowane.
Wskazane akty prawne zostają dostosowane do zasad i przepisów RODO. Akty prawne o których mowa w przepisie zostają dostosowane do przepisów RODO w tym do zasad z art. 5 RODO. Szerzej omawiam to w uwadze *3.2. Art. 2 ust. 3. Uwaga 2. Znaczenie słowa „zasady" w komentowanym przepisie*.

Dostosowanie aktów prawnych mających zastosowanie do przetwarzania danych osobowych, o jakim jest mowa w pierwszym zdaniu przepisu ma miejsce zgodnie z art. 98 RODO. Artykuł 98 RODO nakłada na Komisję Europejską obowiązek przedkładania w stosownych przypadkach wniosków ustawodawczych związanych z ochroną danych

2. Art. 2 ust. 3. Analiza

Ze słów wytłuszczonych w przepisie: „**Do przetwarzania danych osobowych** przez instytucje, organy i jednostki organizacyjne Unii **zastosowanie ma rozporządzenie (WE) nr 45/2001**. (…)", wynika, że do przetwarzania danych osobowych opisanego w przepisie ma zastosowanie rozporządzenie (WE) nr 45/2001. Tym samym przepis komentowany wskazuje że przetwarzanie danych osobowych opisane w nim regulowane jest przez wskazany akt prawny.

Ze słów wytłuszczonych w przepisie: „Do **przetwarzania** danych osobowych **przez** (…)" wynika, że przepis dotyczy przetwarzania danych osobowych przez podmioty wskazane w przepisie.

Ze słów wytłuszczonych w przepisie: „Do przetwarzania danych osobowych **przez instytucje, organy i jednostki organizacyjne Unii** (…)" wynika, że podmioty o których mowa w przepisie i do przetwarzania danych osobowych przez które przepis się odnosi to instytucje, organy i jednostki organizacyjne Unii. Niestety przepis jest źle napi-

sany w wersji angielskiej i źle przetłumaczony na język polski. Odnoszę się do tego w uwadze *3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora „i" oraz przecinka* i w postulacie *6.1 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego*.

Użycie w przepisie: „Do przetwarzania danych osobowych przez instytucje, organy **i** jednostki organizacyjne Unii (…)" przecinka między słowem *instytucje* a słowem *organy* oraz użycie słowa *i* pomiędzy słowem *organy* a słowem *jednostki organizacyjne* prowadzi do wniosków, które przedstawiam w uwadze *3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora „i" oraz przecinka*. Tu prezentuję interpretację celowościową, nieco poprawioną wobec językowej. Wskazane w przepisie rozporządzenie ma zastosowanie do przetwarzania danych osobowych:

- jedynie przez instytucje UE lub
- jedynie przez organy UE lub
- jedynie przez jednostki organizacyjne UE lub
- przez organy UE i jednocześnie przez jednostki organizacyjne UE lub
- przez instytucje UE i jednocześnie przez organy UE i jednocześnie przez jednostki organizacyjne UE.

Ze słów wytłuszczonych w przepisie: „(…) **Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do** zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98." wynika, że Rozporządzenie (WE) nr 45/2001 oraz inne akty prawne wydane przez organy UE, które to akty prawne mają zastosowanie do przetwarzania danych osobowych przez podmioty wskazane w przepisie, zostają zmienione a dokładniej, dostosowane.

Ze słów wytłuszczonych w przepisie: „(…) zostają **dostosowane do zasad i przepisów niniejszego rozporządzenia** zgodnie z art. 98." wynika, że wskazane akty prawne zostają dostosowane do zasad i przepisów RODO. Przepis nie jest, w omawianym zakresie, najszczęśliwiej skonstruowany. Przepisy RODO to po prostu przepisy RODO – jest to truizm, ale zasady RODO to również przepisy RODO.

Szerzej omawiam to w uwadze *3.2. Art. 2 ust. 3. Uwaga 2. Znaczenie słowa „zasady" w komentowanym przepisie*. Tu jako wniosek z rozważań prowadzonych we wskazanej Uwadze, wskazuję jedynie, że akty prawne o których mowa w przepisie zostają dostosowane do przepisów RODO w tym do zasad z art. 5 RODO.

Ze słów wytłuszczonych w przepisie: „(…) zostają **dostosowane** do zasad i przepisów niniejszego rozporządzenia **zgodnie z art. 98**." wynika, że dostosowanie, o którym mowa w przepisie, czyli dostosowanie aktów prawnych mających zastosowanie do przetwarzania danych osobowych, o jakim jest mowa w pierwszym zdaniu przepisu ma miejsce zgodnie z art. 98 RODO. Artykuł 98 RODO nakłada na Komisję Europejską obowiązek przedkładania w stosownych przypadkach wniosków ustawodawczych związanych z ochroną danych osobowych.

3. Art. 2 ust. 3. Uwagi

3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora *i* oraz przecinka

Z następującego fragmentu przepisu „Do przetwarzania danych osobowych przez instytucje, organy **i** jednostki organizacyjne Unii (…)" interpretowanego językowo wynika że przepis ma zastosowanie, o czym piszę wyżej w analizie *2. Art. 2 ust. 3. Analiza* do przetwarzania danych osobowych:

- jedynie przez instytucje UE lub
- przez organy UE i jednocześnie przez jednostki organizacyjne UE lub
- przez instytucje UE i jednocześnie przez organy UE i jednocześnie przez jednostki organizacyjne UE.

Taka konstrukcja przepisu jest błędna prowadzi bowiem do wniosku, że przetwarzanie o którym mowa w przepisie nie obejmuje przetwarzania jedynie przez organy UE ani nie dotyczy przetwarzania jedynie przez jednostki organizacyjne UE, co jest oczywistym błędem. Błąd taki należy odrzucić. w niniejszej analizie odrzucam go w drodze interpretacji, niżej w postulatach *6.1 Art. 2 ust. 3. Postulat 1. Zamiana funktora „i" na funktor „lub"* i *6.1 Art. 2 ust. 3. Postulat 2. Usunięcie błędu logicznego po usunięciu błędu translatorskiego*, przedstawiam postulaty nowelizacyjne. Konstrukcja przepisu, połączenie organów

UE z jednostkami organizacyjnymi UE, powoduje, że przetwarzanie regulowane rozporządzeniem (WE) nr 45/2001 to przetwarzanie jedynie w sytuacjach tu opisanych. (Pomijam w dalszym wywodzie przetwarzanie jedynie przez instytucje UE, ponieważ nie budzi ono moich wątpliwości.).

Przetwarzanie wskazane w przepisie to zatem przetwarzanie przez organy UE i jednocześnie przez jednostki organizacyjne UE. Prowadzi to do wniosku, że jeżeli dane są przetwarzane jednocześnie (może wspólnie) przez organy UE i przez jednostki organizacyjne UE, to przetwarzania takiego dotyczy rozporządzenie (WE) nr 45/2001. Jeżeli jednak dane są przetwarzane wyłącznie przez organy UE albo wyłącznie przez jednostki organizacyjne UE, to przetwarzania takiego nie dotyczy rozporządzenie (WE) nr 45/2001. Trudno znaleźć racjonalne wyjaśnienie dla takiej regulacji. Niestety wersja polskojęzyczna jest powtórzeniem wersji anglojęzycznej, więc pomocy przez odwołanie się do wersji anglojęzycznej nie można się tu spodziewać. Jest gorzej, wersja polskojęzyczna i wersja anglojęzyczna są odmienne, o czym dalej w postulacie *6.2 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego*.

Należy pamiętać, że przepis dotyczy uprawnień osób, których dane dotyczą. Niezrozumiałe jest dlaczego inaczej miałyby się owe uprawnienia kształtować przy jednoczesnym przetwarzaniu przez organy UE i przez jednostki organizacyjne UE a inaczej miałyby się owe uprawnienia kształtować przy osobnym przetwarzaniu przez organy UE i przez jednostki organizacyjne UE. Jest to niezrozumiałe, absurdalne, bezsensowne a po prawdzie zawstydzające dla prawnika czytającego ten przepis. Mogę sobie wyobrazić, że przetwarzanie jednoczesne przez podmioty należące do dwóch kategorii jest przez prawodawcę traktowane inaczej niż przetwarzanie przez podmioty należące do jednej kategorii. Mogę sobie to wyobrazić, nie zamiaruję jednak tego poglądu uzasadniać, uważam bowiem, że jest to pogląd horrendalny, który prawdę mówiąc prezentuję tu tylko roboczo, jako coś co należy odrzucić i o czym należy zapomnieć.

W związku z powyższym uważam, że należy zaproponować interpretację, zgodnie z którą przetwarzanie czy to przez podmioty należące do jednej kategorii czy to przez podmioty należące do dwóch kategorii należy traktować jednako. W związku z odrzuceniem błędnej, choć językowej interpretacji przepisu należy stwierdzić, że wska-

zane w przepisie rozporządzenie ma zastosowanie do przetwarzania danych osobowych:
- jedynie przez instytucje UE lub
- jedynie przez organy UE lub
- jedynie przez jednostki organizacyjne UE lub
- przez organy UE i jednocześnie przez jednostki organizacyjne UE lub
- przez instytucje UE i jednocześnie przez organy UE i jednocześnie przez jednostki organizacyjne UE.

3.2. Art. 2 ust. 3. Uwaga 2.
Znaczenie słowa *zasady* w komentowanym przepisie

Omawiany przepis w części stanowi: *akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia*. Jak widać, w przepisie jest mowa o „zasadach RODO" i o „przepisach RODO".

Łatwo ustalić czym są przepisy RODO, są to po prostu kolejne, wszystkie, przepisy tego aktu prawnego. Oczywiście nie sposób dostosować innych aktów prawnych, na które wskazuje komentowany przepis, do wszystkich przepisów RODO, na przykład do przepisów określających zakresy RODO, czy do przepisów stanowiących o kompetencjach organu ochrony danych. Tym niemniej da się wskazane akty prawne dostosować do przepisów RODO, przynajmniej do niektórych przepisów RODO.

Pewien problem może sprawić ustalenie tego, czym są „zasady RODO. Rozdział II RODO nosi tytuł „Zasady". Tytuł ten nadany jest niewątpliwie na wyrost, w rozdziale tym mowa jest bowiem o zasadach, w artykule 5 RODO i o innych kwestiach, nie mających już raczej rangi zasad. Piszę „raczej", bowiem kolejne przepisy Rozdziału II RODO odnoszą się głównie, o ile nie jedynie, do zasady zgodności z prawem, doprecyzowując ją. Artykuł 5 RODO nosi tytuł: „Zasady dotyczące przetwarzania danych osobowych". W tym właśnie przepisie wskazane (i częściowo zdefiniowane) są zasady. Należy zatem zadać sobie pytanie, czy słowa *zasad (...) niniejszego rozporządzenia* odnoszą się do zasad z Rozdziału II RODO, zasad z art. 5 RODO czy do jakichś innych jeszcze, nie do końca wskazanych przez prawodawcę, zasad RODO. Zasady z Rozdziału II RODO, poza zasadami z art., 5 RODO, są trudno uchwytne. Jeśli chodzi o zasady RODO znajdu-

jące się być może poza Rozdziałem II RODO a zwłaszcza poza art. 5 RODO, to również trudno je wskazać. Najłatwiejsze do wskazania, ponieważ wskazane przez prawodawcę, są zasady z art. 5 RODO. Są to zasady w znaczeniu dyrektywalnym[111]. Możliwe jest zapewne wyinterpretowanie z RODO jakichś jeszcze zasad, poza zasadami z art. 5 RODO. Te wyinterpretowane zasady byłyby to zasady – postulaty[112]. Nie czynię tego, uważam bowiem, że wobec jedenastu zasad z art. 5 RODO, szukanie jakichś jeszcze zasad jest niepotrzebne. Jednocześnie dla potrzeb realizacji obowiązków, wynikających z niniejszego przepisu, szukanie zasad poza art. 5 RODO jest pozbawione sensu. Pozbawione sensu ponieważ przepisy, o których mowa, zostają dostosowane do *zasad (...) niniejszego rozporządzenia*, skoro zaś nie wiadomo by było o jakie zasady chodzi, to zrealizowanie obowiązku dostosowania byłoby niemożliwe. Z opisanych względów wynika, że zasady, o których tu mowa, to zasady z art. 5 RODO, ewentualnie doprecyzowane przepisami Rozdziału II RODO.

Oczywiście tak sformułowany przepis wymaga nie tylko uwagi komentatora, ale i bacznej uwagi prawodawcy, owocującej nowelizacją, której projekt wskazuję w postulacie *6.4 Art. 2 ust. 3. Postulat 4. Uporządkowanie przepisu*.

4. Art. 2 ust. 3. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Art. 2 ust. 3. RODO pozornie nie nakłada na ADO żadnych konkretnych obowiązków (dlaczego „pozornie", o tym niżej). Z punktu widzenia Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, komentowany przepis jedynie informuje, że jeżeli dane osobowe są przetwarzane przez podmioty wymienione w przepisie, to do takiego przetwarzania podmioty te mają obowiązek stosować rozporządzenie (WE) nr 45/2001 (Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobo-

[111] K. Opałek, J. Wróblewski, Zagadnienia teorii prawa, Warszawa 1969, s. 92-96.

[112] K. Opałek, J. Wróblewski, *loc. cit.*

wych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych). Podmioty te, to (zależnie od wersji językowej): instytucje UE, organy UE, urzędy UE, agencje UE, jednostki organizacyjne UE. *6.2 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego*.

Piszę wyżej, że art. 2 ust. 3 RODO nie nakłada pozornie na administratoora żadnych obowiązków. Uważam, że jest tak jedynie pozornie, bowiem komentowany przepis jednak na niektóre kategorie administratorów pewne obowiązki nakłada. Piszęo tym niżej.

- Art. 2 ust. 3 RODO nakłada na podmioty wymienione w przepisie, (zależnie od wersji językowej): instytucje UE, organy UE, urzędy UE, agencje UE, jednostki organizacyjne UE. *6.2 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego*, obowiązek stosowania rozporządzenia (WE) nr 45/2001, do przetwarzania danych osobowych przez te podmioty.
- Jednocześnie art. 2 ust. 3 RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba której dane dotyczą ma prawo oczekiwać, że jeżeli dane osobowe przetwarzane są przez podmioty wymienione w przepisie, (zależnie od wersji językowej): instytucje UE, organy UE, urzędy UE, agencje UE, jednostki organizacyjne UE. *6.2 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego* to podmioty te do przetwarzania danych osobowych stosować będą rozporządzenie (WE) nr 45/2001

5. Art. 2 ust. 3. Konkretyzacja zasady I

Artykuł 2 ust. 3 RODO nie konkretyzuje zasad z art. 5 RODO. Można jednak wskazać na pewne związki między art. 2 ust. 3 RODO a zasadami z art. 5 RODO.

Po pierwsze, art. 2 ust. 3 RODO wskazuje, że znaczna cześć aktów przetwarzania danych osobowych, mająca miejsce na terenie UE jest regulowana przez inny niż RODO akt prawny. Przetwarzanie danych osobowych, w zakresie opisanym w komentowanym przepisie, w oparciu o rozporządzenie (WE) nr 45/2001, to przetwarzanie, które z punktu widzenia RODO jest na pierwszy rzut oka **zgodne z prawem**, czyli realizuje zasadę zgodności z prawem, zapisaną w art. 5 ust. 1 lit. a RODO. Na pierwszy rzut oka, ponieważ zgodność z pra-

wem takiego przetwarzania powinna być oceniana nie na podstawie RODO a właśnie na podstawie rozporządzenia (WE) nr 45/2001, który to akt prawny zawiera własne przepisy szczególne dotyczące szczegółów przetwarzania danych ale i własne zasady, w tym własną zasadę zgodności z prawem, zapisana w art. 4 ust. 1 lit. a rozporządzenia (WE) nr 45/2001

6. Art. 2 ust. 3. Postulaty de lege ferenda

6.1 Art. 2 ust. 3. Postulat 1.
Zamiana funktora *i* na funktor „lub".

Przepis w pewnym zakresie stanowi: *(...) przez instytucje, organy i jednostki organizacyjne Unii (...)*. W uwadze *3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora „i" oraz przecinka* opisane jest, że użycie w cytowanej cześci przepisu funktora „i" prowadzi na manowce wykładni prawa. W zwiazku z tym należy przepis poprawić.

W związku z powyższym postuluję aby cytowany fragment przepisu brzmiał: „(...) przez instytucje, organy ~~i~~ **lub** jednostki organizacyjne Unii (…)". (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Cytowany fragment przepisu po nowelizacji miałby postać:
„„(...) przez instytucje, organy lub jednostki organizacyjne Unii (…)"

Analogiczny błąd znajdujemy w wersji angielskiej przepisu: *offices and agencies*, nie stawiam jednak postulatu nowelizacyjnego wobec wersji angielskiej, przekracza to bowiem założenia niniejszej pracy. Wersja polska i wersja angielska są odmienne, na niekorzyść polskiej, postuluję zatem niżej ich ujednolicenie poprzez usuniecie błędu translatorskiego a następnie poprawienie poprzez usuniecie błędu logicznego.

6.2 Art. 2 ust. 3. Postulat 2.
Usunięcie błędu translatorskiego

Pierwsze zdanie przepisu, w wersji polskiej, brzmi: „Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001."

Pierwsze zdanie przepisu, w wersji angielskiej, brzmi: *For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies.*

W wersji polskiej widnieją zatem *instytucje, organy i jednostki organizacyjne Unii*.

W wersji angielskiej widnieją *Union institutions, bodies, offices and agencies*.

Wydaje się, że *institutions* to *instytucje*, wydaje się, że „*bodies*" to *organy*, dalej jednak tłumaczenie staje się zaskakujące. *offices and agencies* przetłmaczono na *jednostki organizacyjne*. Można przyjąć, że *offices* to *urzędy* (rozumiane jako biurokratyczne aparaty obsługi organów), zaś *agencies* to *agencje* (rozumiane jako coś zewnętrznego, takiego jak placówka, oddział, filia. „Agency" to też „biuro", ale znaczenie „biura" ma też po części „urząd" dlatego też uważam użycie słowa „agency" a właściwie *agencies* za najdokładniej oddające istotę.

W związku z powyższym postuluję aby cytowany fragment przepisu brzmiał: „Do przetwarzania danych osobowych przez instytucje, organy, **urzędy** i ~~jednostki organizacyjne~~ **agencje** Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)". (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Cytowany fragment przepisu po nowelizacji miałby postać:
„Do przetwarzania danych osobowych przez instytucje, organy, urzędy i agencje Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)".

Analiza kilku wersji językowych pozwala mi na wniosek cokolwiek dziwaczny, niestety na inny nie pozwala. Otóż w zakresie komentowanego przepisu, RODO ma dwie wersje. Co najmniej dwie, porównywałem bowiem wersje: polską, angielską, czeską, chorwacką i niemiecką. Wersje, w której występują cztery kategorie podmiotów związanych z UE i wersję, w której występują trzy kategorie podmiotów związanych z UE. Wersja czeska przepisu stanowi: *Na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie se vztahuje nařízení (ES) č. 45/2001. Nařízení (ES) č. 45/2001 a další právní akty Unie týkající se takového zpracování osobních údajů jsou uzpůsobeny zásadám a pravidlům tohoto nařízení podle článku 98*. Jest ona bliższa wersji polskiej niż angielskiej, nie analizuję jej tu detalicznie, zwracam jedynie uwagę, że w wersji tej występują 3 kategorie podmiotów, co wnioskujemy ze słów: *orgány, institucemi a jinými subjekty*. Z kolei w wersji chorwackiej znajdujemy cztery kate-

gorie podmiotów: *institucije, tijela, uredi i agencije Unije*. Wersja niemiecka zawiera cztery kategorie podmiotów, co wynika ze słów: *die Organe, Einrichtungen, Ämter und Agenturen der Union*. Widać, że tłumaczenie szło co najmniej dwiema ścieżkami, ale wersję chorwacką, przynajmniej w zakresie komentowanego przepisu, ktoś sprawdził i ujednolicił z wersją angielską, wersja polska i czeska pozostały w wersji surowej tłumaczenia – bez redakcji.

6.3 Art. 2 ust. 3. Postulat 3.
Usunięcie błędu logicznego po usunięciu błędu translatorskiego

Pierwsze zdanie przepisu, w wersji polskiej, brzmi: *Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001*.

Po usunięciu błędy translatorskiego, w wposób zaproponowany w postulacie *6.1 Art. 2 ust. 3. Postulat 2. Usunięcie błędu translatorskiego*, fragment przepisu, którego poprawienie postuluję w niniejszym postulacie ma postać: *Do przetwarzania danych osobowych przez instytucje, organy, urzędy i agencje Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (...)*. Przepis w zaprezentowanej wersji prowadzi do wniosku, że rozporządzenie (WE) nr 45/2001 ma zastosowanie do przetwarzania danych osobowych:
- jedynie przez instytucje UE albo
- jedynie przez organy UE albo
- przez urzędy UE i jednocześnie przez agencje UE.

Interpretacja taka, mimo, że jezykowo poprawna, jest nie do zaakceptowania. Na drodze wykładni odzrzucam ją (na gruncie niepoprawionej translatorsko wersji polskojęzycznej przepisu) w uwadze *3.1. Art. 2 ust. 3. Uwaga 1. Niewłaściwe użycie funktora „i" oraz przecinka*. Tu proponuję poprawienie przepisu, stawiajac postulat jego nowelizacji.

W związku z powyższym postuluję aby cytowany fragment przepisu brzmiał: „Do przetwarzania danych osobowych przez instytucje, organy, urzędy ~~i~~ **lub** agencje Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)". (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane. Z uwagi na możliwość złego odczytania moich intencji, z tej racji, że

przekreślone „ł” może być wzięte za nieprzekreślone „i”, wskazuję, że usuwam literę: „i” i dodaję słowo: „lub”.)

Cytowany fragment przepisu po nowelizacji miałby postać: „Do przetwarzania danych osobowych przez instytucje, organy, urzędy lub agencje Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)”.

6.3 Art. 2 ust. 3. Postulat 4. Poprawienie treści przepisu

Powyżej zastanawiam się jak poprawić treść komentowanego przepisu, jednak czynię to w pewnych ramach. Ramami tymi są zasady wykładni prawa (o których twórcy przepisu zdaje się, że zapomnieli), ramamy tymi są różne wersje jezykowe przepisu. Poza te ramy, powyżej, nie wychodzę. Wydaje się, że poza te ramy wyjść należy. Przepis komentowany odsyła do rozporządzenia (WE) nr 45/2001 (Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych). Konstrukcja komentowanego przepisu jest taka, że jeżeli wymienione w przepisie podmioty przetwarzają dane osobowe, to do tego przetwarzania należy stosować rozporządzenie (WE) nr 45/2001. Jednocześnie rozporządzenia (WE) nr 45/2001 ma swój zakres podmiotowy. Wydaje się, że skoro komentowany przepis odsyła do rozporządzenia (WE) nr 45/2001, wtedy kiedy pewne, wymienione w przepisie podmioty przetwarzają dane osobowe, to dobrze by było, gdyby przepis komentowany wskazywał na przetwarzanie danych osobowych przez podmioty, znajdujące się w zakresie podmiotowym rozporządzenia (WE) nr 45/2001.

Można sobie oczywiście wyobrazić, że zakres podmiotów wskazanych w przepisie komentowanym jest **węższy** od zakresu podmiotów wskazanego w zakresie podmiotowym rozporządzenia (WE) nr 45/2001, wtedy nie ma to to daleko idących skutków. Można sobie też oczywiście wyobrazić, że zakres podmiotów wskazanych w przepisie komentowanym jest **szerszy** od zakresu podmiotów wskazanego w zakresie podmiotowym rozporządzenia (WE) nr 45/2001 albo wskazuje podmioty inne niż w zakresie podmiotowym rozporządzenia

(WE) nr 45/2001, wtedy RODO rozszerza zakres podmiotowy rozporządzenia (WE) nr 45/2001.

Artykuł 3 ust. 1 Rozporządzenia (WE) nr 45/2001 stanowi: „Niniejsze rozporządzenie stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu.". Czyli jak widać przepis ten wskazuje na przetwarzanie danych osobowych przez *wszystkie instytucje i organy wspólnotowe* (*by all Community institutions and bodies* w wersji angielskiej). Wydaje się, że z uwagi na konieczność spójności prawa, jak również po prostu dlatego, by niepotrzebne były rozważania prowadzone przeze mnie w uwagach i postulatach do omawianego przepisu RODO, dobrze by było, gdyby przepis ten wskazywał na przetwarzanie danych osobowych właśnie *przez wszystkie instytucje i organy wspólnotowe*.

W związku z powyższym postuluję aby cytowany fragment przepisu brzmiał: „Do przetwarzania danych osobowych przez instytucje lub organy ~~i jednostki organizacyjne~~ Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)". (Czcionką przekreśloną zaznaczam słowa usunięte.)

Cytowany fragment przepisu po nowelizacji miałby postać:

„Do przetwarzania danych osobowych przez instytucje lub organy Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. (…)".

6.5 Art. 2 ust. 3. Postulat 5.
Uporządkowanie przepisu

Pierwsze zdanie przepisu, w wersji polskiej, brzmi: „Do przetwarzania danych osobowych

Przepis w pewnym zakresie stanowi: *(...) Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98*. W uwadze *3.2. Art. 2 ust. 3. Uwaga 2. Znaczenie słowa „zasady" w komentowanym przepisie* analizuję zakres słowa „zasady" użytego w przepisie komentowanym. Rozważania prowadzą do malo odkrywczego wniosku, że zasady to zasady, a dokładniej, do wniosku, że zasady, o których mowa w przepisie omawianym to zasady z art. 5 RODO. Dla uniknięcia takich rozważań, jak również dla rozjaśnie-

nia przepisu należy go znowelizować. Uważam, że racjonalne jest pozostawienie w przepisie słów o zasadach, jednak o zasadach traktowanych dyrektywalnie, o konkretnych zasadac z art. 5 RODO.

W związku z powyższym postuluję aby cytowany fragment przepisu brzmiał: „(...) Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do ~~zasad i p~~przepisów niniejszego rozporządzenia**, w tym do zasad z art. 5**, zgodnie z art. 98. (…)". (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Cytowany fragment przepisu po nowelizacji miałby postać: „(...) Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do przepisów niniejszego rozporządzenia**, w tym do zasad z art. 5**, zgodnie z art. 98.".

Rozdział trzeci

Artykuł 3 RODO

Artykuł 3 RODO

Terytorialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Terytorialny zakres stosowania

Artykuł 3 ust. 1 RODO.

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

1. Art. 3 ust. 1. Komentarz

Przepis określa na jakim terytorium stosowane jest RODO.

Przepis określa również zakres podmiotowy RODO.

Z analizy słów samego tylko tytułu wynika, że art. 3 RODO wskazuje, na jakim terenie RODO znajduje zastosowanie.

Przepis precyzuje zakres przedmiotowy RODO.

Zakres przedmiotowy RODO regulowany w art. 3 ust. 1 RODO, odwołuje się, do przetwarzania danych osobowych. RODO stosuje się do przetwarzania danych osobowych w sposób opisany w przepisie.

Zakres RODO określony w przepisie uzależniony jest od pewnych warunków, w jakich zachodzi przetwarzanie danych osobowych. Zakres RODO określony w przepisie uzależniony jest od warunków jakie spełnia działalność prowadzona przez podmioty wskazane w przepisie.

Pierwszym z warunków jakie musi spełnić przetwarzanie, by miało do niego zastosowanie RODO, jest by dane były przetwarzane przez jednostkę organizacyjną administratora, lub by dane były przetwarzane przez jednostkę organizacyjną podmiotu przetwarzającego lub by dane były przetwarzane przez jednostkę organizacyjną administratora i przez jednostkę organizacyjną podmiotu przetwarzającego, czyli tylko przez administratora, tylko przez podmiot przetwarzający, przez administratora i podmiot przetwarzający.

Drugim z warunków jakie musi spełnić przetwarzanie, by miało do niego zastosowanie RODO, jest by dane były przetwarzane w związku z działalnością prowadzoną w UE. Niestety nie wiadomo jak szeroko należy to rozumieć, kiedy dane są przetwarzane w związku z działalnością (prowadzoną w UE) a kiedy nie. Omawiam to niżej.

RODO ma zastosowanie jeżeli działalność jest prowadzona przez administratora lub przez podmiot przetwarzający lub przez administratora i przez podmiot przetwarzający. Należy zwrócić uwagę, że wskazane słowa art. 3 ust. 1 RODO, interpretowane oczywiście łącznie z definicją administratora znajdującą się w art. 4 pkt 7 RODO i z definicją podmiotu przetwarzającego, znajdującą się w art. 4 pkt 8 RODO, statuują zakres podmiotowy RODO.

Dla stosowalności RODO, nieistotne jest czy przetwarzanie odbywa się na terenie UE czy poza terenem UE. Co może być źródłem pewnych problemów, zwłaszcza w przypadku przetwarzania odbywającego się poza terenem UE, o czym mowa niżej w uwagach *3. Art. 3 ust. 1. Uwagi I - 3.1. Art. 3 ust. 1. Uwaga 1. Wątpliwa konieczność rozszerzenia zakresu terytorialnego RODO poza UE. 3.3.* i *Art. 3 ust. 1. Uwaga 3. Propozycja skróconego zapisu opisu relacji na gruncie RODO*.

2. Art. 3 ust. 1. Analiza

Słowa: „**Terytorialny zakres stosowania**" stanowią tytuł art. 3 RODO. Z analizy słów samego tylko tytułu wynika, że art. 3 RODO wskazuje, na jakim terenie RODO znajduje zastosowanie. Z analizy treści przepisu, prowadzonej niżej, wynika, że przepis dotyczy nie samego tylko terytorialnego zakresu stosowania, ale też zakresu przedmiotowego RODO. Przepis precyzuje zakres przedmiotowy RODO w sytuacjach, kiedy zachodzi przetwarzanie z elementem przetwarzania poza UE i kiedy zachodzi przetwarzanie bez tego elementu, czyli jedynie na terenie UE, czyli przepis po prostu statuuje zakres przedmiotowy RODO, szerzej w uwadze *3.2. Art. 3 ust. 1. Uwaga 2. Szczegóły zakresu terytorialnego RODO*.

Ze słów: „**Niniejsze rozporządzenie ma zastosowanie do** (...)" wynika, że przepis statuuje zakres przedmiotowy RODO. Art. 3 ust. 1 RODO, podobnie jak art. 2 ust. 1 RODO statuuje zakres przedmiotowy RODO w sposób pozytywny – wskazując jakie czynności objęte są zakresem RODO.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie **ma zastosowanie do przetwarzania danych osobowych** (...)" wynika, że zakres przedmiotowy RODO regulowany w art. 3 RODO, odwołuje się, podobnie jak zakres przedmiotowy, regulowany w art. 2 RODO, do

przetwarzania danych osobowych. RODO stosuje się do przetwarzania danych osobowych w sposób opisany w przepisie.

Ze słów: „(...) **do przetwarzania danych osobowych w związku z** (...)" wynika, że zakres RODO określony w przepisie uzależniony jest od pewnych warunków, w jakich zachodzi przetwarzanie danych osobowych.

Ze słów: „(...) **w związku z działalnością prowadzoną przez** (...)" wynika, że zakres RODO określony w przepisie uzależniony jest od warunków jakie spełnia działalność prowadzona przez podmioty wskazane w przepisie.

Ze słów: „(...) **w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego** (...)" wynika, że pierwszym z warunków jakie musi spełnić przetwarzanie, by miało do niego zastosowanie RODO, jest by dane były przetwarzane przez jednostkę organizacyjną administratora, lub by dane były przetwarzane przez jednostkę organizacyjną podmiotu przetwarzającego lub by dane były przetwarzane przez jednostkę organizacyjną administratora i przez jednostkę organizacyjną podmiotu przetwarzającego.

Użycie funktora „(...) **lub** (...)" skutkuje tym, że dane może przetwarzać tylko administrator, tylko podmiot przetwarzający albo administrator i podmiot przetwarzający.

Ze słów: „(...) w związku z działalnością prowadzoną (...) w Unii (...)" wynika, że drugim z warunków jakie musi spełnić przetwarzanie, by miało do niego zastosowanie RODO, jest by dane były przetwarzane w związku z działalnością prowadzoną w UE. Słowa *w Unii* powinny znajdować się w innym miejscu przepisu, szerzej w uwagach, 3.2. Art. 3 ust. 1. Uwaga *2. Szczegóły zakresu terytorialnego RODO*.

Niestety nie wiadomo jak szeroko należy rozumieć słowa: *przetwarzania danych osobowych w **związku z działalnością***. Kiedy dane są przetwarzane w związku z działalnością (prowadzoną w UE przez jednostkę organizacyjną administratora lub PP) a kiedy nie. Rozstrzygnięcie tego dylematu jest kluczowe. Jeżeli dane przetwarzane są w związku z działalnością prowadzoną w UE to RODO

ma zastosowanie do ich przetwarzania, jeżeli dane są przetwarzane bez związku z działalnością w UE, to RODO nie ma zastosowania do ich przetwarzania. Analizując zagadnienie, kiedy przetwarzanie ma miejsce w związku z działalnością, napotykamy na pewien problem. Rozpatrzenie różnicy miedzy „w związku z działalnością" a „bez związku z działalnością" w teorii wydaje się być proste.

Jeżeli przetwarzanie bez działalności administratora lub podmiotu przetwarzającego nie miało by miejsca, to znaczy, że zachodzi ono w związku z działalnością (jednostki organizacyjnej) administratora lub podmiotu przetwarzającego. Wyrażona w poprzednim zdaniu myśl wydaje się przecinać rozważania. Sytuacja wygląda tak optymistycznie tylko jeżeli rozpatrujemy ją w teorii. Przełożenie sytuacji na konkretny przykład już tak optymistycznie nie nastraja. Ze względu na zakres rozważań prowadzę je niżej w uwagach, uwaga *3.2. Art. 3 ust. 1. Uwaga 2. Szczegóły zakresu terytorialnego RODO*.

Ze słów: „(...) **działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego** (...)" wynika, że RODO ma zastosowanie jeżeli działalność jest prowadzona przez administratora lub przez podmiot przetwarzający lub przez administratora i przez podmiot przetwarzający. Należy zwrócić uwagę, że wskazane słowa art. 3 ust. 1 RODO, interpretowane oczywiście łącznie z definicją administratora znajdującą się w art. 4 pkt 7 RODO i z definicją podmiotu przetwarzającego, znajdującą się w art. 4 pkt 8 RODO, statuują zakres podmiotowy RODO. Z tego względu dobrze by było by tytuł przepisu oddawał jego treść, o czym szerzej piszę w uwagach.

Ze słów: „(...) **niezależnie od tego, czy przetwarzanie odbywa się w Unii.**" wynika, że dla stosowalności RODO, nieistotne jest czy przetwarzanie odbywa się na terenie UE czy poza terenem UE. Co może być źródłem pewnych problemów, zwłaszcza w przypadku przetwarzania odbywającego się poza terenem UE, o czym mowa niżej w uwagach, *3.1. Art. 3 ust. 1. Uwaga 1. Wątpliwa konieczność rozszerzenia zakresu terytorialnego RODO poza UE. 3.3.* i *Art. 3 ust. 1. Uwaga 3. Propozycja skróconego zapisu opisu relacji na gruncie RODO*.

3. Art. 3 ust. 1. Uwagi
3.1. Art. 3 ust. 1. Uwaga 1.
Wątpliwa konieczność rozszerzenia zakresu terytorialnego RODO poza UE

Artykuł 3 RODO, statuujący zakres przedmiotowy RODO, ale w ujęciu terytorialnym, stanowi m.in., że RODO dotyczy przetwarzania „(...) **niezależnie od tego, czy przetwarzanie odbywa się w Unii** (...)". Dla porządku trzeba pamiętać, że art. 3 RODO jest jednym z trzech przepisów, które niejako na raty statuują zakres przedmiotowy RODO, czyli każde przetwarzanie danych osobowych, zanim zostaną wobec niego zastosowane przepisy szczególne RODO musi przejść przez test znajdowania się w zakresie RODO, czyli owo przetwarzanie musi spełnić jednocześnie warunki wynikające z art. 1 RODO i z art. 2 RODO i z art. 3 RODO. Pamiętając o powyższym, wracamy do rozważań nad tym, że RODO dotyczy przetwarzania niezależnie od tego czy owo przetwarzanie odbywa się w UE. RODO dotyczy zatem przetwarzania danych na terenie UE i poza tym terenem jeżeli tylko przetwarzanie odbywa się w związku z prowadzoną na terenie UE działalnością jednostki organizacyjnej podmiotu – administratora lub podmiotu przetwarzającego.

RODO ma zatem zastosowanie do przetwarzania jeżeli:
- przetwarzanie jest prowadzone w związku z działalnością którą
- jednostka organizacyjna administratora lub jednostka organizacyjna podmiotu przetwarzającego
- prowadzi na terenie UE
- niezależnie od tego czy przetwarzanie odbywa się na terenie UE czy poza terenem UE.

Jeżeli popatrzymy na RODO w sposób idealistyczny, to rozszerzenie zakresu RODO na całą kulę ziemską ma wiele uroku. Urok ten polega na tym, że RODO chroni prawa osób, których dane dotyczą, również poza UE.

Kiedy popatrzymy w sposób bardziej krytyczny, to dostrzegamy UE i resztę świata, resztę świata, która do UE nie należy. I tej reszcie świata UE oznajmia w RODO, że jeśli przetwarzanie danych osobowych, które się w tej reszcie świata odbywa, odbywa się w związku z działalnością prowadzoną w UE (cokolwiek to znaczy, ale o tym dalej), to RODO ma zastosowanie do tego przetwarzania. Po

pierwsze jest to po prostu wkraczanie w suwerenność prawną państw spoza UE. Można uważać, że RODO jest genialne, konieczne i że w ogóle jest to niezwykły akt prawny (wiele postulatów w niniejszej książce podważa taki pogląd, ale możliwy on jest) ale skoro państwo nie należy do UE to dlaczego miałoby zwracać na swoim terytorium uwagę na prawo UE. Poza tym państwo spoza UE może mieć własne regulacje sprzeczne z RODO. Oczywiste jest, że przetwarzanie danych na terenie państwa spoza UE musi być zgodne z prawem tego państwa, ale dlaczego ma być zgodne z RODO?

Kiedy wreszcie popatrzymy w sposób praktyczny to dostrzegamy, że jeśli chodzi o zastosowanie RODO do przetwarzania danych poza terenem UE, to zgodność przetwarzania z RODO może być trudna do wyegzekwowania.

3.2. Art. 3 ust. 1. Uwaga 2. Szczegóły zakresu terytorialnego RODO

Dla zakresu przedmiotowego RODO istotna jest treść art. 3 ust. 1 RODO. Przepis ten stanowi: *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii*. Dla ułatwienia rozważań przepis ten należy nieco uporządkować. Możliwie najmniejsza ingerencja w przepis, która go nieco jednak uczytelnia skutkuje następującą jego redakcją: „RODO ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną w Unii przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego, niezależnie od tego, czy przetwarzanie odbywa się w Unii.”.

Żeby dalsze wywody jeszcze bardziej uprościć można próbować utożsamić jednostkę organizacyjną administratora z administratorem i jednostkę organizacyjną podmiotu przetwarzającego z podmiotem przetwarzającym. Przepis można uprościć więc do formy: „RODO ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną w Unii przez administratora lub podmiot przetwarzający, niezależnie od tego, czy przetwarzanie odbywa się w Unii.”. Uproszczenie takie idzie jednak za daleko, trzeba bowiem pamiętać, że administrator może mieć siedzibę poza UE i jednocześnie przetwarzać dane osobowe w UE, podobnie podmiot

przetwarzający może mieć siedzibę poza UE i jednocześnie przetwarzać dane osobowe w UE. Dla zakresu przedmiotowego RODO nieistotne jest zatem czy przetwarzanie odbywa się w UE czy poza UE, istotne jest za to czy przetwarzanie danych osobowych ma związek z działalnością, którą prowadzi w UE jednostka organizacyjna administratora lub podmiotu przetwarzającego.

Niżej, w kolejnych przykładach dotyczących zakresu terytorialnego RODO, dla ich uczytelnienia posługuję się skrótami, dla administratora używam skrótu: „ADO", dla podmiotu przetwarzającego używam skrótu: „PP"

Przykład 1
Przetwarzanie w UE przez jednostkę organizacyjną ADO w związku z działalnością ADO w UE – RODO ma zastosowanie, art. 3 ust. 1 RODO.

Przykład 2
Przetwarzanie poza UE przez jednostkę organizacyjną ADO w związku z działalnością ADO w UE – RODO ma zastosowanie, art. 3 ust. 1 RODO

Przykład 3
Przetwarzanie w UE przez jednostkę organizacyjną PP w związku z działalnością PP w UE – RODO ma zastosowanie, art. 3 ust. 1.

Przykład 4
Przetwarzanie poza UE przez jednostkę organizacyjną PP w związku z działalnością PP w UE – RODO ma zastosowanie, art. 3 ust. 1.

Pierwsze cztery przykłady są proste. Jeżeli jednostka organizacyjną administratora lub podmiotu przetwarzającego przetwarza dane osobowe, to oczywiste jest, że do takiego przetwarzania RODO ma zastosowanie. Wynika to z zasady a fortiori, skoro RODO ma zastosowanie do przetwarzania danych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego, to tym bardziej RODO ma zastosowanie do przetwarzania danych przez jednostkę organizacyjną administratora lub

podmiotu przetwarzającego.[113] Jednocześnie jeżeli dane osobowe są przetwarzane przez jednostkę organizacyjna administratora lub podmiotu przetwarzającego to nie ma wątpliwości, że są one przetwarzane w związku z działalnością tej właśnie jednostki organizacyjnej administratora lub podmiotu przetwarzającego, która dane przetwarza.

Kolejne przykłady to przykłady przetwarzania już nie przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego ale dokładnie tak jak przepis stanowi, w związku z działalnością takiej jednostki. Jeżeli przetwarzanie danych ma mieć miejsce nie przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego, ale przez inny podmiot, to między przetwarzaniem danych przez ten inny podmiot a działalnością administratora lub podmiotu przetwarzającego musi istnieć związek. Związek ten może mieć postać umowy powierzenia przetwarzania, ale z RODO nie wynika, by ta umowa była tu konieczna. Związek miedzy przetwarzaniem danych osobowych a działalnością administratora może mieć tez charakter faktyczny, mający postać udostępnienia danych. W takich właśnie sytuacjach mam wątpliwość, czy tak szeroki jak w przepisie zakres przedmiotowy w ujęciu terytorialnym, ma sens.

Rozważania prowadzone poniżej, prowadzone są przy założeniu, że administrator jest administratorem unijnym.

Dla potrzeb wywodu wprowadzam pojęcie ADO/odbiorca danych – jest to inny administrator niż administrator, z którego punktu widzenia prowadzone jest rozważanie, jest to administrator, któremu dane są udostępniane przez administratora, z którego punktu widzenia prowadzone jest rozważanie.

Przykład 5

(Zapis symboliczny, zastosowany w dalszych wyjaśnieniach objaśniam niżej w uwadze *3.3. Art. 3 ust. 1. Uwaga 3. Propozycja skróconego zapisu opisu relacji na gruncie RODO*).

Przetwarzanie w UE przez PP w związku z działalnością jednostki organizacyjnej administratora w UE. RODO ma zastosowanie, art. 3 ust. 1 RODO, również art. 2 ust. 1 RODO.

[113] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 219-222.

ADO powierza przetwarzanie danych podmiotowi przetwarzającemu, PP działa na terenie UE i przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej ADO w UE.
ADOue > PPue
Przykład 5a
ADOue > PPue >> PPue
Przykład 5b
ADOue > PPue : ADO2ue
Przykład 5c
ADOue > Ppue >> PP¬ue
Przykład 5c opis.

ADO A prowadzi działalność na terenie UE. ADO A powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu PPue. Podmiot przetwarzający PPue również prowadzi działalność na terenie UE. Podmiot przetwarzający PPue przekazuje dane osobowe podmiotowi poza UE, który nazywamy PP2¬ue. PP2¬ue wykonuje na zlecenie PPue czynności na danych. (Przekazanie poza UE zgodnie z Rozdziałem V RODO). Prócz tego, skoro PP2¬ue wykonuje czynności w imieniu PPue, to jest on, czyli Podmiot PP¬ue, podmiotem przetwarzającym. Zachodzi tu co prawda podpowierzenie, zaś Podmiot PP2¬ue jest PP drugiego stopnia, wiele to jednak nie zmienia. PPue podpisuje zatem umowę powierzenia przetwarzania z pP2¬ue. W opisanej sytuacji wydaje się, że przetwarzanie danych osobowych zachodzi w związku (bo w imieniu) z działalnością prowadzoną w Unii przez jednostkę organizacyjną PP (bo PPue powierzył przetwarzanie PP2¬ue). W opisanej sytuacji RODO ma więc zastosowanie do przetwarzania przez PP2¬ue.
Można wysnuć tu wniosek, że przetwarzanie danych osobowych zachodzi w związku z działalnością prowadzoną przez PP jeżeli PP powierza przetwarzanie danych osobowych PP 2 stopnia.
Przykład 5d
ADOue > PPue : ADO2¬ue

Przykład 6
Przetwarzanie w UE przez ADO/odbiorcę danych w związku z działalnością jednostki organizacyjnej ADO w UE. RODO ma zastosowanie ze względu na art. 3 ust. 1 RODO, również art. 2 ust. 1 RODO.
ADO udostępnia dane osobowe innemu ADO, czyli ADO/odbiorcy danych, ADO/odbiorca danych działa w UE i przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej ADO w UE.
ADOue : ADO2ue
Przykład 6a
ADOue : ADO2ue > PPue
Przykład 6b
ADOue : ADO2ue : ADO3ue
Przykład 6c
ADOue : ADO2ue > PP¬ue
Przykład 6d
ADOue : ADO2ue : ADO3¬ue

Przykład 7
Przetwarzanie poza UE przez PP w związku z działalnością jednostki organizacyjnej ADO w UE. RODO ma zastosowanie ze względu na art. 3 ust. 1 RODO
ADO powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu, PP działa poza UE i przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej ADO w UE.
ADOue > PP¬ue
Przykład 7a
ADOue > PP¬ue >> PP2¬ue
Przykład 7b
ADOue > PP¬ue >> ADO2¬ue
Przykład 7c
ADOue > PP¬ue >> PPue
Przykład 7d
ADOue > PP¬ue >> ADO2ue
Przykład 7d opis.
ADO A prowadzi działalność na terenie UE. ADO A przekazuje dane osobowe podmiotowi poza UE, który nazywamy PP¬ue. Podmiot poza UE wykonuje na zlecenie ADO czynności na danych. Oczywiście przekazanie poza UE powinno mieć miejsce zgodnie z Rozdziałem V RODO, jednak to tu uważam za pewnik i pomijam w wywodzie. Prócz

tego, skoro PP¬ue wykonuje czynności w imieniu ADO A to jest on, czyli PP¬ue, podmiotem przetwarzającym. ADO A podpisuje zatem umowę powierzenia przetwarzania z PP¬ue. W opisanej sytuacji wydaje się, że przetwarzanie danych osobowych zachodzi w związku (bo w imieniu) z działalnością prowadzoną w Unii przez jednostkę organizacyjną administratora (bo ADO powierzył przetwarzanie Podmiotowi B). W opisanej sytuacji RODO ma więc zastosowanie do przetwarzania przez podmiot B. Można wysnuć tu wniosek, że przetwarzanie danych osobowych zachodzi w związku z działalnością prowadzoną przez ADO jeżeli ADO powierza przetwarzanie danych osobowych.

Innymi słowy, przetwarzanie danych osobowych zachodzące w związku z działalnością prowadzoną przez ADO na terenie UE jest tożsame przetwarzaniu danych osobowych przez PP znajdujący się poza UE, któremu ADO powierzył przetwarzanie.

Przykład 8

Przetwarzanie poza UE przez ADO/odbiorcę danych w związku z działalnością jednostki organizacyjnej ADO w UE – RODO ma zastosowanie ze względu na art. 3 ust. 1 RODO.

ADO udostępnia dane osobowe innemu ADO, czyli aDO/odbiorcy danych, ADO/odbiorca danych działa poza terenem UE i przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej ADO w UE. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO.

Tu mam pewne wątpliwości. Jeżeli ADO udostępnia dane osobowe innemu ADO, nazwanemu tu ADO/odbiorcą, to nie bez powodu ten ADO/odbiorca nie jest PP. Ma zapewne własną podstawę prawną do przetwarzania danych osobowych, albo nie ma tej podstawy, bo w jego kraju sprawa nie jest uregulowana i po prostu przetwarza dane osobowe, które otrzymał od ADO, ponieważ wolno mu to czynić. Mam wątpliwość czy ochrona danych na gruncie RODO jest tu realna.

ADOue : ADO2¬ue

Przykład 8a

ADOue : ADO2¬ue >> PP2¬ue

Przykład 8b

ADOue : ADO2¬ue : ADO3¬ue

Przykład 8c

ADOue : ADO2¬ue >> PPue

Przykład 8d

ADOue : ADO2¬ue >> ADO3ue

Przykład 9
Przetwarzanie w UE przez PP 2stopnia w związku z działalnością jednostki organizacyjnej PP w UE. RODO ma zastosowanie ze względu na art. 3 ust. 1 RODO
PP w UE powierza przetwarzanie danych osobowych PP2° w UE. PP2° w UE przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej PP w UE. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO.
PPue >> PP2ue
Przykład 9a
PPue >> PP2ue >>>PP3ue
Przykład 9b
PPue >> PP2ue : ADO2ue
Przykład 9c
PPue >> PP2ue>>> PP3¬ue
Przykład 9d
PPue >> PP2ueE : ADO2¬ue

Przykład 10
Przetwarzanie w UE przez ADO/odbiorcę w UE w związku z działalnością jednostki PP w UE.
PP w UE udostępnia w imieniu ADO dane osobowe ADO/odbiorcy. ADO/Odbiorca przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej PP w UE. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO.
PPue >> ADO2ue
Przykład 10a
PPue >> ADO2ue >>> PPue
Przykład 10b
PPue >> ADO2ue : ADO3ue
Przykład 10c
PPue >> ADO2ue >>> PP¬ue
Przykład 10d
PPue >> ADO2ue : ADO3¬ue

Przykład 11
Przetwarzanie poza UE przez PP2° w związku z działalnością jednostki PP w UE.
PP w UE powierza przetwarzanie danych osobowych w imieniu ADO podmiotowi przetwarzającemu 2°. PP2° przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej PP w UE. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO.
PPue >> PP2¬ue
Przykład 11a
PPue >> PP2¬ue >>> PP3¬ue
Przykład 11b
PPue >> PP2¬ue : ADO2¬ue
Przykład 11c
PPue >> PP2¬ue >>> PP3ue
Przykład 11d
PPue >> PP2¬ue :ADO2ue

Przykład 12
Przetwarzanie poza UE przez ADO/odbiorcę w związku z działalnością jednostki PP w UE.
PP w UE udostępnia w imieniu ADO dane osobowe ADO/odbiorcy. ADO/Odbiorca przetwarza dane osobowe w związku z działalnością jednostki organizacyjnej PP w UE. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO. RODO ma zastosowanie ze względu na art. 3 ust 1 RODO.
PPue >> ADO2¬ue
Przykład 12a
PPue >> ADO2¬ue >>> PP3¬ue
Przykład 12b
PPue >> ADO2¬ue : ADO3¬ue
Przykład 12c
PPue >> ADO2¬ue >>> PP3ue
Przykład 12d
PPue >> ADO2¬ue >>> ADO3ue

3.3. Art. 3 ust. 1. Uwaga 3.
Propozycja skróconego zapisu opisu relacji na gruncie RODO

Podczas omawiania RODO, podczas omawiania relacji powstających na gruncie RODO między administratorem, podmiotem przetwarzającym, odbiorcą, często pojawia się potrzeba szybkiego a zwłaszcza czytelnego zapisu zjawiska powierzenia, podpowierzenia, udostępnienia. Proponuję niżej opracowany przy okazji pisania niniejszej pracy, sposób zapisu, który umożliwia szybkie i czytelne (po szybkim opanowaniu) zapisanie relacji.

W RODO występuje kilka różnych podmiotów. Relacje między tymi podmiotami wymagają często opisania. Różni opisujący, opisują różnymi słowami te same relacje. Nawet ten sam opisujący może jedną relację opisać na kilka różnych sposobów, co czasem utrudnia zrozumienie istoty relacji. Drugim problemem, który się pojawia jest czas, jaki marnuje czytelnik, na zrozumienie, niejasnych czasem wywodów opisującego. By zapobiec tym zjawiskom proponuję stosowanie zapisu symbolicznego. Zapis ten zainspirowany jest zapisem logicznym i wykorzystuje niektóre używane w zapisie logicznym symbole. Dopuszczam, że relacje z dziedziny danych osobowych są możliwe do opisania z użyciem symboli logicznych, jednak w nieco okrężny sposób. Celem, który przyświecał mi przy opracowywaniu zapisu skróconego było uproszczenie zapisu relacji, dzięki któremu relacje można zapisywać i odczytywać w sposób szybki i sprawny. Zapis jest możliwy w każdym języku, symbole są językowo neutralne. Skróty nazw podmiotów nie są językowo neutralne. Posługuję się skrótami nazw polskich.

ADO – administrator danych (osobowych)
ADO1 – administrator danych (osobowych), czyli to samo co ADO, ale w relacjach, kiedy występuje kilku ADO.
ADO2 – administrator danych (osobowych), któremu ADO udostępnia dane osobowe.
ADO3 – administrator danych (osobowych), któremu ADO2 udostępnia dane osobowe
PP – podmiot przetwarzający
PP1 – podmiot przetwarzający pierwszego stopnia, czyli to samo co PP, zapis używany do opisu relacji, w których występuje kilka PP

PP2 – podmiot przetwarzający drugiego stopnia, czyli podmiot przetwarzający, któremu powierza przetwarzanie danych podmiot przetwarzający pierwszego stopnia
PP3 – podmiot przetwarzający trzeciego stopnia, czyli podmiot przetwarzający, któremu powierza przetwarzanie danych podmiot przetwarzający drugiego stopnia
W przypadku długich łańcuchów powierzenia, po literach „PP" dodaje się liczbę oznaczającą stopień podmiotu przetwarzającego.
PP1(X1) – podmiot, który otrzymał od ADO zgodę na powierzenie wybranemu przez siebie podmiotowi, jednak bez możliwości dalszego powierzenia
PP1(X2) – podmiot, który otrzymał od ADO zgodę na powierzenie wybranemu przez siebie podmiotowi, z możliwością dalszego, ale tylko jednokrotnego podpowierzenia
W przypadku długich łańcuchów możliwego podpowierzenia, po literach „PP" dodaje się liczbę oznaczającą najwyższy stopień akceptowanego przez administratora.
W przypadku długich łańcuchów możliwego podpowierzenia, po literach „PP" dodaje się symbol" XX", oznaczający, że administrator akceptuje każdy stopień podpowierzenia.

> - symbol powierzenia przetwarzania danych
ADO > PP co czytamy: administrator danych (osobowych) powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu

>> - symbol podpowierzenia przetwarzania danych
PP >> PP2 co czytamy: podmiot przetwarzający powierza (podpowierza) przetwarzanie danych osobowych podmiotowi przetwarzającemu (drugiego stopnia)

: - symbol udostępnienia danych osobowych
ADO1:ADO2 co czytamy: administrator danych udostępnia dane osobowe innemu administratorowi danych

4. Art. 3 ust. 1. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- art. **Art. 3 ust. 1.** RODO **nakłada na administratora obowiązek** stosowania RODO jeżeli zachodzą pewne, opisane w przepisie warunki.

Administrator ma zatem obowiązek stosować RODO:

-- jeżeli przetwarza dane osobowe w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora w Unii
-- i niezależnie od tego, czy przetwarzanie odbywa się w Unii
lub
-- jeżeli przetwarza dane osobowe w związku z działalnością prowadzoną przez jednostkę organizacyjną podmiotu przetwarzającego w Unii
i
-- niezależnie od tego, czy przetwarzanie odbywa się w Unii

- jednocześnie art. **Art. 3 ust. 1.** RODO **ustanawia uprawnienie**, które przysługuje każdej osobie której dotyczą dane osobowe. Uprawnienie polega na tym że osoba, której dotyczą dane osobowe ma prawo oczekiwać, że administrator stosuje RODO wobec dotyczących jej danych osobowych jeżeli zachodzą pewne, opisane w przepisie warunki.

Osoba, której dane dotyczą ma zatem prawo oczekiwać, że administrator stosuje RODO:

-- jeżeli przetwarza dane osobowe w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora w Unii
-- i niezależnie od tego, czy przetwarzanie odbywa się w Unii
lub
-- jeżeli przetwarza dane osobowe w związku z działalnością prowadzoną przez jednostkę organizacyjną podmiotu przetwarzającego w Unii
i
-- i niezależnie od tego, czy przetwarzanie odbywa się w Unii

5. Art. 3 ust. 1. Konkretyzacja zasady

Artykuł 3 ust.1 RODO nie konkretyzuje zasad z art. 5 RODO. Można jednak wskazać na pewne związki miedzy art. 3 ust. 1 RODO a zasadami z art. 5 RODO.

Po pierwsze, art. 3 ust. 1 RODO warunkuje stosowanie zasad z art. 5 RODO. Jeżeli przetwarzanie danych osobowych nie spełnia warunków opisanych w art. 3 ust. 1 RODO to RODO, w danej sytuacji, nie skutkuje obowiązkami po stronie osób przetwarzających dane ani uprawnieniami po stronie osób, których dane dotyczą.

Po drugie, jeżeli przetwarzanie danych osobowych spełnia warunki opisane w art. 3 ust. 1 RODO to przepis ten, podobnie jak art. 1 RODO i jak art. 2 RODO, uznać należy za przepis kierunkujący interpretację przepisów RODO, w tym kierunkujący interpretację art. 5 RODO.

6. Art. 3 ust. 1. Postulaty de lege ferenda

6.1 Art. 3 ust. 1. Postulat 1. Zawężenie zakresu RODO

Z uwagi na zaprezentowane w uwadze *3.1. Art. 3 ust. 1. Uwaga 1. Wątpliwa konieczność rozszerzenia zakresu terytorialnego RODO poza UE*, rozumowania, uważam, że lepiej by było gdyby prawodawca nie próbował rozciągać działania RODO na świat cały. Słowa: *niezależnie od tego, czy przetwarzanie odbywa się w Unii* powinny zostać z przepisu usunięte.

Z tego punktu widzenia art. 3 ust 1 RODO powinien mieć postać: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii".

6.2 Art. 3 ust. 1. Postulat 2. Uporządkowanie przepisu

Przepis stanowi: *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego* ***w Unii,*** *niezależnie od tego, czy przetwarzanie odbywa się w Unii.*. Słowa *w Unii* znajdują się gdzie się znajdują

i właśnie ich miejsce w przepisie może skutkować złym rozumieniem przepisu. Nieuważny interpretator może uznać, że słowa *w Unii* odnoszą się do *administratora* i do *podmiotu przetwarzającego*, tworząc tym samym złożenia: „administratora w Unii" i „podmiotu przetwarzającego w Unii". Trudno orzec co oznacza „administrator w UE" lub „podmiot przetwarzający w UE" czy mowa tu o administratorze lub podmiocie przetwarzającym z siedzibą w UE, czy o coś, kogoś innego. Nie wiadomo, jednak obecna forma przepisu do rozważań takich niestety jednak uprawnia. By tego uniknąć słowa *w Unii* powinny zostać przeniesione, tak by przepis miał formę: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną w **Unii** przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego, niezależnie od tego, czy przetwarzanie odbywa się w Unii."

6.3 Art. 3 ust. 1. Postulat 1+2 =3. Zawężenie zakresu RODO i uporządkowanie przepisu

Połączenie wniosków wynikających z postulatu *6.1 Art. 3 ust. 1. Postulat 1. Zawężenie zakresu RODO* i z postulatu *6.2 Art. 3 ust. 1. Postulat 2. Uporządkowanie przepisu*, prowadzi do wniosku, że przepis powinien brzmieć: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w **związku z działalnością prowadzoną** w **Unii** przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego". Słowa: *niezależnie od tego, czy przetwarzanie odbywa się w Unii* zostają usunięte, a słowa *w Unii* przeniesione.

6.3 Art. 3 ust. 1. Postulat 4. Zmiana tytułu przepisu

Art. 3 ust. 1 stanowi: *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z* ***działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego*** *w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.* Czyli, jak widać, z przepisu tego wynika m.in. czyja działalność znajduje się w zakresie RODO. W zakresie RODO, jak zatem widać, znajduje się działalność jednostki organizacyjnej administratora i jednostki organizacyjnej podmiotu przetwarzającego. Definicja ADO znajduje się w art. 4 pkt 7 RODO zaś definicja PP znajduje się w art. 4 pkt 8 RODO. Uprawnione jest zatem

stwierdzenie, że art. 3 RODO statuuje nie tylko zakres terytorialny RODO, ale również zakres przedmiotowy RODO. Jak napisałem w analizie, P*rzepis precyzuje zakres przedmiotowy RODO w sytuacjach, kiedy zachodzi przetwarzanie z elementem przetwarzania poza UE i kiedy zachodzi przetwarzanie bez tego elementu, czyli jedynie na terenie UE, czyli przepis po prostu statuuje zakres przedmiotowy RODO.*W związku z tym tytuł przepisu nie powinien brzmieć tak jak obecnie, zaś w tytule powinna być oddana treść przepisu. Tytuł powinien brzmieć: „Zakres przedmiotowy. Zakres terytorialny.”.

Artykuł 3 ust. 2 RODO.

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

1. Art. 3 ust. 2. Komentarz

Przepis statuuje zakres przedmiotowy RODO, przepis podobnie jak art. 2 ust. 1 RODO i jak art. 3 ust. 1 RODO statuuje zakres przedmiotowy RODO w sposób pozytywny – wskazując jakie czynności objęte są zakresem RODO.

Zakres przedmiotowy RODO regulowany w art. 3 ust. 2 RODO, odwołuje się, podobnie jak zakres przedmiotowy, regulowany w art. 2 RODO i w art. 3 ust. 1 RODO, do przetwarzania danych osobowych. RODO stosuje się do przetwarzania danych osobowych w sposób opisany w przepisie.

RODO dotyczy przetwarzania danych osobowych osób, które przebywają na terenie Unii Europejskiej, oczywiście przy jednoczesnym zrealizowaniu pozostałych warunków zawartych w przepisie.

RODO ma zastosowanie jeżeli dane są przetwarzane przez administratora danych niemającego jednostki organizacyjnej na terenie Unii Europejskiej lub przez podmiot przetwarzający niemający jednostki organizacyjnej na terenie Unii Europejskiej.

Przetwarzanie aby obejmowało je RODO musi być prowadzone przez administratora danych albo przez podmiot przetwarzający albo przez administratora danych i przez podmiot przetwarzający.

Poza warunkami zawartymi w pierwszej części przepisu, przetwarzanie musi spełniać dodatkowe jeszcze warunki by mieściło się w zakresie przedmiotowym, nazywanym tu terytorialnym.
Dodatkowe warunki, o których piszę, to cechy jakie musi spełniać przetwarzanie danych.

Dodatkowym warunkiem, od którego, na gruncie przepisu uzależnione jest czy RODO dotyczy danego przetwarzania danych jest to czy przetwarzanie wiąże się z oferowaniem osobom, których dane dotyczą, towarów lub usług. Nieistotne dla spełnienia warunku jest czy oferowane usługi lub towary są oferowane odpłatnie czy nieodpłatnie. Konstrukcja przepisu każe sądzić, że towary lub usługi, o których mowa, oferowane są przez administratora danych lub przez podmiot przetwarzający, dokładna analiza przepisu, nie potwierdza jednak tego sądu, usługi (przynajmniej na gruncie językowo rozumianego przepisu) nie musi świadczyć administrator ani podmiot przetwarzający. Piszę o tym w uwadze *3.1. Art. 3 ust. 2. Uwaga 1. Zakres RODO a świadczenie usług przez podmiot pozaunijny*.

Drugim dodatkowym warunkiem, od którego, na gruncie przepisu uzależnione jest czy RODO dotyczy danego przetwarzania danych jest to, czy przetwarzanie wiąże się z monitorowaniem zachowania osób, których dane dotyczą przy spełnieniu dodatkowego warunku, że zachowanie monitorowane ma miejsce na terenie Unii Europejskiej.

Przetwarzanie, aby obejmowało je RODO musi spełniać warunek z art. 3 ust. 2 lit. a RODO, albo z art. 3 ust. 2 lit. b RODO albo z art. 3 ust. 2 lit. a RODO, albo z art. 3 ust. 2 lit. b RODO.

2. Art. 3 ust. 2. Analiza

Ze słów: „**Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych** (…)" wynika, że przepis statuuje zakres przedmiotowy RODO. Artykuł 3 ust. 2 RODO, podobnie jak art. 2 ust. 1 RODO i jak art. 3 ust. 1 RODO statuuje zakres przedmiotowy RODO w sposób pozytywny – wskazując jakie czynności objęte są zakresem RODO.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie ma zastosowanie **do przetwarzania danych osobowych** (…)" wynika, że zakres przedmiotowy RODO regulowany w art. 3 ust. 2 RODO, odwołuje

się, podobnie jak zakres przedmiotowy, regulowany w art. 2 RODO i w art. 3 ust. 1 RODO, do przetwarzania danych osobowych.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie ma zastosowanie **do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii** (…)" wynika, że RODO dotyczy przetwarzania danych osobowych osób, które przebywają na terenie Unii Europejskiej, oczywiście przy jednoczesnym zrealizowaniu pozostałych warunków zawartych w przepisie.

Ze słów wytłuszczonych: „Niniejsze rozporządzenie ma zastosowanie **do przetwarzania** danych osobowych osób, których dane dotyczą, przebywających w Unii **przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii**, (…)" wynika, że RODO ma zastosowanie jeżeli dane są przetwarzane przez administratora danych niemającego jednostki organizacyjnej na terenie Unii Europejskiej lub przez podmiot przetwarzający niemający jednostki organizacyjnej na terenie Unii Europejskiej.

Użycie wytłuszczonego funktora „lub" w przepisie: „(…) Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora **lub** podmiot przetwarzający niemających jednostek organizacyjnych w Unii, (…)" skutkuje tym, że przetwarzanie aby obejmowało je RODO musi być prowadzone przez administratora danych albo przez podmiot przetwarzający albo przez administratora danych i przez podmiot przetwarzający.

Ze słów: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych (…) **jeżeli** (…)" wynika, że poza warunkami zawartymi w pierwszej części przepisu, przetwarzanie musi spełniać dodatkowe jeszcze warunki by mieściło się w zakresie przedmiotowym, nazywanym tu terytorialnym.

Ze słów: „(…) **jeżeli czynności przetwarzania wiążą się z:** (…)" wynika, że dodatkowe warunki, o których piszę, to cechy jakie musi spełniać przetwarzanie danych.

Ze słów: „(…) **jeżeli czynności przetwarzania wiążą się z:**

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; (…)" wynika, że dodatkowym warunkiem, od którego, na gruncie przepisu uzależnione jest czy RODO dotyczy danego przetwarzania danych jest to czy przetwarzanie wiąże się z oferowaniem osobom, których dane dotyczą, towarów lub usług. Nieistotne dla spełnienia warunku jest czy oferowane usługi lub towary są oferowane odpłatnie czy nieodpłatnie. Konstrukcja przepisu każe sądzić, że towary lub usługi, o których mowa, oferowane są przez administratora danych lub przez podmiot przetwarzający, dokładna analiza przepisu, nie potwierdza jednak tego sądu, usługi (przynajmniej na gruncie językowo jedynie rozumianego przepisu) nie musi świadczyć administrator ani nie musi jej świadczyć podmiot przetwarzający. Piszę o tym w uwadze *3.1. Art. 3 ust. 2. Uwaga 1. Zakres RODO a świadczenie usług przez podmiot pozaunijny*.

Ze słów: „(…) **jeżeli czynności przetwarzania wiążą się z:** (…)
b) **monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii**." wynika, że drugim dodatkowym warunkiem, od którego, na gruncie przepisu uzależnione jest czy RODO dotyczy danego przetwarzania danych jest to, czy przetwarzanie wiąże się z monitorowaniem zachowania osób, których dane dotyczą przy spełnieniu dodatkowego warunku, że zachowanie monitorowane ma miejsce na terenie Unii Europejskiej.

Użycie wytłuszczonego funktora „lub" w przepisie: „(…)
a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; **lub**
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii." skutkuje tym, że przetwarzanie aby obejmowało je RODO musi spełniać warunek z art. 3 ust. 2 lit. a RODO, albo z art. 3 ust. 2 lit. b RODO albo z art. 3 ust. 2 lit. a RODO, albo z art. 3 ust. 2 lit. b RODO.

3. Art. 3 ust. 2. Uwagi
3.1. Art. 3 ust. 2. Uwaga 1.
Zakres RODO a świadczenie usług przez podmiot pozaunijny

Z części wstępnej przepisu wynika, że RODO ma zastosowanie jeżeli dane osobowe są przetwarzane przez administratora lub przez podmiot przetwarzający. Dalej z przepisu wynika, że administrator danych lub podmiot przetwarzający nie ma jednostki organizacyjnej w UE. W skrócie zatem można uznać, że RODO ma zastosowanie do przetwarzania danych przez pozaunijnego administratora lub przez pozaunijny podmiot przetwarzający.

Dalej przepis zawiera dwa warunki, spełnienie któregokolwiek z nich, przy jednoczesnym spełnieniu warunku, że administrator (danych) lub podmiot przetwarzający nie ma jednostki organizacyjnej w UE, skutkuje stosowaniem RODO do przetwarzania, które te warunki spełnia.

Pierwszy warunek stanowi, że przetwarzanie musi być związane z oferowaniem towarów lub usług osobom, których dane osobowe dotyczą. I tu pojawia się problem. Mianowicie nie wiadomo o czyje towary lub usługi chodzi w przepisie. (Drugiego warunku nie poddaję analizie, bo nie dostrzegam, by mógł on być źródłem analogicznych problemów jak pierwszy).

W analizie *2. Art. 3 ust. 2. Analiza* napisałem, że *Konstrukcja przepisu każe sądzić, że towary lub usługi, o których mowa, oferowane są przez administratora (danych) lub przez podmiot przetwarzający (...)*. Napisałem tak ponieważ, co opisałem we wskazanym miejscu, w przepisie jest mowa o przetwarzaniu danych osobowych przez administratora lub przez podmiot przetwarzający. I tu właśnie pojawia się, skryty głęboko problem, a mianowicie w przepisie mowa jest o przetwarzaniu danych osobowych przez administratora lub przez podmiot przetwarzający jednak tylko właśnie w odniesieniu do przetwarzania danych wskazano przez kogo dane te przetwarzane być mają. Przepis nie wskazuje kto ma oferować towary lub usługi osobom, których dane dotyczą. Skoro przepis tego nie wskazuje, to towary lub usługi, o których mowa w przepisie może oferować administrator danych, może oferować podmiot przetwarzający, ale może je też oferować osoba trzecia. Osoba trzecia będąca administratorem

danych, innym, autonomicznym wobec wymienionych w przepisie administratora i podmiotu przetwarzającego.

Może się zatem zdarzyć, że:
- towary lub usługi oferowane są osobom, których dane dotyczą
  i
- towary lub usługi oferowane są przez kogoś innego niż administrator danych, lub podmiot przetwarzający, wymienieni w przepisie
  i
- osoby, których dane dotyczą przebywają na terenie UE i
- dane osobowe przetwarzane są przez administratora danych lub przez podmiot przetwarzający niemających jednostek organizacyjnych w na terenie Unii Europejskiej.

Stan faktyczny wydaje się tu karkołomny, jednak niekoniecznie taki musi być. Wystarczy wyobrazić sobie, że na terenie Unii Europejskiej funkcjonuje biuro, biuro to nie zbiera danych osób, które do niego przychodzą, jednak udostępnia komputer. Osoby, które przychodzą do biura logują się do interfejsu internetowego przedsiębiorstwa spoza UE. Podają swoje dane, jednak, co podkreślam, nie unijnemu przedsiębiorstwu ale przedsiębiorstwu pozaunijnemu. W opisanej sytuacji przetwarzanie danych objęte jest zakresem RODO. Opisany stan faktyczny może wydawać się karkołomny, jest jednak prawdziwy. Jeśli chodzi o opisywany stan faktyczny, to można sobie wyobrazić uzasadnienie dla tego, że przetwarzanie danych osobowych przez podmiot nieunijny znajduje się w zakresie RODO. Podmiot pozaunijny współpracuje z unijnym, unijny prowadzi reklamę usług podmiotu pozaunijnego.

Oczywiście weryfikacja tego czy pozaunijny podmiot przestrzega RODO może nie być łatwa na przykład dla PUODO, o ile nie niemożliwa, to jednak zupełnie inna sprawa. Inna sprawa a mianowicie namysł nad tym, czy tak szeroki zakres przedmiotowo-terytorialny RODO ma sens.

4. Art. Art. 3 ust. 2. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- art. **Art. 3 ust. 2.** RODO nakłada na ADO obowiązek stosowania RODO jeżeli zachodzą pewne, opisane w przepisie warunki.

Administrator ma zatem obowiązek stosować RODO:

-- jeżeli administrator (danych) nie ma jednostki organizacyjnej na terenie UE
-- i jeżeli przetwarza dane osobowe osób których dane dotyczą
-- i osoby te przebywają w na terenie UE
-- i czynności przetwarzania danych osobowych wiążą się z
--- oferowaniem towarów lub usług osobom, których dane dotyczą
---- i od osób, których dane dotyczą wymaga się zapłaty
albo
---- od osób, których dane dotyczą nie wymaga się zapłaty
-- lub czynności przetwarzania danych osobowych wiążą się z
--- monitorowaniem zachowania osób których dane dotyczą
--- i monitorowanie zachowania osób których dane dotyczą zachodzi na terenie UE.

I

- art. **Art. 3 ust. 2.** RODO nakłada na podmiot przetwarzający obowiązek stosowania RODO jeżeli zachodzą pewne, opisane w przepisie warunki.

Podmiot przetwarzający ma zatem obowiązek stosować RODO :

-- jeżeli podmiot przetwarzający nie ma jednostki organizacyjnej na terenie UE
-- i jeżeli przetwarza dane osobowe osób których dane dotyczą
-- i osoby te przebywają w na terenie UE
-- i czynności przetwarzania danych osobowych wiążą się z
--- oferowaniem towarów lub usług osobom, których dane dotyczą
---- i od osób, których dane dotyczą wymaga się zapłaty
albo
---- od osób, których dane dotyczą nie wymaga się zapłaty
-- lub czynności przetwarzania danych osobowych wiążą się z
--- monitorowaniem zachowania osób których dane dotyczą
--- i monitorowaniem zachowania osób których dane dotyczą zachodzi na terenie UE.

5. Art. 3 ust. 2. Konkretyzacja zasady I

Artykuł 3 ust. 2 RODO nie konkretyzuje zasad z art. 5 RODO. Można jednak wskazać na pewne związki miedzy art. 3 ust. 2 RODO a zasadami z art. 5 RODO.

Po pierwsze, art. 3 ust. 2 RODO warunkuje stosowanie zasad z art. 5 RODO. Jeżeli przetwarzanie danych osobowych nie spełnia warunków opisanych w art. 3 ust. 2 RODO to RODO, w danej sytuacji, nie skutkuje obowiązkami po stronie osób przetwarzających dane ani uprawnieniami po stronie osób, których dane dotyczą.

Po drugie, jeżeli przetwarzanie danych osobowych spełnia warunki opisane w art. 3 ust. 2 RODO to przepis ten, podobnie jak art. 1 RODO i jak art. 2 RODO, uznać należy za przepis kierunkujący interpretację przepisów RODO, w tym kierunkujący interpretację art. 5 RODO.

Rozdział czwarty

Artykuł 4 RODO

Artykuł 4 RODO

Na użytek niniejszego rozporządzenia:

W RODO znajduje się znaczna ilość definicji legalnych. Rację ma P. Fajgielski, który twierdzi, że *(...) prawodawca posługuje się wieloma definicjami legalnymi, których znaczenie odbiega niekiedy od potocznego ich rozumienia*[114]. Przed powyższym cytowanym zdaniem, P. Fajgielski pisze[115] o konieczności wyjaśnienia terminologii. Czyni to, takie bowiem jest. m.in. założenie jego książki, ja za cel postawiłem sobie nie tylko objaśnienie terminologii, ale również jej krytykę i przedstawienie postulatów nowelizacyjnych. Czynię to niżej w niniejszym rozdziale.

Tekst niniejszego rozdziału podzielony jest na podrozdziały – warstwy.

Warstwa 1 (komentarz) to komentarz do odpowiedniego przepisu RODO. Komentarz ten ma charakter bardzo skrótowy. Polecam jego lekturę osobom, które pragną ogólnie zapoznać się z kolejnymi przepisami, którym jednak jednocześnie nie wystarcza lektura samych tylko przepisów.

Warstwa 2 (analiza) to drobiazgowa analiza odpowiedniego przepisu RODO. Analiza ta ma m. in. Na celu dokładne poznanie treści analizowanego przepisu, oraz, w miarę możliwości pewne, ustalenie zakresu uprawnień i obowiązków jakie z przepisu wynikają. Polecam lekturę podrozdziałów tej warstwy osobom, które dokonują własnej analizy przepisów, nie są jednak pewne jej wyników. Lekturę podrozdziałów tej warstwy polecam też osobom, które wiedze swoją opierają nie tyle na analizie przepisów ile na lekturze literatury fachowej i na lekturze rozmaitych dokumentów oficjalnych i pseudooficjalnych. Osoby idące ta drogą mogą mieć problemy z niespójnością wiedzy płynącej z różnych źródeł. Mam nadzieję, że drobiazgowa analiza przepisu może pomóc im w wyrobieniu sobie zdania kto, w kolejnych sporach ma rację, tym bardziej, że w podrozdziałach tej warstwy ograniczam na ile potrafię, zajmowanie stanowiska w sprawach wynikających z przepisów. Staram się by prowadzona analiza była możliwie „przezroczysta", by rozważania prowadzone były w oparciu o zasady

[114] P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu,* Warszawa 2019, s. 17.

[115] P. Fajgielski, *loc. cit.*

wykładni i by wnioski z rozważań miały charakter wniosków płynących od rozważań, a nie pseudowniosków apriorycznych, przez pryzmat których rozważania mogłyby być prowadzone, jednak zaburzyłoby to ich obiektywizm. Wnioski, do których dochodzę w podrozdziałach tej warstwy są umieszczone w podrozdziałach warstwy 1 (komentarz.).

Warstwa 3 (uwagi) zawiera klasyczny wywód prawniczy. Umieszczam tam wszystko co chcę powiedzieć na temat kolejnych przepisów i w związku z nimi, co jednak wychodzi poza zakres samej tylko czystej analizy przepisów. W podrozdziałach tej warstwy prowadzę pogłębione rozważania, które odwołują się do ustaleń poczynionych w podrozdziałach warstwy 2. Jeżeli rozważania prowadzą do postulatów nowelizacyjnych, to jedynie sygnalizuję tam możliwość ich postawienia a postulaty stawiam w podrozdziałach warstwy 6 (postulaty de lege ferenda). Lekturę podrozdziałów warstwy 3 polecam wszystkim osobom zainteresowanym pogłębieniem swojej wiedzy na temat spraw, których dotyczą przepisy, do których się w danej warstwie odnoszę.

Rozważania te mogą być wartościowe dla praktyków ochrony danych, dla sędziów, dla pracowników PUODO, śmiem również sądzić, że mogą się okazać interesujące dla osób zajmujących się RODO czy też szerzej pojętą ochroną danych w sposób naukowy czy też nawet jedynie problemowy. Niektóre podrozdziały warstwy 3 mogą, przez wnikliwych badaczy, zostać rozbudowane do osobnych monografii czy chociaż artykułów naukowych, są bowiem czasem takimi właśnie zjawiskami, tyle, że sprowadzonymi do skali podrozdziału w monografii. Zachęcam ewentualnych Czytelników, do takich operacji, mogą one bowiem przynieść pożytek tak naukowy jak i praktyczny. Jednocześnie, mimo ograniczonego wymiarami publikacji, wymiaru kolejnych podrozdziałów, staram się by zawierały one czy to wnioski czy to gotowe rozwiązania, tak by czytający te podrozdziały naukowiec mógł poznać moje zdanie w opisywanych tam kwestiach a czytający te podrozdziały praktyk mógł znaleźć w tych podrozdziałach odpowiedzi na nurtujące go pytania.

Warstwa 4 (podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa). Zamieszczone są w tej warstwie krótkie podsumowania analizowanych przepisów, przeprowadzone na gruncie Konceptualizmu Prawniczego. Teoria ta (moja własna) pozwala na sprowadzenie każdego przepisu do obowiązków i uprawnień

(praw). To właśnie przy kolejnych przepisach czynię. Wskazuję w podrozdziałach tej warstwy jakie to obowiązki i jakie to uprawnienia z danego, analizowanego przepisu wynikają. Lektura rozważań zamieszczonych w tej warstwie może być kształcąca dla osób, które mają problem ze zrozumieniem, że, jakkolwiek dziwnie to brzmi, prawo jest. „Jest" w znaczeniu ontologicznym, jest czyli istnieje, istnieje, więc wywołuje skutki. Możemy się z tym prawem nie zgadzać, postulować jego zmianę, ba – zdarza się, że je łamiemy, nie możemy jednak udawać, że go nie ma.

Warstwa 5 (konkretyzacja zasad). Jak sam tytuł wskazuje, rozważania prowadzone w tej kategorii podrozdziałów mają za zadanie wskazać w jaki sposób konkretyzowane są kolejne zasady z art. 5 ust. 1 RODO.

Warstwa 6 (postulaty de lege ferenda). W warstwie tej umieszczone są kolejne postulaty nowelizacyjne, które stawiam po drobiazgowym przeanalizowaniu kolejnych przepisów.

Lektura podrozdziałów tej warstwy może być kształcąca dla ewentualnych legislatorów. Nie wierzę, by legislatorzy zwracali uwagę na głos nauki, gdyby zwracali to RODO nie byłoby takie jakie jest a ja nie mógłbym stawiać postulatów nowelizacyjnych, bo nie byłoby ku temu racjonalnych powodów. Nie wierzę, jednak mam nadzieję. Mam nadzieję, że kiedyś legislatorzy, politycy, władze – sięgną po wiedzę i doświadczenie, które są dostępne. Dostępne na uczelniach, dostępne też wśród pozauczelnianych ekspertów. Sięgną po wiedzę która jest, jest w sensie ontologicznym, która istnieje. Sięgną po wiedzę, miast starać się zdobywać wiedzę swoistym wstępnym bojem – już podczas tworzenia prawa i zarządzania państwem.

Lektura podrozdziałów tej warstwy może być też, jak mniemam, użyteczna dla praktyków, zwłaszcza na etapie sporów sądowych. Możliwe jest wyprowadzenie, w odniesieniu do niektórych analizowanych przepisów, tezy, że nie sposób jest ich stosować, póki nie zostaną znowelizowane, że są napisane błędnie, ponieważ nauka proponuje ich nowelizacje i stawia gotowe postulaty nowelizacyjne. Wreszcie – że nie można ukarać administratora za niedostosowanie się do przepisu, który jest tak źle napisany, że wymaga poprawienia.

Warstwa 7 (rozważania historyczne). Zamieszczam tam krótkie uwagi, poczynione w oparciu o nieobowiązujące już przepisy, jeżeli uważam, że uwagi te mogą być wartościowe dla dzisiejszej wiedzy i dzisiejszego Czytelnika.

Artykuł 4 pkt 1 RODO

„dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

1. Art. 4 pkt 1. Komentarz

Dane osobowe to wszelkie informacje o osobie fizycznej zidentyfikowanej, lub o osobie fizycznej możliwej do zidentyfikowania.

Innymi słowy:

dane osobowe to informacje o osobie fizycznej, którą można wskazać lub o osobie fizycznej, którą można odróżnić od innych osób fizycznych lub o osobie wskazanej lub o osobie odróżnionej od innych osób fizycznych.

Przepis statuuje znaczenie pojęcia „dane osobowe", pojęcie „dane osobowe" należy rozumieć tak jak zdefiniowano w tym przepisie[116].

2. Art. 4 pkt 1. Analiza[117]

Ze słów wytłuszczonych w cytacie: „oznaczają **wszelkie informacje** (...)" wnioskujemy, że każda informacja może być daną osobową.

---

[116] M. Zirk-Sadowski, *Problemy wykładni językowej w prawie administracyjnym.* w: *System Prawa Administracyjnego tom IV. Wykładnia w prawie administracyjnym,* Red: R Hauser, Z Niewiadomski, A. Wróbel, Warszawa 2012, s. 199.

[117] Zawartość warstwy *Analiza* została wykorzystana i w znacznej mierze zacytowana w publikacji: J. Rzymowski, *op. cit.* s. 15-20.

(...) charakter osobowy nie może zostać z góry przypisany żadnej kategorii danych[118] – to zdanie oddaje istotę zagadnienia. Nie ma informacji, która zawsze jest daną osobową. Informacja to po prostu informacja, daną osobową jest o ile spełnia warunki z komentowanej definicji.

Ciekawe jest stanowisko P. Litwińskiego, P. Barty i M Kaweckiego, że: *Nie jest (...) z góry możliwe ustalenie katalogu, nawet o charakterze otwartym, informacji, które mogą zostać uznane za mające charakter danych osobowych*[119]. Prawdą jest, że nie jest możliwe ustalenie, że te a te informacje są danymi osobowymi, a te a te informacje nie są danymi osobowymi,[120] jednak zwracam uwagę na fakt, że (w zasadzie) każda informacja może być daną osobową.[121]

Daną osobową może być imię, nazwisko, numer buta, czy tonaż posiadanego statku albo wagomiar ulubionej haubicy. Stanowisko P. Litwińskiego, P. Barty i M. Kaweckiego jest ciekawe i prawie się z nim zgadzam. Prawdą jest, że nie można ustalić katalogu informacji, które są danymi osobowymi, jednak jeśli chodzi o informacje *które mogą zostać uznane za mające charakter danych osobowych*, to katalog takich informacji ustalić można dość łatwo – są to wszystkie informacje które można komukolwiek przypisać. Co ciekawe takie właśnie stanowisko wyrażają ci sami autorzy, tyle, że dwie strony dalej w swoim Komentarzu, piszą w nim bowiem: *Każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu widzenia pojęcia danych osobowych i każda informacja może zostać uznana za informacje o charakterze osobowym*[122] – z tym poglądem się zgadzam. Podobny pogląd prezentuje w Komentarzu D. Lubasz.[123]

---

[118] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 172. Zdanie to wyrasta z myśli A. Mednisa, a cytuję je tu za wskazanym Komentarzem.

[119] P. Litwiński, P. Barta, M. Kawecki, *loc. cit.*

[120] Podobnie: M. Sakowska-Baryła w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 72.

[121] Podobnie, nieważne, że w poprzednim stanie prawnym: L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 29

[122] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 174.

[123] D. Lubasz w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czer-

Ze słowa „o" wytłuszczonego w cytacie: „(...) oznaczają informacje **o** zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") (...)" wnioskujemy, że dane osobowe to informacje dotyczące które dotyczą osoby fizycznej. W polskiej wersji językowej widnieje *o (...) osobie fizycznej*. Nie wydaje się to najszczęśliwszym tłumaczeniem angielskiej wersji językowej. W wersji angielskiej widnieje: *information relating to (...) identifiable natural person*. Na poziomie tłumaczenia odbywa się tu pewne przekłamanie i to przekłamanie nie tylko językowe ale znaczeniowe. Informacje, które są *relating to* to informacje odnoszące się do osoby fizycznej. Informacje, które są **o** osobie fizycznej, to informacje te osobę opisujące. Informacja, która się do kogoś odnosi a informacja, która kogoś opisuje, to jednak dwie różne kategorie informacji. Informacje, które kogoś opisują, zawsze się do tej osoby odnoszą, jednak informacje, które się do kogoś odnoszą nie zawsze tę osobę opisują.

Ze słów wytłuszczonych w cytacie: „(...) oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania **osobie fizycznej** („osobie, której dane dotyczą") (...)" wnioskujemy, że dane osobowe to informacje dotyczące żywych ludzi.[124] Możliwe są szersze rozważania dotyczące definicji osoby fizycznej, w tym jednak miejscu nie wydają się one konieczne, ponieważ motyw 27 Preambuły RODO stanowi: *Niniejsze rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych*. W Polsce takimi przepisami są np. przepisy dotyczące ochrony informacji o pacjencie po śmierci pacjenta, przepisy dotyczące tajemnic medycznych itp.[125]

Ze słów wytłuszczonych w cytacie: „oznaczają informacje o **zidentyfikowanej lub możliwej do zidentyfikowania** osobie fizycznej („osobie, której dane dotyczą")" wnioskujemy, że dane osobowe to informacje dotyczące dwóch kategorii ludzi. Jedna to ludzie zidenty-

niawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 170-173.

[124] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 175.

[125] Podobnie: D. Lubasz, *op. cit.* s. 168.

fikowani, druga to ludzie możliwi do zidentyfikowania. Podkreślenia wymaga, że dane osobowe to informacje o osobie zidentyfikowanej lub możliwej do zidentyfikowania nie zaś jedynie informacje umożliwiające identyfikację osoby. Informacje umożliwiające identyfikacje osoby są, z samej ich istoty, danymi osobowymi. Jeżeli informacja umożliwia identyfikację osoby, to oczywiste jest że jest informacją o konkretnej osobie i tym samym daną osobową[126]. Jeżeli informacja w oderwaniu od innych nie umożliwia identyfikacji osoby, jednak dotyczy ona osoby zidentyfikowanej lub możliwej do zidentyfikowania z wykorzystaniem innych informacji, to jest ona oczywiście daną osobową. o identyfikacji, takiej jak w komentowanym przepisie można powiedzieć, że jest to identyfikacja indywidualna, czyli *możliwość wskazania w populacji konkretnej osoby*[127].

Należy podkreślić fakt, że dane osobowe to informacje *o **zidentyfikowanej lub możliwej do zidentyfikowania** osobie fizycznej* nie zaś jedynie *(...) informacje, które identyfikują lub umożliwiają identyfikację osoby, której dotyczą*[128]. Zwracam na to uwagę, ponieważ z drugim, błędnym, stanowiskiem spotkałem się w komentarzu M. Krzysztofka. Wywód M. Krzysztofka, którego część zacytowałem jest dłuższy, jednak zawarte są w nim słowa wskazane w cytacie. Należy zwrócić baczną uwagę na fakt, że danymi osobowymi są dane dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania (czyli niekoniecznie dane identyfikacyjne, ale jakiekolwiek dane, które dotyczą osoby zidentyfikowanej lub możliwej do zidentyfikowania).[129] Dane umożliwiające identyfikację – dane identyfikacyjne – są danymi osobowymi, ale nie dlatego, że umożliwiają identyfikację, bo o tym mowy w definicji danych osobowych nie ma, ale dlatego, że

---

126 Rzeczownik *dane* pozornie nie posiada w języku polskim liczby pojedynczej. Omawiam to niżej w uwadze *3.7. Art. 4 pkt 1. Uwaga 7. Dane osobowe a dana osobowa*.

127 R. Szałowski, *Ochrona danych osobowych. Komentarz do ustawy z dnia 29 sierpnia 1997 r,* Zielona Góra. 2000, s. 27.

128 M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016, s. 42.

129 Podobnie: M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, *GDPR / Obecné nařízení o ochraně osobních údajů. Prakticy komentař.* Praha 2017, s. 77.

skoro umożliwiają identyfikację, to tym samym dotyczą osoby możliwej do zidentyfikowania.

Pewną ciekawostkę stanowi fakt, że w przepisie definiuje się osobę możliwą do zidentyfikowania, ale nie sposób znaleźć ani słowa o tym, kim jest osoba zidentyfikowana. Nie wydaje się jednak by było to problemem. Jeżeli ktoś jest osobą zidentyfikowaną, to tym samym jest osobą możliwą do zidentyfikowania. Relację: zidentyfikowany a możliwy do zidentyfikowania, można rozpatrywać dla jednego momentu jak również relację tę można rozpatrywać na tle toczącego się czasu. Jeżeli w danym momencie i w danym kontekście konkretną osobę można uznać za zidentyfikowaną, to w tym samym momencie osobę tę trzeba uznać za możliwą do zidentyfikowania, bo przecież jeżeli osoba ta nie była by możliwa do zidentyfikowania to tym samym nie byłaby zidentyfikowana.

W opisany tu sposób zagadnienie rozpatrzone zostało dla jednego momentu w czasie. Rozpatrywanie zagadnienia na tle toczącego się czasu musi prowadzić do wniosku, że jeżeli osoba jest w danej chwili identyfikowana to nieco wcześniej - przed chwilą albo bardzo dawno temu - osoba ta była osobą możliwą do zidentyfikowania. Element „zidentyfikowana lub możliwa do zidentyfikowania", D. Lubasz nazywa przesłanką identyfikowalności.[130]

Ze słów: „**możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej**" wnioskujemy, że przepis definiuje „możliwą do zidentyfikowania osobę fizyczną". By kogoś uznać za osobę możliwą do zidentyfikowania, konieczne jest by istniała możliwość identyfikacji tej osoby. Przepis wskazuje, że możliwość identyfikacji Może mieć charakter bezpośredni lub pośredni. W przepisie wskazany jest katalog kategorii informacji, umożliwiających identyfikację osoby. Jest to katalog otwarty, zatem również inne informacje mogą należeć do informacji umożliwiających

[130] D. Lubasz, *op. cit.* s. 166.

identyfikacje osoby. Zjawisku geolokalizacji poświecił nieco miejsca L. Kępa.[131] Autor ten omawia również inne kategorie danych osobowych, w tym niektóre z kategorii znajdujących się we wskazanym tu ustawowym katalogu.[132]

Opisywana otwartość katalogu informacji jest istotna. Możliwe jest że administrator przetwarza informacje spoza katalogu zamieszczonego w komentowanych przepisie, jeżeli jednak informacje te umożliwiają identyfikację osoby, to one same są one danymi osobowymi i jak również danymi osobowymi są inne informacje dotyczące tak zidentyfikowanych osób.[133]
Należy zwrócić uwagę na fakt, że dane, które służą do identyfikacji osoby fizycznej, z założenia tej osoby fizycznej dotyczą, są zatem danymi osobowymi. Szerzej piszę o tym w uwadze *3.11. Art. 4 pkt 1. Uwaga 11. Ryzyko błędnego koła w definicji*.

Ze słów wytłuszczonych w cytacie: „możliwa do zidentyfikowania osoba fizyczna to osoba, którą można **bezpośrednio lub pośrednio zidentyfikować**" wnioskujemy, że przepis przewiduje, że osobę fizyczną można zidentyfikować bezpośrednio lub pośrednio. Niestety ani ze słów *bezpośrednio lub pośrednio* ani z dalszej, niżej omawianej części przepisu, nie wynika jaka jest różnica miedzy identyfikacją bezpośrednią a pośrednią. Pobieżny rzut oka na przepis pozwala domniemywać, że identyfikacja bezpośrednia to identyfikacja za pomocą imienia i nazwiska zaś identyfikacja pośrednia to identyfikacja za pomocą innych, wymienionych w przepisie identyfikatorów czyli: numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego. Dokładniejsze przyjrzenie się przepisowi pozwala jednak wątpić w tę koncepcję.

W przepisie wymienione są cztery przykładowe kategorie identyfikatorów umożliwiających identyfikację osoby fizycznej są to: „imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy". Prawodawca europejski w żaden sposób nie różnicuje wymienionych identyfikatorów. Wymienione identyfikatory nie zostały podzielone na kategorie które umożliwiają identyfikację bez-

[131] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2014, s. 45-47.

[132] L. Kępa, *op. cit.* s. 42-64.

[133] Por. D. Lubasz, *op. cit.* s. 176.

pośrednią lub pośrednią. Oczywiście samo znaczenie identyfikatorów pozwala, czemu dałem wyraz wyżej, domniemywać, że identyfikacja za pomocą imienia i nazwiska to identyfikacja bezpośrednia a identyfikacja za pomocą numeru identyfikacyjnego, danych o lokalizacji lub identyfikatora internetowego to identyfikacja pośrednia. Możliwa jest też inna interpretacja dotycząca różnicy między identyfikacją bezpośrednią i pośrednią. W przepisie najpierw wymieniono cztery rodzaje identyfikatorów umożliwiających identyfikację osoby fizycznej są to: *imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy*. Dalej w przepisie wymieniono czynniki, które umożliwiają identyfikację człowieka dzięki temu, że określają jego tożsamość *fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną*". Możliwa jest zatem interpretacja zgodnie z którą identyfikacja bezpośrednia zachodzi dzięki identyfikatorom takim jak: *jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy* zaś identyfikacja pośrednia zachodzi dzięki jednemu lub kilku szczególnym czynnikom określającym *fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej*.

Jak wynika z powyższych rozważań, interpretacje dotyczące różnicy miedzy identyfikacją bezpośrednią a pośrednią możliwe są co najmniej dwie i nie wiadomo, która jest właściwa. Możliwe są i inne, jednak ich wywodzenie nie ma sensu. Nie jest ważne co różni identyfikację bezpośrednią od pośredniej. Nie jest ważne gdzie przebiega granica między identyfikacją bezpośrednią a pośrednią, gdziekolwiek by ona nie przebiegała. Nie jest to przynajmniej ważne dla zrozumienia znaczenia definicji danych osobowych. Prawodawca podzielił możliwości identyfikacji na bezpośrednie i pośrednie, jednak nie uzależnił czegokolwiek od tego, czy dana możliwość, metoda identyfikacji to możliwość bezpośrednia czy pośrednia. Nieistotne dla zrozumienia znaczenia definicji jest czy identyfikacja ma charakter bezpośredni czy pośredni. Dla określenia zakresu definicji danych osobowych ważne jest czy identyfikacja jest możliwa czy nie jest możliwa.

Dla określenia zakresu definicji danych osobowych nieistotne jest, czy identyfikacja jest bezpośrednia czy pośrednia. W motywie 26 Preambuły czytamy: *Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasad-*

nione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas, potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.. Jak widać dla określenia zakresu definicji istotne jest czy konkretne, dostępne o danym człowieku informacje umożliwiają identyfikację tego człowieka, a nie czy identyfikację te nazwiemy identyfikacją bezpośrednią czy nazwiemy ją identyfikacją pośrednią.

3. Art. 4 pkt 1. Uwagi

Dla pełnego zrozumienia definicji danych osobowych należy zwrócić uwagę na kilka jeszcze zagadnień. Zagadnienia te omawiam w uwagach poniżej.

3.1. Art. 4 pkt 1. Uwaga 1. Zakres definicji

Dane osobowe to informacje dotyczące żywego człowieka, którego można zidentyfikować w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy. Należy zwrócić uwagę, że imię i nazwisko uznano w przepisie za identyfikator analogiczny wobec pozostałych trzech. Wynika z tego wniosek, że jeżeli znamy jakieś imię i nazwisko, nie jesteśmy jednak w stanie powiązać tego imienia z konkretnym, żywym człowiekiem, to to imię i nazwisko nie jest daną osobową ani nie umożliwia identyfikacji tego człowieka. Jeżeli identyfikujemy człowieka nie używając w tym celu innej metody niż posługiwania się imieniem i nazwiskiem, po czym łączymy z danym zidentyfikowanym człowiekiem to konkretne imię i nazwisko, to to imię i nazwisko jest daną osobowa tego człowieka. Jeżeli zatem jesteśmy w stanie jedynie dzięki podaniu imienia i nazwiska wskazać na konkretnego, żywego człowieka, to człowiek ten jest osobą zidentyfikowaną, wszelkie informacje, które z nim łączymy są danymi osobowymi, jednocześnie imię i nazwisko tego człowieka też są danymi osobowymi tego człowieka.

Podobnie rzecz się ma z numerem identyfikacyjnym. Jeżeli jesteśmy w stanie jedynie dzięki podaniu numeru identyfikacyjnego wskazać na konkretnego, żywego człowieka, to człowiek ten jest osobą zidentyfikowaną, wszelkie informacje, które z nim łączymy są danymi osobowymi, jednocześnie numer identyfikacyjny tego człowieka, używany do identyfikacji też jest daną osobową tego człowieka. Przykładem numeru, który może służyć do identyfikacji jest numer studenckiego indeksu. Numer ten umożliwia identyfikację studenta o ile jesteśmy w stanie powiązać ten numer z konkretnym studentem. Podobnie rzecz się ma z numerem dowodu osobistego, paszportu itp. Jeśli chodzi o numer PESEL, to przyjęło się uważać, że numer ten jest daną osobową. Przemawiają za tym względy historyczne,[134] jest to jednak pogląd błędny. Jeżeli jesteśmy w stanie ustalić kogo dotyczy dany PESEL, to umożliwia on identyfikację osoby i jednocześnie jest daną osobową, jeżeli nie jesteśmy w stanie ustalić kogo dotyczy dany PESEL, to nie umożliwia on identyfikacji osoby i jednocześnie nie jest daną osobową.

Z ostrożności, w praktyce ADO i IOD należy traktować PESEL jak daną osobową, mylne, ale powszechne poglądy są bowiem trudne do zwalczenia. Z punktu widzenia podmiotu, który nie ma dostępu no bazy PESEL, numer ten stanowi dane osobowe dopiero kiedy zostaje zestawiony z innymi danymi, które identyfikują danego człowieka, z punktu widzenia tego podmiotu. O zjawisku danych, które są danymi osobowymi dopiero, kiedy zestawi się je z innymi danymi, które niewątpliwie danymi osobowymi są, pisze[135], choć w innym niż ja tu, kontekście M. Gumularz. Niestety, jeśli chodzi o sam PESEL, to wskazany M. Gumularz pisze: *Przykładem pojedynczej informacji sta-*

[134] Wynikają one z równie jak one historycznego poglądu GIODO, który wyrażono w publikacji, *ABC ochrony danych osobowych*. Warszawa 2007. str. 9. Dosłownie: *Numer ten, występując nawet bez zestawienia z innymi informacjami o osobie, stanowi dane osobowe, a ich przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych*. Zastanawia brak podstawy prawnej dla tak kategorycznie wyrażonego poglądu. Najstraszniejszy jest fakt, że elektroniczna wersja tej publikacji nadal dostępna jest pod adresem: edugiodo.giodo.gov.pl/file.php/1/ODO/ODO_R02_03.htm (dostęp 6 XI 2018 godz. 20.12.) Zmieniono jej formę, w miejsce broszurki jest kilka stroniczek www, ale zawartość jest równie wartościowa.

[135] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział II. POJĘCIE DANYCH OSOBOWYCH. 1.Informacje ogólne.* Warszawa 2018. Lex.

nowiącej daną osobową jest natomiast numer PESEL (...)[136], opisując dalej szczegóły tego numeru, jednak nie uzasadniając, przynajmniej w sposób mnie jakkolwiek przekonujący, swego poglądu.

Dane o lokalizacji o których tu mowa to na przykład dane o lokalizacji zbierane przez stronę www, dane o lokalizacji użytkownika urządzenia nawigacyjnego na przykład w samochodzie, dane o lokalizacji telefonu komórkowego itp. Danymi o lokalizacji są też informacje o położeniu samochodu, którym jedzie konkretny, zidentyfikowany człowiek. Mowa tu o informacjach, jakie posiadają niektórzy przedsiębiorcy, którzy wiedzą dzięki danym o lokalizacji, co mniej więcej w danej chwili robi ich pracownik, a przynajmniej gdzie on jest. Pozornie są to dane o lokalizacji pojazdu, jeżeli jednak pracodawca wie kto w tym pojeździe się znajduje, to dla tego pracodawcy są to dane tego właśnie, znajdującego się w pojeździe człowieka.

Identyfikator internetowy o którym tu mowa to na przykład numer komunikatora, na przykład Gadu-gadu, nazwa w portalu społecznościowym, na przykład w Facebooku, adres poczty elektronicznej, nazwa użytkownika forum internetowego itp.

Jeśli chodzi o czynniki określające *fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej*, to należy przyjąć, że jeżeli jesteśmy w stanie wskazać na konkretnego człowieka poprzez określenie nie identyfikatora (bo o identyfikatorach było wyżej), ale poprzez określenie cech jego tożsamości, to informacje dotyczące tego człowieka są dla nas jego danymi osobowymi.

Na niezwykle ciekawą, choć pozornie oczywistą rzecz zwraca uwagę M. Gumularz, pisze on: *(...) poufność nie jest elementem definiującym „dane osobowe". Oznacza to, że informacje publicznie dostępne, jeżeli dotyczą osoby fizycznej, nie tracą statusu danych osobowych*.[137] Dane niepoufne nie tracą przymiotu danych osobowych, inaczej – dane jawne są danymi osobowymi nie mniej niż dane poufne.

[136] M. Gumularz, *loc. cit.*

[137] M. Gumularz, *loc. cit.*

3.1. Art. 4 pkt 1. Uwaga 2.
Zakres definicji. Obiektywizacja zakresu definicji

Niezwykle ciekawy wniosek wynika z motywu 26 Preambuły RODO. Jedno ze zdań tego przepisu stanowi: *Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie* ***obiektywne czynniki****, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny*. Zdanie to jest niezwykle doniosłe, czyni bowiem bardzo szerokim zakres definicji danych osobowych. Prawodawca wskazuje, że o identyfikowalności osoby decydują obiektywne czynniki i dostępna w momencie przetwarzania danych technologia. Lektura cytowanego zdania preambuły nie nastraja optymistycznie. Jeżeli brano by pod uwagę jedynie czynniki takie jak technologia i postęp technologiczny, to zakres definicji danych osobowych byłby niezwykle szeroki.[138]

Współczesne technologie umożliwiają identyfikację osób, naprawdę na podstawie niezwykle nikłych danych. Państwa posiadają zbiory danych, na podstawie, których zapewne mogą identyfikować obywateli. Myśl tu przedstawiona ma charakter pewnej, trudnej dla mnie do udowodnienia hipotezy, ale zakładam, że zdjęcia we współczesnych dowodach osobistych wydawanych w Polsce, mają charakter biometryczny. Nie wiem oczywiście, czy państwo polskie zbiera zdjęcia obywateli, by móc ich rozpoznawać, jest to jednak możliwe, a co więcej wydaje się to racjonalne. Zostawiając na boku, wskazany tu hipotetyczny przykład, zwracam uwagę na fakt, że państwa, służby specjalne, czy nawet prywatne agencje, nie dzielące się szeroko wiedzą, którą posiadają lub podmioty lecznicze posiadają zapewne zbiory danych, do których nie udzielają dostępu zwykłym obywatelom. Jak więc widać obiektywizacja czynników umożliwiających identyfikację osoby fizycznej, nie do końca jest możliwa. Administrator danych może posiadać pewne dane dotyczące osoby fizycznej, dane te obiektywnie umożliwiają identyfikację, ale na przykład jedynie wtedy, jeżeli identyfikacji tej dokonać pragnie któraś z licznych służb specjalnych. Dla danego ADO identyfikacja osoby fizycznej, na podstawie posiadanych przez tego ADO danych, nie jest w opisywanej

[138] Por. M. Gumularz, *loc. cit*

sytuacji możliwa. W ten sposób pozornie obiektywne możliwości identyfikacji, nabierają waloru subiektywnego. Administrator danych posiada dane, które obiektywnie umożliwiają identyfikację, jednak administrator, który dane posiada, nie może tej identyfikacji dokonać, choćby dlatego, że żadna ze służb państwowych, czy żaden podmiot leczniczy, nie podzieli się z nim posiadaną przez siebie wiedzą.

Z założenia subiektywny charakter mają dwa pozostałe czynniki wskazane przez prawodawcę, a to koszt i czas. Być może inaczej niż prawodawca rozumiem obiektywność kosztu i obiektywność czasu, ale dla mnie te czynniki mają charakter subiektywny. Koszt zidentyfikowania osoby jest jakiś. Administrator danych może ten koszt ponieść lub nie. Może ponieść – ustali kogo dotyczą posiadane przezeń informacje, nie może ponieść – nie ustali kogo dotyczą posiadane przezeń informacje. O tym czy informacje umożliwiają identyfikację osoby, decyduje to, czy administrator może na zidentyfikowanie osoby na podstawie tych informacji ponieść takie a nie inne koszta. Wynika z tego, że informacje, które dla jednego administratora są danymi osobowymi, dla innego nie są. Dostrzegam tu silny element subiektywizujący zakres definicji.[139]

3.2. Art. 4 pkt 1. Uwaga 3. Dane spseudonimizowane

Naukowa uczciwość nakazuje odnieść się do poglądu P. Litwińskiego dotyczącego danych spseudonimizowanych. Otóż autor ten pisze: *Ponieważ pseudonimizacja jest czynnością odwracalną, spseudonimizowane dane osobowe należy traktować jak dane osobowe*[140]. Dalej P. Litwiński wskazuje na motyw 26 Preambuły RODO. Warto zacytować odpowiednie słowa Preambuły: *Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej*. Pogląd P. Litwińskiego jest zbieżny z wnioskiem, który z cytatu z preambuły RODO wypływa, czyli że dane

[139] Podobnie o subiektywnej stronie definicji: L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 29.

[140] P. Litwiński, P. Barta, M. Kawecki. w: Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 174.

spseudonimizowane to dane osobowe. Należy zwrócić tu uwagę na pewien niuans. Uważam, że pogląd P. Litwińskiego i wniosek z preambuły są trafne jednak trzeba być ostrożnym, by nie wpaść tu w pewną pułapkę. Tego czy jakieś informacje są danymi osobowymi nie powinno się oceniać tylko z punktu widzenia administratora. Wystarczy wyobrazić sobie, że administrator spseudonimizował dane osobowe, po czym dane spseudonimizowane przekazał podmiotowi przetwarzającemu. Pogląd P. Litwińskiego i zacytowany fragment Preambuły nakazują sądzić, że podmiot przetwarzający jest, w opisanej sytuacji, w posiadaniu danych osobowych, i tak właśnie jest. W opisanej sytuacji podmiot przetwarzający jest w posiadaniu danych spseudonimizowanych, które administrator, w każdej chwili, w drodze odwrócenia pseudonimizacji, może zamienić w niespseudonimizowane dane osobowe. Należy jednak przy tym pamiętać, że art. 4 pkt 1 nie ogranicza danych osobowych do informacji, które dotyczą osoby fizycznej identyfikowalnej dla tego czy innego podmiotu czy ADO. Jeśli informacja spełnia warunki z art. 4 pkt 1 RODO, to należy do danych osobowych. To wynika z definicji. Takie podejście ogromnie rozszerza zakres informacji, które są danymi osobowymi a tym samym czyni szerokim zakres RODO.

Jeżeli definicja nie jest analizowana przez pryzmat tego czy innego podmiotu przetwarzającego dane osobowe, administratora, podmiotu przetwarzającego – kogokolwiek, to okazuje się, że każde dane, które kogoś dotyczą są danymi osobowymi. Nieważne czy osoba jest identyfikowalna dla administratora. Czyni to zakres definicji danych osobowych, a przez to i zakres pojęcia: „administrator" bardzo szerokim, ale tak właśnie jest. Bardzo dobrym komentarzem może być tu zdanie czeskich autorów: *Osobę fizyczną można uważać za zidentyfikowaną, jeżeli administrator lub podmiot przetwarzający może ją odróżnić od innych osób z użyciem danych które ma w dyspozycji*.[141] Dalej ci sami autorzy zwracają uwagę na fakt, że człowieka można uważać za możliwego do zidentyfikowania, jeżeli ADO, PP lub ktoś inny jest w stanie go zidentyfikować za pomocą posiadanych danych lub za pomocą danych, które posiada ktoś inny. Czescy

[141] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, *GDPR / Obecné nařízení o ochraně osobních údajů. Prakticy komentař,* Praha 2017, s. 78. Nieco niepokoi użycie słowa „lub", w czeskim oryginale: „nebo", na co zwrócił mi uwagę, podczas pewnej fascynującej, publicznej, fejsbukowej, dyskusji K. Wygoda.

autorzy zwracają uwagę na element rozsądku, limitujący czy w danej sytuacji identyfikacja jest możliwa czy nie.[142] Do problemu tego odnoszę się też nieco w komentarzu do art. 4 pkt. 5 RODO.

3.4. Art. 4 pkt 1. Uwaga 4.
Dane dotyczące dzieci urodzonych żywo i nieurodzonych

Naukowa uczciwość nakazuje też odnieść się do rozważań P. Litwińskiego na temat danych osobowych dzieci. Informacje dotyczące dzieci są danymi osobowymi. Jeśli dziecko urodzi się żywe to informacje go dotyczące, jednak z okresu życia przed urodzeniem, są danymi osobowymi, jeżeli urodzenie żywe nie zajdzie to informacje na temat bytu, któremu nie dane było urodzić się żywym są danymi osobowymi jego matki lub/i ojca – streszczam tu ogólną wiedzę dotyczącą danych osobowych dzieci, obecną u P. Litwińskiego, P. Barty i M Kaweckiego[143], z którą się oczywiście zgadzam, musze jednak dodać kilka uwag. Dane bytu, który nie urodził się jako żywe dziecię mogą być (zależnie od sytuacji) danymi ojca, matki, surogatki, dawcy nasienia, dawczyni komórki jajowej. Kiedy dziecię urodzi się żywe to dane te są również danymi osobowymi dziecięcia.

3.5. Art. 4 pkt 1. Uwaga 5.
Uprawnienia osób nieletnich na gruncie RODO

Jeśli chodzi o dzieci, to należy dodać, że dzieciom – osobom nieletnim – przysługują wszystkie uprawnienia wynikające z RODO. RODO wprowadza pewne ograniczenia w kwestii zgody, ale nie widzę powodu by uznawać, że wobec osoby nieletniej nie należy realizować art. 13 RODO, art. 14 RODO i przepisów dalszych.

3.6. Art. 4 pkt 1. Uwaga 6.
Szczególne kategorie danych, dane wrażliwe, nazewnictwo

Nie sposób zgodzić się z poglądem P. Litwińskiego, P. Barty i M Kaweckiego, jakoby: *(...) podział na dane osobowe zwykłe oraz dane osobowe wrażliwe (lub sensytywne (...)) został zastąpiony na*

[142] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek,*op. cit*. s. 79. Relacja poglądu czeskich autorów nie jest dokładnym cytatem, dlatego też nie jest jako cytat oznaczona, jest pewnym uprzystępnieniem tego poglądu.

[143] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 176.

gruncie RODO przez wyodrębnienie szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 i art. 10 RODO[144]. Co prawda dane nazywane tradycyjnie danymi wrażliwymi zostały w tytule art. 9 RODO nazwane: „szczególnymi kategoriami danych osobowych", tytuł art. 9 RODO brzmi bowiem: *Przetwarzanie szczególnych kategorii danych osobowych*. Tajemnicą pozostanie, dlaczego art. 9 RODO nie został zatytułowany: „przetwarzanie danych osobowych wrażliwych", lub „przetwarzanie wrażliwych danych osobowych". Motyw 10 Preambuły RODO zawiera między innymi słowa: *Niniejsze rozporządzenie umożliwia też państwom członkowskim doprecyzowanie jego przepisów, w tym w odniesieniu do przetwarzania szczególnych kategorii danych osobowych (zwanych dalej „danymi wrażliwymi").*

Jak widać twórcy RODO utożsamiają nazwę „szczególne kategorie danych osobowych" z nazwą: „dane wrażliwe". Ja, dla jasności posługuję się dla danych wrażliwych nazwą: „wrażliwe dane osobowe". Po co wprowadzono dwie nazwy dla określenia jednej grupy danych, po co w ogóle wprowadzono nową nazwę – nie wiadomo. By oddać sprawiedliwość M. Gumularzowi, przyznaję, że o włos dalej zwrócił uwagę na *orzeczenie Trybunału Sprawiedliwości UE w sprawie C-434/16, Peter Nowak przeciwko Data Protection Commissioner, ECLI:EU:C:2017:994.*[145], z którego bezspornie wynika, że treść odpowiedzi na egzaminie stanowi dane osobowe.

3.7. Art. 4 pkt 1. Uwaga 7.
Szczególne kategorie danych, dane wrażliwe, nazewnictwo

Na niezwykle ciekawą, choć wydawałoby się oczywistą, rzecz zwrócili autorzy czeskiego Komentarza. Zauważyli oni, że nieistotne jest czy dane są „prawdziwe i obiektywnie mierzalne (data narodzenia, miejsce zamieszkania, dane o własności konkretnej rzeczy", czy są to przewidywania dotyczące cech człowieka, czy osoba ta będzie

[144] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 191.

[145] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Dane osobowe podane, zaobserwowane, pochodne oraz wywnioskowane,* Warszawa 2018, Lex.

dobrym wierzycielem lub klientem.[146] Nieco współgra to z rozważaniami M. Gumularza, który twierdzi, że dane dzielą się na: *podane dane osobowe*, *zaobserwowane dane osobowe*, *pochodne dane osobowe*, *wywnioskowane dane osobowe*.[147]

Podane dane osobowe to dane osobowe, *świadomie podawane przez osoby fizyczne*[148], acz wskazany autor pomija tu fakt, czy dane są podawane przez osoby fizyczne, których dane dotyczą, czy również przez inne osoby.

Zaobserwowane dane osobowe to dane osobowe *rejestrowane automatycznie, np. za pomocą plików cookies lub czujników online, lub telewizji przemysłowej umożliwiającej rozpoznanie twarzy*[149]. Tu z kolei nie rozumiem, czemu zaobserwowanymi danymi osobowymi nie miałyby być dane osobowe rejestrowane nieautomatycznie.

Pochodne dane osobowe to dane osobowe *„tworzone" z innych danych w stosunkowo prosty i bezpośredni sposób, np. przy obliczaniu zdolności kredytowej klienta*[150].

Wywnioskowane dane osobowe to „dane osobowe tworzone za pomocą bardziej złożonych metod analitycznych"[151].

Różnica między pochodnymi danymi osobowymi a wywnioskowanymi danymi osobowymi jest wątła, mniej więcej taka jak między bardzo słoną zupą a niezwykle słoną zupą – językowa. Mirosław Gumularz dodaje, co prawda, że *Dane wywnioskowane są oparte na prawdopodobieństwach i w związku z tym są mniej pewne niż dane pochodne.*[152], jednak podziały przezeń podane mnie nie przekonują. Przywołuję je tu z naukowej uczciwości, nie dostrzegam jednak by miały konkretną wartość.

[146] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, *GDPR / Obecné nařízení o ochraně osobních údajů. Prakticy komentař,* Praha 2017, s. 78. Słowa w cudzysłowie przetłumaczone przez J. Rzymowskiego. Przykład dotyczący wierzyciela pochodzi również od wskazanych czeskich autorów.

[147] M. Gumularz, *loc. cit.*

[148] M. Gumularz, *loc. cit.*

[149] M. Gumularz, *loc. cit.*

[150] M. Gumularz, *loc. cit.*

[151] M. Gumularz, *loc. cit.*

[152] M. Gumularz, *loc. cit.*

3.8. Art. 4 pkt 1. Uwaga 8.
Dane osobowe a dana osobowa

Rzeczownik „dane" nie posiada w języku polskim liczby pojedynczej. Jest to rzeczownik zbiorowy, podobny do rzeczowników: spodnie i nożyczki. O ile jednak można sobie bezproblemowo poradzić bez liczby pojedynczej spodni i nożyczek, o tyle w przypadku danych, szczególnie danych osobowych, brak liczby pojedynczej jest brakiem, który czasem utrudnia wywód, zwłaszcza prawniczy, który winien być precyzyjny. Z tego względu używam, w niniejszej publikacji, formy: dana osobowa, w nadziei, że forma ta na stałe zagości w polskiej mowie. Może się tak stać, że czasem formę tę spotkać można, przykładem jest choćby archiwalna dziś strona GIODO, na której czytamy: *Czy sam numer karty miejskiej jest daną osobową w rozumieniu ustawy o ochronie danych osobowych?*[153].

Należy też zwrócić uwagę na pewien inny niż językowy aspekt rzeczownika: „dane". Zastanawiam się otóż, nad tym czy rzeczownik: „dane" występuje w liczbie mnogiej tylko ze względów językowych. Jeżeli wyobrazimy sobie jakąś informację, która może dotyczyć człowieka, na przykład, że człowiek ten ma na imię Zdenek. Samo imię, w tym wypadku Zdenek, nie ma charakteru danych osobowych, jeżeli ADO, z którego punktu widzenia patrzymy, nie wie kto nosi to imię. By informacja miała charakter danych osobowych informacja ta musi się składać z dwóch elementów, po pierwsze istotna jest sama treść informacji „że Zdenek", po drugie, istotne jest kto nosi to imię „że ADO wie kim jest Zdenek". Dane są dwie. ADO wie że Zdenek i kto jest tym Zdenkiem. Jak zatem widać dane są dwie – treść i do kogo się owa treść odnosi. Wydaje się, że dane osobowe muszą występować co najmniej w takich parach, mogą i w większych grupach, kiedy to ADO wie kogo dotyczy cały szereg informacji. Właśnie z uwagi na fakt, że dane osobowe, dla swego istnienia, muszą koniecznie występować co najmniej po dwie, prawdopodobnie właściwe jest używanie określenia „dane osobowe" nie zaś: „dana osobowa". Tym niemniej, kiedy bierzemy pod uwagę jedną informację „że Zdenek", albo „że Czech", to niezwykle wygodnie jest posługiwać się pojęciem: „dana osobowa".

[153] https://archiwum.giodo.gov.pl/pl/319/3512 (dostęp 20.11.2020 godz. 17.00)

Należy przywołać tu również stanowisko P. Fajgielskiego, który w swoim Komentarzu twierdzi: *(...) o niewłaściwej praktyce używania pojęcia danych osobowych w liczbie pojedynczej („dana osobowa"*. Tego rodzaju sformułowanie jest niezgodne z regułami językowymi, ponieważ określenie *dane* występuje języku polskim w omawianym tu znaczeniu jako wyraz nieposiadający liczby pojedynczej."[154]. Jak widać wskazany autor odwołuje się jedynie do argumentów językowych.

3.9. Art. 4 pkt 1. Uwaga 9.
Dane osobowe w nazwach przedsiębiorstw

Należy zwrócić uwagę na fakt, że dane osobowe występują często w sytuacjach, w których, z samej natury tych sytuacji, mają charakter jawny, jednak nadal są danymi osobowymi.

Przykładem takich danych są dane osób prowadzących działalność gospodarczą. Imiona i nazwiska w nazwach przedsiębiorstw prowadzonych w oparciu o konstrukcję jednoosobowej działalności gospodarczej czy w nazwach spółek, nie tracą przymiotu danej osobowej jedynie dlatego, że właśnie w nazwach się znajdują.[155]

3.10. Art. 4 pkt 1. Uwaga 10.
Dane zwykłe

Dane osobowe dzielą się obecnie na dane osobowe i dane osobowe szczególnej kategorii. Dla danych osobowych szczególnej kategorii funkcjonuje nadal, a funkcjonuje ponieważ ma to podstawę w Preambule RODO, nazwa: „dane wrażliwe. Dane osobowe, które nie są danymi wrażliwymi wygodnie jest również jakoś nazywać, jeszcze na gruncie UODO97 przyjęła się nazwa „dane zwykłe", by być precyzyjnym lepiej jest używać nazwy: „zwykłe dane osobowe" lub: „dane osobowe zwykłe". Nazwy „dane zwykłe" używa L. Kępa, używa jej

[154] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* w: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* WKP 2018 – Komentarz, Kom. do art. 4 pkt 1.

[155] Podobnie, choć nie o spółkach: L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 9

do tego stopnia, że tytułuje tak nawet podrozdział swej publikacji i podejmuje próbę ich zdefiniowania. Najistotniejszym elementem propozycji L. Kępy są słowa: „(…) czym są dane zwykłe: to wszystkie dane osobowe, które nie są wrażliwe” [156]

Na gruncie RODO można zatem dane zwykłe zdefiniować w sposób zaproponowany poniżej.

Dane osobowe zwykłe to wszystkie dane, które nie należą do szczególnych kategorii danych.

3.11. Art. 4 pkt 1. Uwaga 11. Ryzyko błędnego koła w definicji

W definicji danych osobowych prawodawca wskazuje na katalog przykładowych informacji, które umożliwiają identyfikacje osoby fizycznej. Dane, które służą do identyfikacji osoby fizycznej, dotyczą tej osoby fizycznej, są zatem danymi osobowymi. Okazuje się zatem, że możliwa do zidentyfikowania osoba fizyczna to ktoś, kogo można zidentyfikować w oparciu o dane, które są z tą osobą połączone w ten czy inny sposób. Pojawia się tu coś na kształt swoistego błędnego koła, prezentuje je poniżej w postaci wyliczenia, tak by rozumowanie było bardziej widoczne.

- Dane osobowe to informacje dotyczące możliwej do zidentyfikowania osoby fizycznej.
- Możliwa do zidentyfikowania osoba fizyczna to ktoś kogo można zidentyfikować.
- Identyfikacja osoby fizycznej następuje w oparciu o cechy tej osoby związane z tą osobą tak mocno i tak mocno na nią wskazujące, że wskazanie cechy lub zestawu cech pozwala na identyfikacje osoby.
- Cechy, które pozwalają na identyfikację osoby to informacje które dotyczą tej osoby.
- Informacje, które dotyczą osoby fizycznej to dane osobowe.

Wskazane tu błędne koło nie skutkuje, jak mi się zdaje, niemożnością zdefiniowania danych osobowych, jednak jest to zjawisko, nad którym warto się zastanowić, prowadzić może bowiem do niepokojących wniosków. Podstawowy wniosek, który się tu nasuwa jest taki, że należy się zastanowić nad tym skąd wiemy, że te a nie inne

[156] L. Kępa *Ochrona danych osobowych w praktyce.* Warszawa 2014. s. 31

informacje (cechy) pozwalają na identyfikację tej a nie innej osoby fizycznej. Czy wiemy o tym z doświadczenia? Być może problem może wydawać się wydumany, uważam jednak, że takim nie jest. Nie jest ponieważ od ustalenia czy konkretne informacje są danymi osobowymi czy nie są nimi, zależeć może czy dany administrator poniesie w danej sytuacji karę czy nie. Z tego choćby względu warto się nad problemem przypisywalności konkretnych informacji, zwłaszcza danych identyfikacyjnych, zastanowić.

3.12. Art. 4 pkt 1. Uwaga 12.
Dane osobowe a stosowalność RODO

Na ciekawą myśl natknąłem się w komentarzu do omawianej tu definicji, autorstwa L. A. Bygravea i L. Tosoniego. Myśl ta ma charakter pewnego truizmu, jednak kiedy zostaje wypowiedziana, to można dostrzec doniosłość zjawiska jakie zauważyli jej autorzy.

Wskazani autorzy piszą: *The definition of 'personal data' is of vital importance for determining whether or not the GDPR applies. Indeed, 'personal data' (or equivalents, such as 'personal information') is a threshold concept for the application of data protection law generally: if data being processed are not personal data, their processing is not subject to such law*[157], w języku polskim tłumaczy się na: *Definicja «danych osobowych» jest niezwykle ważna dla ustalenia czy RODO się stosuje czy nie. W istocie «dane osobowe» (lub ekwiwalenty znaczeniowe, takie jak informacje osobowe) są pojęciem progowym dla stosowanie prawa ochrony danych w ogólności: jeśli przetwarzane dane nie są danymi osobowymi, ich przetwarzanie nie podlega takiemu prawu.*[158].

Zwracam uwagę na zacytowaną wyżej myśl, wskazuje ona bowiem na niezwykle doniosłe zjawisko. Jeżeli podmiot nie przetwarza danych osobowych, to RODO w ogóle nie ma do niego zastosowania. Dla stosowania RODO, przepis ten jest równie doniosły jak prze-

[157] L. A. Bygrave, L. Tosoni w: *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 105.

[158] Tłumaczenie: J. Rzymowski. Wyjaśniam, że *equivalents* przetłumaczyłem na *ekwiwalenty znaczeniowe* nie zaś na „synonimy" ponieważ chciałem wskazać raczej na desygnat, niż na nazwę. Każde tłumaczenie jest w istocie adaptacją, na co chcieli wskazać autorzy – trudno orzec.

pisy ustanawiające zakres RODO czyli art. 1 RODO, art. 2 RODO i art. 3 RODO.

3.13. Art. 4 pkt 1. Uwaga 13.
Dane grup ludzi jako dane osobowe

Na marginesie prowadzonych rozważań, warto zastanowić się nad sytuacją, w której informacje odnoszą się nie do konkretnej osoby fizycznej ale do grup osób fizycznych. Istotne jest, czy informacje odnoszące się do takich grup są danymi osobowymi. Problemowi temu przyglądają się L. A. Bygrave i L. Tosoni,[159] trudno jednak ustalić ich stanowisko w tej sprawie. Autorzy ci odnoszą się do wyroków ETS, które to wyroki nie są tu jednak jednolite w wymowie.

Wydaje się, że jeżeli zadajemy pytanie o to czy informacje odnoszące się do grup ludzi są danymi osobowymi, to aby na nie odpowiedzieć trzeba ustalić jedno. Trzeba mianowicie ustalić czy informacje takie można powiązać z konkretnymi członkami takiej grupy. Jeśli można – są to dane osobowe.

3.14. Art. 4 pkt 1. Uwaga 14.
Dane osobowe osób zmarłych

Jeśli chodzi o dane osobowe osób zmarłych to sytuacja jest niezwykle ciekawa. Motyw 27 Preambuły RODO stanowi, że: *Niniejsze rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych*. Jak widać, RODO nie ma zastosowania do danych osobowych osób zmarłych. Z zacytowanego motywu wynika jednak, że zjawisko takie jak „dane osobowe osób zmarłych" funkcjonuje. Funkcjonuje, ponieważ cytowany motyw 27 Preambuły RODO stanowi właśnie o takich danych, o danych osobowych osób zmarłych.

W art. 4 pkt 1 RODO zdefiniowano dane osobowe. Nie sposób nie zadać sobie pytania, czy definicja ta odnosi się tylko do danych osobowych osób żyjących, czy również do danych osobowych osób zmarłych. Cytowani już wyżej, L. A. Bygrave i L. Tosoni[160] twierdzą, że *The definition of 'personal data' in Article 4(1) GDPR does not*

[159] L. A. Bygrave, L. Tosoni, *op. cit.* s. 110.

[160] L. A. Bygrave, L. Tosoni, *op. cit.* s. 112.

cover data on deceased persons., czyli, że: *Definicja danych osobowych nie obejmuje osób zmarłych*[161]. Wniosek taki jest najprostszy, sam się nasuwa, przecież skoro prawodawca w motywie 27 pisze, że RODO *(...) nie ma zastosowania do danych osobowych osób zmarłych. (...)* i skoro definicja znajduje się w RODO, to definicja nie obejmuje (*does not cover*) osób zmarłych. Nie wiem oczywiście czy zrekonstruowałem rozumowanie cytowanych autorów, czy je całkiem wymyśliłem, jednak ufam, że zrekonstruowałem ponieważ to właśnie oni powołują motyw 27 Preambuły RODO w swoim wywodzie.

I tu właśnie pojawia się problem, który wymaga nieco głębszego podejścia. W motywie 27 Preambuły RODO jest napisane co jest napisane (cytuję wyżej), jednak nie sposób nie zauważyć, że prawodawca używa zwrotu: *dane osobowe osób zmarłych*. Zgodnie z dyrektywą języka prawnego[162], znaczenia tego pojęcia należy najpierw szukać w akcie prawnym, w którym pojęcie występuje. Szukamy. I znajdujemy definicję danych osobowych w art. 4 pkt 1 RODO. Zasady wykładni są, jak uważam, nadrzędne wobec znaczeń pojęć, których wykładnia jest dokonywana, bowiem to właśnie dzięki zasadom wykładni można ustalić znaczenie tych pojęć. Idąc zatem dalej należy stwierdzić, że dane osobowe osoby zmarłej, to dane osobowe zdefiniowane w art. 4 pkt 1 RODO, tyle, że odnoszące się nie do żyjącego człowieka ale do człowieka zmarłego i że poza faktem częściowego zdefiniowania tych danych, RODO się nimi nie zajmuje.

3.15. Art. 4 pkt 1. Uwaga 15.
Preparaty medyczne a dane osobowe

By nie pozostawić niedopowiedzeń w wywodach warto ustosunkować się jeszcze do problemu preparatów, substancji, płynów z ciała ludzkiego. Przyznam, że nie dostrzegam doniosłości problemu, z uwagi na jego niezwykłą prostotę. Same substancje uzyskane z ciała ludzkiego nie są danymi osobowymi. Dane osobowe można uzyskać z analizy tych substancji. Wynika to, jak uważam z definicji danych osobowych. Wynika to również z motywu 24 Preambuły RODO i z motywu 35 Preambuły RODO. Rozumowanie takie prowadzą

[161] Tłumaczenie: J. Rzymowski.

[162] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

L. A. Bygrave i L. Tosoni.[163] Rozumowanie to należy jednak poprowadzić dalej. Substancja pobrana od osoby fizycznej nie stanowi danych osobowych, dane sobowe można dopiero z niej uzyskać – to wiemy, to piszą cytowani autorzy. Należy jednak dodać, że:

- informacja, że od osoby fizycznej pobrano taką to a taką substancję, stanowi dane osobowe,
- informacja dotycząca osoby fizycznej znajdująca się np. na probówce zawierającej substancję pobraną od osoby fizycznej, stanowi dane osobowe,
- informacja, że dana substancja została pobrana od tej to a tej osoby fizycznej stanowi dane osobowe,
- informacja jakie badania należy wykonać wobec danej próbki, jakim analizom ja poddać, również stanowi dane osobowe.

Jak piszę wyżej, nie dostrzegam, doniosłości czy odkrywczości zapisanych powyżej konstatacji, zamieszczam je jednak jako uzupełnienie wypowiedzi L. A. Bygravea i L. Tosoniego.

4. Art. 4. pkt 1. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 1 RODO definiuje dane osobowe, zatem zgodnie z dyrektywą języka prawnego[164], każdy kto interpretuje RODO powinien rozumieć pojęcie „dane osobowe" tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „dane osobowe" tak jest ono zdefiniowane w art. 4 pkt. 1 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, ze ADO będzie rozumiał znaczenie pojęcia „dane osobowe" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

---

[163] L. A. Bygrave, L. Tosoni *loc. cit.*

[164] M. Zirk-Sadowski w: *System Prawa Administracyjnego* Red: R Hauser, Z Niewiadomski, A Wróbel. *Tom IV. Wykładnia w prawie administracyjnym.* L. Leszczyński, B. Wojciechowski, M. Zirk-Sadowski. Warszawa 2012. s. 199.

5. Art. 4. pkt 1. Konkretyzacja zasad

Znaczenie pojęcia „dane osobowe" jest istotne w kontekście rozumienia zasad z art. 5 RODO. Jest istotne, ponieważ zasady te to *Zasady dotyczące przetwarzania danych osobowych* – tak stanowi tytuł przepisu. W związku z tym, znaczenie art. 5 RODO, znaczenie zasad ustanowionych w tym przepisie, jest ściśle związane ze znaczeniem pojęcia „dane osobowe". W tym samym przepisie, jego część wstępna brzmi: *Dane osobowe muszą być:* i dalej ustanowione są zasady. Czyli zasady to tak naprawdę warunki przetwarzania danych osobowych.

Można tu wysnuć pewną ryzykowną tezę, uważam jednak, że takie jak ta, nie komentarzowe części niniejszej publikacji są właściwym miejscem na takowe tezy. Można otóż stwierdzić, że *Zasady dotyczące przetwarzania danych osobowych* to dodatkowa grupa przesłanek legalizujących przetwarzanie danych osobowych. Że są to przesłanki analogiczne do tych z art. 6 RODO i z art. 9 RODO i z art. 10 RODO. Mam świadomość, że teza ta jest rewolucyjna, nie dlatego jednak ją stawiam.

6. Art. 4. pkt 1. Postulaty de lege ferenda.
6.1. Art. 4. pkt 1. Postulat 1.
Uproszczenie treści przepisu

Jasność przepisu i jego dostępność dla osób bez przygotowania prawniczego skłaniają do zaproponowania jego modyfikacji. Zamiast pisać o „osobie fizycznej" i na podstawie Preambuły doprecyzowywać, że osoba fizyczna to na pewno żywy człowiek, można po prostu zastąpić słowa: *osobie fizycznej* słowami: *żywym człowieku*. Przepis miałby wtedy postać: „(...) oznaczają informacje o zidentyfikowanym lub możliwym do zidentyfikowania **żywym człowieku** („osobie, której dane dotyczą") (...)".

6.2. Art. 4. pkt 1. Postulat 2.
Dalsze uproszczenie treści przepisu

Około 8 tys. znaków poświęciłem na to by wyjaśnić kto to tak naprawdę jest „możliwa do zidentyfikowania osoba fizyczna". Rozważania te nasuwają mi wniosek, zgodnie, z którym i w tym zakresie przepis należałoby zmodyfikować, tak by miast pretensjonalnych wy-

wodów o tym któż to jest możliwa do zidentyfikowania osoba fizyczna i żenującego braku tekście prawnym, w postaci zapomnienia o zidentyfikowanej osobie fizycznej wprowadzić do przepisu sam konkret, o którym piszę wyżej. Przepis może zatem mieć treść: „(...) oznaczają wszelkie informacje o osobie fizycznej, którą administrator danych jest w stanie odróżnić od innych osób fizycznych".

6.3. Art. 4. pkt 1.Postulat 1 + Postulat 2 = Postulat 3. Jeszcze dalsze uproszczenie treści przepisu

Jednoczesne zastosowanie wniosków wynikających z obu postulatów nasuwa wniosek, ze przepis może wyglądać jeszcze inaczej, przepis może mieć treść: „(...)" oznaczają wszelkie informacje o żywym człowieku, którego administrator danych jest w stanie odróżnić od innych żywych ludzi".

6.4. Art. 4. pkt 1. Postulat 4. Uproszczenie treści przepisu w mniejszym zakresie

Możliwa jest też mniej radykalna zmiana przepisu. Z rozważań prowadzonych wyżej wynika, że nie da się w sposób uczciwy wskazać różnicy między identyfikacją bezpośrednią a identyfikacją pośrednią. Jednocześnie słowa o identyfikacji bezpośredniej czy pośredniej nie wnoszą nic wartościowego do treści przepisu. Skoro tak, to można, a nawet należy je usunąć. Część przepisu: *(...) możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować (...)* powinna brzmieć: „możliwa do zidentyfikowania osoba fizyczna to osoba, którą można zidentyfikować", Słowa *bezpośrednio lub pośrednio* powinny zostać usunięte z przepisu, a po prawdzie nie powinny nigdy do niego trafić.

7. Art. 4. pkt 1. Rozważania historyczne.

7.1. Art. 4. pkt 1. Rozważanie 1. Odpowiedniki w dawnej legislacji

Odpowiednikiem art. 4 pkt 1 RODO jest art. 2 lit d Dyrektywy 95/46/WE i art. 7 pkt 4 UODO97.

Definicja danych osobowych jest podobna do definicji w Dyrektywie 95/46/WE, A. Krasuski w związku z tym, we właściwy sobie erudycyjny sposób, stwierdził, że: *(...) należy uznać, że przy ustalaniu*

definicji danych osobowych w RODO ustawodawca unijny oparł się na koncepcji kontynuacji w odniesieniu do przyjętego w dyrektywie 95/46/WE sposobu kwalifikowania informacji jako dane osobowe[165].

7.1. Art. 4. pkt 1. Rozważanie 2. Względność ontologiczna danych (osobowych)

Na gruncie poprzedniej legislacji L. Kępa zauważył,[166] że takie same dane w jednych okolicznościach danymi osobowymi są a w innych okolicznościach takie same dane danymi osobowymi nie są. W tym samym miejscy swojej książki L. Kepa zwrócił uwagę na fakt, ze zależnie od tego czy dane są danymi osobowymi czy nie, zależy poziom ich ochrony, co z kolei przekłada się na koszta tegoż.[167] Okoliczności, które decydują o tym czy konkretne informacje są danymi osobowymi czy nie to jak pisze L. Kępa *(...) głównie możliwości zestawienia danych z innymi danymi przez tego, który jest we władaniu danych, prowadzące do ustalenia tożsamości osoby, której dane dotyczą*[168]. O ile uwagi L. Kępy uważam za trafne, dlatego zresztą je cytuję, tu czuję potrzebę poczynienia pewnych uzupełnień.

Podmiot, który „jest we władaniu danych" to zapewne administrator lub podmiot przetwarzający. Nie jestem też pewien czy poprawne są słowa o ustaleniu tożsamości, tę bowiem zwykle utożsamiamy z nazwiskiem i imieniem, a przecież możliwe jest, że administrator wie kogo konkretne informacje dotyczą, mimo, że nie zna imienia i nazwiska tej osoby. Na przykład restaurator, który wie, że ten to a ten gość restauracji zawsze zamawia taką a nie inną potrawę, mówi z cudzoziemskim akcentem itd., zna te właśnie wymienione dane osobowe tego gościa restauracji, nie zna jednak jego imienia ani nazwiska. Czy klient restauracji jedzący zupę jest osobą zidentyfikowaną dla restauratora? Uważam, że tak, ten konkretny człowiek jest zidentyfikowany jako człowiek, który siedzi tu i tu, wygląda tak i tak, ma takie to a takie cechy i je zupę.

---

[165] A. Krasuski, *Ochrona danych osobowych na podstawie RODO. Rozdział 3. PRZETWARZANIE DANYCH OSOBOWYCH. 3.1. Dane osobowe. 3.1.1. Kwalifikacja prawna informacji jako danych osobowych,* Warszawa 2018, Lex.

[166] L. Kępa, Ochrona danych osobowych w praktyce, Warszawa 2014, s. 39.

[167] L. Kępa, *loc. cit.*

[168] L. Kępa, *op. cit.* s. 41.

W swoistą pułapkę wpadł L. Kępa jeśli chodzi o odróżnienie danych osobowych od informacji, które danymi osobowymi nie są. Autor ten przez 22 strony swojej książki rozważa, czy takie to a takie kategorie danych są danymi osobowymi czy nie. Zależnie od konkretnych przykładów L. Kepa dochodzi do jednego z dwóch możliwych wniosków, a mianowicie że konkretna informacja stanowi dane osobowe lub że ich nie stanowi. Nie widzę powodu by powtarzać lub cytować rozważania L. Kepy, zwracam jedynie uwagę, że samo zastanawianie się czy dana kategoria danych to dane osobowe czy nie, to pułapka, bowiem odpowiedź na tak zadane pytanie może być fałszywie negatywna lub fałszywie pozytywna. Jedyna właściwa odpowiedź, w skrócie brzmi „to zależy". To zależy od faktu czy konkretny administrator lub odbiorca jest w stanie połączyć dane informacje, będące przedmiotem oceny, z konkretną osobą fizyczna czy nie. Co ciekawe po 22 stronach zmagań z konkretnymi kategoriami danych, zauważył to wspomniany L. Kępa i napisał: *(...) określone informacje stanowić będą dane osobowe wtedy, gdy osoby, które mają do nich dostęp będą miały możliwość ustalić tożsamość osoby, której dane dotyczą (...)*[169]. Dalej, ponieważ poruszamy się w poprzednim stanie prawnym, autor napisał: *oczywiście bez „zbytniego nakładu"*[170]), dziś mówimy tu o rozsądnym sposobie.

[169] L. Kępa, *op. cit.* s. 65.

[170] L. Kępa, *loc. cit.*

Artykuł 4. pkt 2 RODO

„przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

1. Art. 4 pkt 2. Komentarz

Przez przetwarzanie należy rozumieć każdą czynność wykonywaną na danych osobowych od ich zebrania do ich zniszczenia łącznie z ich zbieraniem i z ich niszczeniem.

Powyższe krótkie zdanie oddaje całość znaczenia definicji przetwarzania danych osobowych. Prawodawca pozornie definiuje jedynie „przetwarzanie", jednak z treści definicji wynika, że w istocie definiowane jest „przetwarzanie danych osobowych.

Definicję przetwarzania danych osobowych można też rozumieć niejako od drugiej strony, a mianowicie, że nie ma takiej czynności na danych osobowych, która nie jest przetwarzaniem tych danych. [171]

2. Art. 4 pkt 2. Analiza

Ze słów: „„„**przetwarzanie**" **oznacza** (..)" wynika, że przepis statuuje znaczenie pojęcia „przetwarzanie", pojęcie „przetwarzanie" należy rozumieć tak jak zdefiniowano w tym przepisie[172]. Prawodawca definiuje przetwarzanie w sposób nie budzący wątpliwości, że czynność ta dotyczy danych osobowych, w związku z czym dziwić może, że w przepisie zdefiniowano *przetwarzanie* nie zaś „przetwarzanie

[171] Podobnie: L. A. Bygrave, L. Tosoni *op. cit.* s. 119.

[172] M Zirk-Sadowski *loc. cit.*

danych osobowych"[173]. (Szerzej: *3.1. Art. 4 pkt 2. Uwaga 1. Przetwarzanie, przetwarzanie danych, przetwarzanie danych osobowych. Wątpliwość w kwestii pojęcia definiowanego*).[174]

Ze słów: „**oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych** (...)" wynika, że przetwarzanie to operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych. Użycie słowa „operacja" (dokładnie: *operacji*) w polskiej wersji RODO jest błędem tłumaczenia. W wersji angielskiej użyto słowa *operation*, które, owszem, oznacza operację wojskową, chirurgiczną, ale oznacza też czynność.[175] Przetwarzanie to zatem czynność wykonywana na danych osobowych. Jeśli chodzi o słowa *lub zestaw czynności*, to słowa te niestety nie ułatwiają zrozumienia definicji. Nie wiadomo, a nie wiadomo ponieważ przepis nie daje ku wiedzy wskazówek, ile czynności co najmniej składa się na zestaw czynności (operacji). Czy dwie czynności to zestaw, czy może dopiero trzy, a może pięć lub siedemnaście. Nie wiadomo.

Wiadomo jednak co innego, że już jedna czynność, o czym pisze wyżej, jest przetwarzanie danych osobowych. Skoro więc już jedna czynność jest przetwarzaniem, to nie ma znaczenia czy rozumiane jako zestaw dwie czynności stanowią jedną czynność, ponieważ stanowią zestaw, czy stanowią dwie, zestawione czynności.

---

[173] Na brak słowa *osobowych* zwrócił uwagę W. Chomiczewski, twierdząc, że brak tego słowa *Pozostaje (...) jednak bez wpływu na samo znaczenie pojęcia, ponieważ z przepisu art. 4 pkt 2 w sposób jednoznaczny wynika, że przetwarzanie dotyczy danych osobowych* (podkreślenie W. Chomiczewskiego). W. Chomiczewski w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 186.

[174] Zawartość warstwy „Analiza" została wykorzystana i w znacznej mierze zacytowana w publikacji: J. Rzymowski op. cit. s. 25-30. Książki tej nie wskazuję jako źródła cytatu, bowiem niniejsza publikacja powstawała wcześniej. Założeniem było, by nie prowadzić wywodów równoległych. Pisząc książkę o dokumentacji skorzystałem z analizy dwóch definicji przygotowanej pod kątem niniejszej publikacji. Publikacja o dokumentacji jest, w pewnym sensie, publikacją pochodną wobec niniejszej i równolegle powstających, tyle, że wydaną wcześniej.

[175] https://translate.google.com/?hl=pl#view=home&op=translate&sl=en&tl=pl&text=operation (dostęp 2020.02.27. godz. 22.20), https://pl.bab.la/slownik/angielski-polski/operation, (dostęp 2020.02.27. godz. 22.19)

Można próbować uzasadniać wprowadzenie do przepisu kategorii „zestaw czynności" (dokładnie: *zestaw operacji*). Można stwierdzić, że wprowadzenie tej kategorii ma ułatwić na przykład upoważnianie do przetwarzania danych osobowych (pomijam kwestię wątpliwej sensowności upoważniania na podstawie RODO). Można, można też jednak, a w zasadzie należy, stwierdzić, że wprowadzenie „zestawu czynności" (dokładniej: „zestawu operacji") obok czynności nie ma realnego znaczenia praktycznego, nie ułatwia nic w interpretacji, jest więc błędem.

Ze słowa podkreślonego: „(...) operację **lub** zestaw operacji (...)" wynika, że przetwarzaniem jest zarówno jedna operacja, jak i ich wiele jak i połączenie jednej i wielu (pomijam fakt, że jedna i wiele czyni odrobinę więcej niż wiele, ale o bezsensowności ujęcia: operacja/zestaw operacji piszę wyżej).

Ze słów: „(...) **wykonywanych na danych osobowych lub zestawach danych osobowych** (...)" wynika, że przetwarzaniem danych osobowych są czynności wykonywane na danych osobowych właśnie jak również czynności wykonywane na zestawach danych osobowych. Jeżeli jakaś czynność nie jest wykonywana na danych osobowych ani na zestawach danych osobowych to nie jest przetwarzaniem (danych osobowych).

Niestety i w odniesieniu do danych osobowych i ich zestawów uczyniono to samo co w odniesieniu do operacji i ich zestawów. Nie wiadomo jaka jest różnica między danymi osobowymi a zestawami tych danych. Być może dwie informacje to dane osobowe a trzy to już zestaw (odsyłam do wywodów prowadzonych w odniesieniu do art. 4 pkt 1 RODO) ale być może zestaw to dopiero cztery informacje. A może zestaw to dopiero sześć czy zgoła osiem informacji bo może par danych osobowych (co i kogo dotyczy) nie należy liczyć jako dwie informacje ale jako jedną. Itd. itd. Ta wyliczanka może trwać długo, uzasadnić też można różne poglądy, a to że zestaw to 2 dane, a to że trzy itd. Wyliczanka ani uzasadnianie nie mają jednak praktycznego sensu. W komentowanej definicji nic by się nie zmieniło gdyby słowa o zestawach danych osobowych nigdy się w niej nie znalazły. Wniosek nasuwa się sam, słowa o zestawach nie powinny się były w RODO znaleźć

Ze słów: „(...) w sposób **zautomatyzowany lub niezautomatyzowany**, (...) ” wynika, że przetwarzaniem danych osobowych są czynności wykonywane w jakikolwiek sposób. Prawodawca, jak widać, podzielił wszystkie możliwe czynności przetwarzania danych na dwie grupy. Jedna grupa to czynności zautomatyzowane, druga grupa to czynności niezautomatyzowane. Nie wiadomo co różni jedne od drugich. Prawodawca nie dał podstaw do rozróżnienia. Oczywiście w tej sytuacji należałoby sięgnąć do rozmaitych słowników, zwłaszcza technicznych, co pozwoliłoby na przeprowadzenie drobiazgowego pseudoprawniczego wywodu, opartego o znaczenie słowa „zautomatyzowany” albo „automatyzacja” lub pseudoerudycyjnego wywodu prowadzącego np. do sztuki R.U.R Karela Čapka. Nie czynię tego, ponieważ prawodawca podzielił wszystkie czynności na dwie grupy i jednocześnie zaliczył do przetwarzania każdą z czynności należącą do którejkolwiek z grup. W związku z tym nie ma znaczenia do której z grup – czy do czynności zautomatyzowanych, czy do czynności niezautomatyzowanych – należy dana czynność, nie ma też znaczenia co różni te grupy. i tu niestety wniosek też nasuwa się sam – podziału na czynności zautomatyzowane lub niezautomatyzowane, w ogóle nie powinno w komentowanym przepisie być, zaś podczas interpretacji przepisu, podział ten można, bez szkody dla poznania znaczenia przepisu, pomijać.

Innymi słowy, w zakresie definicji mieszczą się czynności zautomatyzowane i niezautomatyzowane, czyli wszystkie

Można sobie wyobrazić, że prawodawca podzielił wszystkie czynności wykonywane na danych osobowych na dwie kategorie – czynności wykonywane w sposób zautomatyzowany i w sposób niezautomatyzowany, po czym włączył do zakresu definicji zawartość obu kategorii. Po co w takim razie prawodawca dokonał podziału – nie jest to jasne.

Na temat różnicy między przetwarzaniem w sposób zautomatyzowany i niezautomatyzowany wypowiedzieli się L. A. Bygrave i L. Tosoni. Autorzy ci stwierdzili, że przetwarzanie w sposób zautomatyzowany to przetwarzanie *(...) by means of computer technologies (...)*[176] czyli: *z wykorzystaniem technologii komputerowych* zaś przetwarzanie w sposób inny niż zautomatyzowany to przetwarzanie *(...) executed*

[176] L. A. Bygrave, L. Tosoni, *loc. cit.*

by humans without the use of computing devices (...)[177], czyli: *wykonywane przez ludzi bez używania urządzeń komputerowych*.

Wobec takiego stanowiska, mam pewien dystans. Rozumiem, że porządkuje ono pewne sprawy. Jeśli administrator przetwarza dane osobowe „w sposób całkowicie lub częściowo zautomatyzowany" to przetwarzanie takie, na mocy art. 2 ust. 2 RODO, znajduje się w zakresie RODO. Twierdząc, że przetwarzanie danych osobowych w sposób zautomatyzowany, to przetwarzanie z użyciem sprzętu komputerowego, dokonujemy potężnego skrótu myślowego. Przecież administrator może przetwarzać dane osobowe z użyciem sprzętu komputerowego, jednak w sposób, który trudno nazwać zautomatyzowanym. Administrator może używać komputera jak maszyny do pisania – pisze w komputerze, drukuje drukarką. W takich sytuacjach pojawić się powinno pytanie o to czy w takich czynnościach dostrzegalna jest automatyzacja.

Rozumiem, że patrząc technicznie, możemy stwierdzić, że np. czynność zapisywania pociąga za sobą konieczność wykonywania przez komputer czynności w sposób automatyczny, na przykład automatycznego zapisu dokumentu, można to tak rozumieć, mam jednak wątpliwości. Idąc dalej, jeżeli wyobrazimy sobie bazę danych, administrator przechowuje w niej dane. Jeśli automatycznie odbywa się np. backup bazy – wtedy mamy do czynienia ze zautomatyzowanym przetwarzaniem, jeżeli jednak administrator wykonuje backup na zewnętrznym nośniku, na który kopiuje bazę, to mam wątpliwość czy mamy tu do czynienia ze zautomatyzowanym przetwarzaniem.

Jeżeli administrator przetwarza dane osobowe w sposób inny niż zautomatyzowany, jednak dane te stanowią część zbioru danych lub mają stanowić część zbioru danych, to takiego przetwarzania RODO dotyczy, co również wynika z art. 2 ust. 2 RODO – tu problem pojawia się na poziomie znaczenia pojęcia „zbiór" dlatego dalej tu tego nie rozwijam.

Utożsamienie przetwarzania danych w sposób zautomatyzowany z przetwarzaniem danych z wykorzystaniem sprzętu komputerowego zdaje się być ofiarą art. 2 ust. 2 RODO. Żeby art. 2 ust. 2 RODO łatwo interpretować, przetwarzanie w sposób zautomatyzowany bywa utożsamiane z z przetwarzaniem z wykorzystaniem sprzętu kompute-

[177] L. A. Bygrave, L. Tosoni, *loc. cit.*

rowego. Wydaje mi się, że jest to uproszczenie, które może prowadzić do pokrzywdzenia administratorów. Pokrzywdzenia, bowiem może to prowadzić do nałożenia kary administracyjnej na administratora, który przetwarza dane nie w zbiorze i które nie mają stanowić części zbioru i w sposób który rozumie jako niezautomatyzowany, jednak czyni to z wykorzystaniem komputera, tabletu, smartfona. Ponieważ administrator przetwarza dane z wykorzystaniem sprzętu komputerowego, to przetwarzanie takie może zostać uznane za przetwarzanie w sposób zautomatyzowany i tym samym przetwarzanie to znajdzie się w zakresie RODO, co może skutkować karą administracyjną ponieważ administrator który był przekonany że przetwarza dane poza zakresem RODO, nie realizował obowiązków wynikających z RODO uważał bowiem że obowiązki te na nim nie spoczywają.

Wydaje się, że pojęcie przetwarzania w sposób zautomatyzowany, wymaga głębokiego namysłu doktryny a może po prostu zdefiniowania w akcie prawnym

Ze słów: „**taką jak**" wynika, że w przepisie wymienione są przykładowe czynności przetwarzania danych osobowych.[178] Przykładowe ale nie wszystkie. Jeżeli zatem jakaś czynność jest wykonywana na danych osobowych ale nie jest wymieniona w przepisie, to też jest czynnością przetwarzania danych osobowych – po prostu przetwarzaniem.

Słowa zacytowane „**zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie**;" to przykładowe czynności przetwarzania danych osobowych.

Ciekawą uwagę znaleźć można w angielskiej, biznesowej publikacji na temat RODO, jej autorzy piszą otóż, że jeżeli ktoś wchodzi w kontakt z danymi to prawdopodobne jest, że ma on te dane

[178] Podobnie: P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s 197.

przetwarzać - *(...) any entity coming into contact with personal data is likely to be processing that data*.[179]

Na równie ciekawe zjawisko zwracają też uwagę w komentarzu do przepisu L. A. Bygrave i L. Tosoni. Autorzy ci piszą, że: *The GDPR is aimed at regulating all or most stages of the data processing cycle, including registration, storage, retrieval and dissemination of personal data.*[180], czyli: *RODO jest skierowane na regulowanie wszystkich lub większości stadiów cyklu przetwarzania danych, włączając rejestrację, przechowywanie, pobieranie, rozpowszechnianie danych osobowych*[181]. Przez lata byłem przekonany i nadal jestem, że przetwarzanie danych osobowych to każda czynność wykonywana na danych osobowych. W myśli wskazanych autorów widzę szczególną wartość dlatego, że dostrzegli oni, że nie tylko każda czynność (o czym nie piszą) jest przetwarzaniem, ale że RODO dotyczy przetwarzania danych osobowych na każdym etapie i że dostrzegli, że wynika to właśnie z definicji przetwarzania.

Ze słów podkreślonych: „(...) **zbieranie** (...) **niszczenie**;" wynika, że prawodawca ułożył przykładowe czynności przetwarzania w sposób bardzo rozsądny. Jako pierwszą czynność wskazano *zbieranie*, jako ostatnią czynność wskazano *niszczenie*. Zebranie danych osobowych to czynność graniczna. Rozgranicza ona stan, w którym administrator nie przetwarza danych osobowych od stanu, w którym te dane przetwarza. Kolejność wygląda więc tak, że najpierw administrator nie przetwarza danych osobowych, następnie administrator zbiera dane osobowe, następnie administrator przetwarza dane osobowe.

Niezwykle ciekawą rzecz zauważył K. Wygoda[182], że można wyróżnić czynną i bierną formę zbierania danych osobowych. K. Wygoda pisze co prawda, że formy te da się wyróżnić teoretycznie, z czym się nie zgadzam, ponieważ w praktyce, jak najbardziej, czasem

[179] Steptoe and Johnson LLP. *Commentary on the General Data Protection (GDPR)* by Steptoe and Johnson LLP for BIPAIR *The GDPR from an insurance and financial mediation perspective,* July 2016. s. 16.

[180] L. A. Bygrave, L. Tosoni, *op. cit.* s. 117.

[181] Tłumaczenie: J. Rzymowski.

[182] K. Wygoda w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 81.

administrator jest aktywny przy zbieraniu danych, czasem nie, czyli formy te można wyróżnić nie tylko teoretycznie ale i w praktyce.

3. Art. 4 pkt 2. Uwagi
3.1. Art. 4 pkt 2. Uwaga 1. Przetwarzanie, przetwarzanie danych, przetwarzanie danych osobowych. Wątpliwość w kwestii pojęcia definiowanego

W art. 5 pkt 2 RODO zdefiniowano „przetwarzanie". Nie zdefiniowano przetwarzania danych, nie zdefiniowano przetwarzania danych osobowych, ale zdefiniowano samo właśnie *przetwarzanie*.

Na brak słowa „osobowych" zwrócił uwagę W. Chomiczewski[183], twierdząc, że brak tego słowa *Pozostaje (...) jednak bez wpływu na samo znaczenie pojęcia, ponieważ z przepisu art. 4 pkt 2 w sposób jednoznaczny wynika, że* ***przetwarzanie dotyczy danych osobowych*** (podkreślenie W. Chomiczewskiego). Nie sposób się nie zgodzić z tezą postawioną przez W. Chomiczewskiego, jednak trzeba zwrócić uwagę na to, że jest ona trafna, ponieważ pojęcie przetwarzania po prostu bardzo dokładnie zdefiniowano i to właśnie z tej definicji wynika dokładnie jego znaczenie. Z samego słowa „przetwarzanie" w żaden sposób nie wynika, że owo przetwarzanie to przetwarzanie danych osobowych.

Pierwszy zarzut, który stawiam tu prawodawcy, to fakt, że manewr ze skróceniem „przetwarzania danych osobowych", bo tak powinno brzmieć to pojęcie, do „przetwarzania" powoduje, że pojęcie definiowane jest po prostu niejasne. Fakt, wiadomo, że dotyczy ono danych osobowych, ale wiadomo to z definicji, czyli prawodawca w definicji wyjaśnił to co w pojęciu definiowanym zaciemnił. Z zarzutem tym można się nie zgadzać, rozważania nad tym czy akty prawne powinny być proste i zrozumiałe, czy powinny przypominać niezrozumiałe mamrotania szamanów, przekraczają jednak ramy niniejszego rozważania.

[183] W. Chomiczewski, *loc. cit.*

3.2. Art. 4 pkt 2. Uwaga 2.
Przetwarzanie danych osobowych.
Kolejna wątpliwość w kwestii pojęcia definiowanego

Kolejny zarzut, który stawiam tu prawodawcy, jest poważniejszy. Przetwarzanie to zdaniem prawodawcy: *operacja „lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych (...)*, niestety podczas końcowej redakcji RODO (ufam bowiem, że taka miała miejsce) nie ustrzeżono się przed pozostawieniem zestawień: *przetwarza dane osobowe* i *przetwarzaniu danych osobowych*. Wyglądają one niegroźnie. Niegroźnie do momentu, kiedy uświadamiamy sobie, że samo przetwarzanie zdefiniowano w art. 4 ust. 1 pkt 2 RODO. Wynika więc z tego, że „przetwarzanie danych osobowych" to w istocie: <<operacja „lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych (...)"danych osobowych (sic!)>>, zaś „przetwarza dane osobowe" to w istocie: <<dokonuje operacji lub zestawu operacji na danych osobowych lub zestawach danych osobowych (pomijam resztę definicji) danych osobowych (sic!)>>. Używając zasady argumentum ad absurdum[184] można oczywiście posprzątać ten nieład, uważam jednak, że zasada ta nie powinna być używana jako odkurzacz do uprzątania redakcyjnego śmietnika w aktach prawnych.

Różnicę między przetwarzaniem danych a przetwarzaniem danych osobowych zauważył[185] M. Bochenek. Autor ten dokonał jednak przedziwnych podstawień. *Przetwarzanie danych* autor ten zdefiniował tak, jak jest zdefiniowane *przetwarzanie* w art. 4 pkt 2 RODO, czyli dokonał interpretacji pojęcia definiowanego przy zachowaniu treści definicji. *Przetwarzanie danych osobowych* M. Bochenek zdefiniował jako *wszelkie operacje w rozumieniu art. 4 pkt 2 RODO wykonywane przez osoby przetwarzające powierzone dane osobowe.*[186]. Widać, że autor zmaga się z pojęciami, niepotrzebnie przy tym wprowadza słowa *powierzone dane osobowe*. Jeśli z jakichś powodów obie te definicje były potrzebne M. Bochenkowi, to powinien był on pominąć słowo *powierzone*, jego obecność budzi bowiem niepokój, że

[184] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 150.

[185] M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach,* Warszawa 2019, Lex.

[186] M. Bochenek, *op. cit.*

być może przetwarzanie danych to czynności na danych a przetwarzanie danych osobowych to te same czynności wykonywane przez podmioty przetwarzające. Należy podkreślić, że takie rozróżnienie jest kuriozalne. Jedocześnie należy uczciwie przyznać M. Bochenkowi, że starał się uporządkować prawny nieład w zakresie pojęcia definiowanego i jego definicji w art. 4 pkt 2 RODO.

3.3. Art. 4 pkt 2. Uwaga 3. Przechowywanie danych osobowych jako przetwarzanie danych osobowych

Słowo: „**przechowywanie**" widniejące wśród przykładowych czynności przetwarzania wskazuje na fakt, że przechowywanie jest niewątpliwie, bo wymienione przez prawodawcę, czynnością przetwarzania. Innymi słowy, ADO który przechowuje dane osobowe, już samym przechowywaniem je przetwarza. Przechowywanie nie jest oczywistą czynnością przetwarzania. Kiedy mówimy o przetwarzaniu danych osobowych, to nasuwa nam się obraz urzędników, którzy pilnie wykonują swoje czynności związane z danymi, zbierają te dane, kopiują je, udostępniają, jednym słowem, - opracowują. Tu właśnie kryje się pułapka. Słowo „przetwarzanie" ma w sobie pewną semantyczną inercję, jednak utożsamiając je z opracowywaniem, popełniamy błąd. Przez przetwarzanie danych osobowych należy rozumieć, co napisałem na początku komentarza do przepisu, każdą czynność wykonywaną na danych osobowych od ich zebrania do ich zniszczenia łącznie z ich zbieranie i z ich niszczeniem. Każda czynność, w tym też czynności, których instynktownie nie nazwalibyśmy przetwarzaniem jak niszczenie czy przechowywanie.

W kwestii przechowywania, niezwykle ciekawa konstatacja została sformułowana przez K. Wygodę. Autor ten pisze: *(...) Bez względu na długość okresu przechowywanie występuje zawsze, gdy dojdzie do uprzedniego utrwalenia zebranych danych na dowolnym nośniku.*[187]. Myśl ta wydaje się oczywista, skoro administrator utrwalił dane, to oczywiste jest, że je przechowuje, jednak odkrywczość cytowanej myśli leży w tym, że przechowywanie danych jest kojarzone z ich archiwizacją, przechowywaniem kopii itd., podczas gdy czas nie ma dla przechowywania znaczenia. Administrator zapisał dane to zna-

[187] K. Wygoda, *op. cit.* s. 83.

czy, że administrator je przechowuje. Ma to znaczenie dla określenia zakresu obowiązku prowadzenia RCPD. Nie da się danych przechowywać sporadycznie. Zwłaszcza jeżeli są to dane pracowników lub klientów administratora. Obowiązek wieloletniego przechowywania tych danych wynika z przepisów szczególnych. Skoro (w zasadzie) nie da się danych przechowywać sporadycznie, to każdy administrator, który dane przechowuje, powinien prowadzić RCPD. Wniosek ten jest w mojej ocenie absurdalny.

3.4. Art. 4 pkt 2. Uwaga 4.
Operation a czynność

Z tego, że przetwarzanie danych osobowych oznacza operację lub zestaw operacji nie należy wyciągać wniosków, zgodnie z którymi przetwarzanie to czynność skomplikowana. Słowo „operacja", które znajduje się w definicji jest niczym innym jak tylko nieumiejętnym tłumaczeniem angielskiego słowa „operation".

Oprogramowanie „google translator" jako pierwsze tłumaczenie słowa *operation* na język polski podaje słowo: *operacja*. Jednak to samo oprogramowanie, jako definicję słowa *operation* podaje: *the fact or condition of functioning or being active*, czyli (tu już tłumaczę sam) „zdarzenie lub stan funkcjonowania lub bycia aktywnym". Czyli jest tu pewna niekonsekwencja. Niekonsekwencja jest tym głębsza, że jako pierwszy synonim słowa *operacj*a, „google translator" podaje: *działanie*, które z kolei tłumaczy na: *action, operation, work, acting, working, effect*. Rozważania te można prowadzić długo, sięgając do innych słowników, oraz innych wersji językowych RODO. Można, jednak nie uważam tego za celowe. Uważam za to, że z użycia słowa: *operacja* nie należy próbować wyciągać wniosków, że przetwarzanie danych osobowych to czynność skomplikowana, bowiem takie tylko zasługują na miano operacji, a nie jakakolwiek, ponieważ operacja to właśnie taka jakakolwiek czynność.

3.5. Art. 4 pkt 2. Uwaga 5.
Operacja a zestaw operacji

Niestety, jeśli chodzi o analizowaną definicję, to nie dość nieszczęść z tłumaczeniem, reszta definicji również hołduje zasadzie niedbałej legislacji. Przetwarzanie to operacja lub zestaw operacji. Można by się próbować zastanawiać co różni operację - czynność od zesta-

wu operacji - czynności, gdzie jest granica. Można by, lecz byłby to trud niepotrzebny. W definicji przyjęto, że czynności występują pojedynczo (operacja) i zbiorowo (zestaw operacji) jednak ani nie zdefiniowano zestawu czynności ani nie wskazano różnicy miedzy czynnością a zestawem czynności. Z praktycznego punktu widzenia nie ma to znaczenia, ponieważ zarówno wszystkie operacje jak i wszystkie zestawy operacji na danych osobowych zaliczają się do przetwarzania danych osobowych. Z punktu widzenia zasady przyzwoitej legislacji – słowa o zestawie operacji są w definicji po prostu niepotrzebne. Nie ma znaczenia różnica między operacją a zestawem operacji, czyli między czynnością a zestawem czynności, ponieważ już jedna czynność jest przetwarzaniem danych osobowych.[188]

3.6. Art. 4 pkt 2. Uwaga 6.
Zbędność słów o zestawie w definicji

Nie ma znaczenia różnica między danymi osobowymi a zestawami danych osobowych. Nie jest, dla zakresu przetwarzania danych osobowych istotne czy czynność jest wykonywana na danych czy na zestawie danych. Czynność wykonywana na danych jest ich przetwarzaniem. Oczywiste jest, że i czynność wykonywana na większych ilościach danych osobowych jest przetwarzaniem danych osobowych. Słowa o zestawie, w komentowanym przepisie są niepotrzebne i mylące. Można próbować obronić fakt, że słowa o zestawie jednak są w przepisie. Możliwy do użycia jest tu argument, że jeżeli ktoś wykonuje czynność na zestawie danych osobowych, bez zapoznawania się z tymi danymi, to dzięki temu, że w przepisie są słowa o zestawie – czynność ta jest przetwarzaniem danych osobowych. Niestety argument taki jest nietrafiony – czynność na zestawie to też czynność na danych czyli jeżeli ktoś wykonuje czynność na zestawie danych, to jakby przetwarzał dane podwójnie. Podwójnie bo wykonuje zarówno operację na danych jak i na zestawie danych. W związku z tym podtrzymuję pogląd o zbędności w przepisie słów o zestawie.

[188] W przepisie powinno być użyte słowo: „czynność”

3.7. Art. 4 pkt 2. Uwaga 7.
Dane osobowe a dana osobowa

Należy też zwrócić uwagę, że jeżeli patrzymy na dane osobowe z punktu widzenia poprawnego języka polskiego lub angielskiego, to dane te występują tylko niepojedynczo. W języku polskim mamy „dane", w języku angielskim spotykamy: „data". W języku angielskim jeżeli chcemy wskazać, na jedna informację o charakterze danych osobowych możemy użyć zwrotu: „a piece of data", w poprawnym języku polskim nie ma czego użyć w tej sytuacji. Należy więc chyba odejść od poprawności językowej i swobodnie używać określenia: „dana osobowa".

3.8. Art. 4 pkt 2. Uwaga 8.
Nadmiar nazw na określenie czynności

Na marginesie, warto zwrócić uwagę na jeden jeszcze problem. Jak wiadomo: *Bez uzasadnionych powodów nie powinno się przypisywać różnym terminom tego samego znaczenia*[189] – zasada ta nosi nazwę zakazu wykładni synonimicznej. W art. 4 ust 2 RODO znajdujemy: *przetwarzanie*, *operację* i *zestaw operacji*; w art. 11 ust. 1 RODO mowa jest o „przetwarzaniu danych osobowych" (dokładnie, że: *(...) administrator przetwarza dane osobowe (...)*), podobnie w art 13 ust. 1 lit. c RODO mowa jest o „przetwarzaniu danych osobowych"; w tytule art. 30 RODO mowa jest o „czynnościach przetwarzania" (co prawda w samym przepisie o nich zapomniano, ale w tytule i w art. 30 ust. 1 RODO – w części wprowadzającej przepisu - są obecne); w art. 30 ust. 2 RODO, w części wprowadzającej jest mowa o kategoriach czynności; w art. 30 ust. 2 lit. b RODO mowa jest o „kategoriach przetwarzań" (to jest akurat błąd tłumaczenia, ponieważ w wersji angielskie zarówno w części wprowadzającej art. 30 ust. 2 RODO jak i w art. 30 ust. 2 lit. b RODO mowa jest o the *cathegories of processing*. Po kolei wygląda to jeszcze straszniej: przetwarzanie, operacja, zestaw operacji, przetwarzanie danych osobowych, czynność przetwarzania, kategorie czynności, wreszcie (choć tylko w polskiej wersji) kategorie przetwarzań. Analiza tego nazewniczego bogactwa prowadzi do jednego tylko wniosku – ktoś to powinien zre-

[189] M. Zirk-Sadowski, *Problemy wykładni językowej w prawie administracyjnym.,* w: *System Prawa Administracyjnego tom IV. Wykładnia w prawie administracyjnym.* Red: R Hauser, Z Niewiadomski, A. Wróbel, Warszawa 2012, s. 200.

dagować, ustalić jedną nazwę dla stanu w którym ktoś coś robi z danymi osobowymi, po czym tej nazwy w RODO konsekwentnie się trzymać. Szkoda, że nie zrobił tego prawodawca.

3.9. Art. 4 pkt 2. Uwaga 9.
Brak odpowiednika słowa: *any* w polskiej wersji definicji

Na marginesie prowadzonych rozważań należy poczynić jeszcze uwagę z pogranicza wykładni prawa, tworzenia aktów prawnych i translatoryki.

Początek przepisu w języku polskim stanowi: *„przetwarzanie" oznacza operację (...)*. Ten sam fragment przepisu w języku angielskim stanowi: *'processing' means any operation*. Ten sam fragment przepisu w języku czeskim stanowi: *„zpracováním" jakákoliv operace*. Widać, że w wersji polskiej pominięto odpowiednik słów: *any*, *jakákoliv* czyli jakaś, jakakolwiek. Pierwszy wniosek jaki sie nasuwa, to konieczność uzupełnienia polskiej wersji przepisu o odpowiednik słów: *any*, *jakákoliv*. Analiza wersji słowackiej *„spracúvanie" je operácia* stawia ten wniosek pod znakiem zapytania – brak jest odpowiednika słowa: *any*. Z kolei analiza wersji słoweńskiej: *„obdelava" pomeni vsako dejanje* sugeruje, że jednak odpowiednik słowa *any* w przepisie być powinien, ponieważ jest nim tu słowo: *vsako*. Podobnie wersja włoska stanowi: *«trattamento»: qualsiasi operazione* – tu oczywiście kluczowe jest słowo: *qualsiasi* – dowolny. Jak widać przeważa, przynajmniej we wskazanych wersjach językowych, wersja zawierająca odpowiednik słowa: *any*.

Oczywiście uprawnione jest stwierdzenie, że słowo „operacje" znaczy mniej więcej to samo co słowa: „jakiekolwiek operacje" czy: „wszelkie operacje", jednak oceniając sprawę z punktu widzenia języka prawnego, trzeba uczciwie stwierdzić, że o ile może znaczy to mniej więcej to samo, to jednak nie dokładnie to samo.

Skłania mnie to do postawienia postulatu o konieczności dodania uzupełnienia przepisu. Uważam, że przemawia za tym postulatem jedno jeszcze rozumowanie. Otóż podobnej konstrukcji jak przepis komentowany jest art. 4 pkt 1 RODO czyli definicja danych osobowych. Przepis ten zrazu zaczynał się w języku polskim słowami: *„dane osobowe" oznaczają informacje o*, w języku angielskim przepis ten zaczynał się słowami: *'personal data' means any information*. Jak widać w wersji angielskiej w definicji danych osobowych widnieje

any information, w wersji polskiej: *informacje*. Podobnie jak w definicji przetwarzania, w wersji angielskiej, przypominam, widnieje: *any operation*, w wersji polskiej *operację*. Czyli o ile wersja angielska i polska obydwu definicji do siebie nie przystają, to nie przystają konsekwentnie. Tu można tylko powtórzyć rozumowanie, zgodnie z którym „any information" znaczy mniej więcej to samo co: „informacje" zaś „any operation" znaczy mniej więcej to samo co „operację". Wersje nie są może swój idealnym odbiciem, ale są bardzo bliskie znaczeniowo. Tak mogłoby zostać. Nie zostało. Otóż wydano sprostowanie do RODO[190], w którym poprawiono wersję polską definicji danych osobowych, obecnie analizowane słowa brzmią następująco: *oznaczają wszelkie informacje*. Wnioskujemy z tego, że prawodawca uznał, że jeśli chodzi o polski odpowiednik zwrotu „any operation", to lepszym odpowiednikiem niż „informacje" jest „wszelkie informacje". Zmiana ta wydaje się właściwa. Zagadką pozostaje, dlaczego podobnego rozwiązania nie zastosowano w przypadku definicji przetwarzania danych osobowych, którą, jak uważam, również powinno się uzupełnić.

Na marginesie prowadzonych rozważań zwracam uwagę, że L. A. Bygrave i L. Tosoni, twierdzą, że słowo *any* jest istotne ponieważ *reflects the intention of the legislature to make it technologically neutral in order to prevent risks of circumvention, and to ensure the applicability of the GDPR irrespective of the techniques used to process data*[191] czyli: *jest odbiciem intencji prawodawcy uzyskania technologicznej neutralności aby zapobiec ryzyku obchodzenia przepisów i aby zapewnić możliwość zastosowania RODO, niezależnie od technik używanych do przetwarzania danych*[192].

Zwracam uwagę na ten pogląd, uważam powiem, że pogląd taki, wyrażony przez autorów, którzy jak mniemam, nie znają polskiej wersji językowej, wskazuje na doniosłość słowa *any*. Niestety

[190] Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dziennik Urzędowy Unii Europejskiej L 119 z dnia 4 maja 2016 r.)

[191] L. A. Bygrave, L. Tosoni, *loc. cit*.

[192] Tłumaczenie: J. Rzymowski.

legislator, tłumacz czy redaktor nie dostrzegali tej doniosłości, nad czym pozostaje ubolewać.

4. Art. 4 pkt 2. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 2 RODO definiuje dane osobowe, zatem zgodnie z dyrektywą języka prawnego[193], każdy kto interpretuje RODO powinien rozumieć pojęcie „przetwarzanie" tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „przetwarzanie" tak jest ono zdefiniowane w art. 4 pkt. 2 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „przetwarzanie" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 2. Konkretyzacja zasad

Znaczenie pojęcia „przetwarzanie" jest istotne w kontekście rozumienia zasad z art. 5 RODO. Jest istotne, ponieważ zasady te to „Zasady dotyczące przetwarzania danych osobowych" – tak stanowi tytuł przepisu. W związku z tym, znaczenie art. 5 RODO, znaczenie zasad ustanowionych w tym przepisie, jest ściśle związane ze znaczeniem pojęcia „przetwarzanie".

Zasady ustanowione w art. 5 RODO dotyczą właśnie przetwarzania, czyli czynności wykonywanych na danych osobowych. Zasady te nie odnoszą się do danych osobowych, ale do ich przetwarzania. Zwracam uwagę, że nie są to zasady dotyczące ochrony danych, zasady dotyczące danych osobowych, ale właśnie zasady dotyczące **przetwarzania** danych osobowych.

[193] M. Zirk-Sadowski, *op. cit.* s. 199.

6. Art. 4 pkt 2. Postulaty de lege ferenda

6.1 Art. 4 pkt 2. Postulat 1. Uzupełnienie pojęcia definiowanego

Uzupełniając rozważania prowadzone w uwadze 3.1. Art. 4 pkt 2. Uwaga 1. Przetwarzanie, przetwarzanie danych, przetwarzanie danych osobowych. Wątpliwość w kwestii pojęcia definiowanego, uważam, że art. 4 pkt 2 powinien zostać poprawiony w ten sposób, że zamiast definiować przetwarzanie, powinien on definiować „przetwarzanie danych osobowych". Tak byłoby po prostu jaśniej.

6.2 Art. 4 pkt 2. Postulat 2. Usunięcie fragmentu definicji

W uwadze *3.1. Art. 4 pkt 2. Uwaga 5. „Operation" a czynność* zaprezentowałem wniosek, zgodnie z którym, różnica między operacją a zestawem operacji jest nieistotna ponieważ jest niemożliwa do wskazania. W związku z tym, z przepisu należy usunąć słowa „lub zestaw operacji" skoro i tak nic istotnie merytorycznego do treści przepisu nie wnoszą.

6.3.Art. 4 pkt 2. Postulat 3. Usunięcie fragmentu definicji

Podobnie jak nieistotna bo jest różnica miedzy operacja a zestawem operacji, tak samo nieistotna bo niemożliwa do wskazania jest różnica między danymi osobowymi a zestawami danych osobowych. Wniosek jest oczywiście również analogiczny. z przepisu należy zatem usunąć słowa: „**lub zestawach danych osobowych**".

6.4. Art. 4 pkt 2. Postulat 4. Usunięcie fragmentu definicji

Jak wskazałem wyżej w przepisie, nie wiadomo co różni czynności zautomatyzowane od czynności niezautomatyzowanych. o ile nawet, na drodze badania słowników, można by to z trudem ustalić, to różnica ta dla jest nieistotna dla znaczenia przepisu. W związku z tym, z przepisu powinny zostać usunięte słowa: „(...) w sposób **zautomatyzowany lub niezautomatyzowany**, (...) "

6.5. Art. 4 pkt 2. Postulat 1+2+3+4=5.
Propozycja nowej treści definicji

Uwzględnienie postulatów dotyczących poprawienia definicji przetwarzania (danych osobowych) skutkuje możliwością przedstawienia spójnej propozycji poprawionego przepisu. Powinien on wyglądać następująco: „„przetwarzanie **danych osobowych**" oznacza operację ~~lub zestaw operacji w~~ykonywan**a**~~ych~~ na danych osobowych ~~lub zestawach danych osobowych~~ w sposób ~~zautomatyzowany lub niezautomatyzowany~~, taką jak (...)". (Korzystając z możliwości jakie daje współczesna technika składu tekstu, wyrazy do usunięcia z przepisu oznaczyłem czcionką przekreśloną a wyrazy dodane oznaczyłem czcionką wytłuszczoną i podkreśloną.).

6.6. Art. 4 pkt 2. Postulat 6.
Rozważania meta o postulatach

W uwadze *3.1. Art. 4 pkt 2. Uwaga 9. Brak odpowiednika słowa: „any" w polskiej wersji definicji.* prowadzę rozważania nad tym, że w wersji angielskiej RODO w definicji danych osobowych napotykamy *'personal data' means any information relating to an identified or identifiable natural person*.
W wersji polskiej napotykamy: *„dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej*. Postuluję uzupełnienie polskiej wersji definicji o odpowiednik słowa: „any".

Ostateczna wersja przepisu, gdyby go modyfikowano, zależałaby od tego ile z zaproponowanych tu postulatów uwzględniono by. Najdalej idąca i moim zdaniem najlepsza wersja przepisu uwzględniałaby wszystkie postulaty: postulat 1+2+3+4+5=6a

6.7. Art. 4 pkt 2. Postulat 6a.
Propozycja treści definicji

Dodanie postulatów dotyczących poprawienia definicji przetwarzania (danych osobowych) skutkuje możliwością przedstawienia spójnej propozycji poprawionego przepisu. Powinien on wyglądać następująco: „„przetwarzanie danych osobowych" oznacza **każdą** operację wykonywaną na danych osobowych, taką jak (...)". (Przepis podaję w wersji wyprowadzonej z postulatu 5.).

6.8. Art. 4 pkt 2. Postulat 6b.
Propozycja treści definicji

Zmiany proponowane w postulacie *6.7. Art. 4 pkt 2. Postulat 6a. Propozycja treści definicji.* idą daleko. O ile uważam, że należy kołatać natrętnie w drzwi prawodawcy, nawet wtedy a może zwłaszcza wtedy, gdy prawodawca tworzy akty prawne w sposób niekompetentny lub niedbały, o tyle mam świadomość, że akty prawne piszą ludzie. Ponieważ ludzie piszą akty prawne, to nie wyobrażam sobie legislatorów, którzy przyznają się, że prosta definicja, pojęcia znanego od dziesiątek lat, zawiera 4 zasadnicze błędy i jeden mniejszy, translatorski – w wersji polskiej. Mając tę niewesołą świadomość postuluję, nieco wbrew sobie, by dokonano w wersji polskiej RODO, poprawki poprzez dodanie odpowiednika słowa: „any". Tak po spartańsku poprawiony przepis wyglądałby: „„przetwarzanie" oznacza każdą operację lub zestaw operacji wykonywanych (...)". (Czcionką wytłuszczoną oznaczono słowo dodane do przepisu.)

7. Art. 4 pkt 2. Rozważania historyczne.
7.1. Art. 4 pkt 2. Rozważanie 1.
Odpowiedniki w dawnej legislacji

Odpowiednikiem art. 6 ust. 1 RODO jest art. 2 lit. b Dyrektywy 95/46/WE i art. 7 pkt 2 UODO97.

7.2. Art. 4 pkt 2. Rozważanie 2.
Przetwarzanie krótkotrwałe

Ciekawą obserwację poczynił M. Gumularz, autor ten zwrócił uwagę na fakt, że przepisy UODO97 „przewidywały ograniczenie ich stosowania w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddawanych anonimizacji" [194] i że przepisy RODO ograniczenia takiego nie przewidują. Rozwijając myśl M. Gumularza, należy dodać, że tym samym poziom ochrony danych osobowych został podniesiony.

[194] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział II. POJĘCIE DANYCH OSOBOWYCH. 2. Podziały danych osobowych i ich praktyczne konsekwencje. 2.5. Krótkotrwałe i długotrwałe przetwarzanie danych,* Warszawa 2018, Lex.

Artykuł 4 pkt 3 RODO.

„ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

1. Art. 4 pkt 3. Komentarz

Przez „ograniczenie przetwarzania" należy rozumieć oznaczenie danych osobowych. Ograniczenie przetwarzania danych osobowych to czynność prowadzona w pewnym celu. Celem tym jest ograniczenie przetwarzania danych osobowych w przyszłości.

Powyższe krótkie zdanie oddaje całość znaczenia definicji przetwarzania danych osobowych. Prawodawca pozornie definiuje jedynie „ograniczenie przetwarzania", jednak z treści definicji wynika, że w istocie definiowane jest „ograniczenie przetwarzania danych osobowych".

Więcej o ograniczeniu przetwarzania można się dowiedzieć z art. 18 RODO, zatytułowanego: *Prawo do ograniczenia przetwarzania*.

2. Art. 4 pkt 3. Analiza

Ze słów: „(...) **oznacza oznaczenie przechowywanych danych osobowych** (...)" wnioskujemy, że ograniczenie przetwarzania danych osobowych to oznaczenie tych danych.

Ze słów: „(...) **w celu** (...)" wnioskujemy, że ograniczenie przetwarzania danych osobowych to czynność prowadzona w pewnym celu. Cel ten jest określony dalej w przepisie.

Ze słów: „(...) **w celu ograniczenia ich przyszłego przetwarzania**" wnioskujemy, że celem ograniczenia przetwarzania danych osobowych jest ograniczenie przetwarzania danych osobowych w przyszłości.

3. Art. 4 pkt 3. Uwagi
3.1. Art. 4 pkt 3. Uwaga 1.
Zakres znaczenia pojęcia *ograniczenie przetwarzania*

Należy zwrócić uwagę, że znaczenie słów: „ograniczenie przetwarzania (danych osobowych)" jest zdecydowanie odmienne, od rozumienia tych słów, jakie nasuwa się przy pierwszym spojrzeniu na ten przepis. Wydaje się, że ograniczenie przetwarzania to takie czy inne zmniejszenie zakresu przetwarzania danych osobowych, podczas gdy jest inaczej, ograniczenie przetwarzania to jedynie oznaczenie danych osobowych. Dane są oznaczane po to, by w przyszłości rzeczywiście ograniczyć ich przetwarzanie czyli zmniejszyć zakres przetwarzania. Zmniejszyć ilość przetwarzanych danych lub zmniejszyć ilość podejmowanych czynności przetwarzania.

Należy zwrócić uwagę, że o tym, co w szczegółach należy rozumieć przez ograniczenie przetwarzania dowiadujemy się dopiero z art. 18 RODO. Z przepisu tego, wynika, że w związku z żądaniem ograniczenia przetwarzania trzeba podjąć kilka, powiązanych, czynności. Wynika to jednak dopiero z art. 18 RODO. Z przepisu omawianego, obowiązek wykonania czegokolwiek nie wynika. Przepis ten jedynie wskazuje, że *ograniczenie przetwarzania* to nic więcej jak tylko oznaczenie danych. Oznaczenie danych mające pewien cel, jakim jest ograniczenie przetwarzania danych w przyszłości, jednak omawiany przepis wyłącznie definiuje ograniczenie przetwarzania i to definiuje je właśnie jako samo oznaczenie.

Nieco odmiennie rzecz przedstawiają P. Litwiński, P. Barta i M. Kawecki podnosząc w swoim Komentarzu, że *(...) Stąd sprowadzenie nakazu ograniczenia przetwarzania danych wyłącznie do poziomu odpowiedniego oznaczenia danych wydaje się być nieporozumieniem*[195]. O ile bowiem z ograniczeniem przetwarzania związany jest cały łańcuch czynności, o tyle czynności te wynikają z art. 18 RODO, nie zaś z samej definicji ograniczenia przetwarzania.

Patrząc surowo na wypowiedź wskazanych autorów, należy stwierdzić, że dokonali oni swoistej życzeniowej wykładni prawa. Uznali, że skoro ograniczenie przetwarzania znaczy to co znaczy,

[195] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 204.

jednak oni uznają to za niewłaściwe to nieporozumieniem jest to co znaczy definicja. Patrząc aprobatywnie na zdanie wskazanych autorów, można stwierdzić że zinterpretowali oni definicję ograniczenia przetwarzania w duchu art. 18 RODO.

Pewien sens to ma. Artykuł 18 dotyczy ograniczenia przetwarzania, wynikają z niego pewne procedury związane z ograniczeniem przetwarzania. Nie zmienia to jednak faktu, że definicja ograniczenia przetwarzania znaczy to co znaczy.

Zupełnie nie do przyjęcia jest stanowisko P. Litwińskiego, P. Barty i M. Kaweckiego, wyrażone zdaniem: „Treść art. 5 RODO w ocenie autorów powinna być traktowana jako doprecyzowująca ogólną definicję „ograniczenia przetwarzania".[196] Przede wszystkim zadziwiają słowa o ogólnej definicji ograniczenia przetwarzania. Zapewne przez ogólną definicję wspomniani autorzy rozumieją definicję z art. 4 pkt 3 RODO. Skoro jednak to jest definicja ogólna, to gdzież szukać szczególnej. Z cytatu wynika, że należy ją zapewne skonstruować w oparciu o art. 5 RODO, tyle tylko, że art. 5 RODO statuuje zasady dotyczące przetwarzania danych osobowych.

O zasadach piszę dalej w komentarzu do art. 5 RODO, tu zwracam jedynie uwagę na fakt, że zasady nic nie precyzują, że jest wręcz odwrotnie, zasady mają charakter ogólny i one same precyzowane są przez odpowiednie przepisy szczególne.

3.2. Art. 4 pkt 3. Uwaga 2.
Skutek na przyszłość
wywierany przez ograniczenie przetwarzania

Zgadzam się ze stanowiskiem A. Nerki, że: „Zastosowane ograniczenie wywiera skutek na przyszłość (...)"[197] – ADO oznacza dane, a następnie podejmuje dalsze, wynikające z art. 18 RODO czynności.

[196] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 204-205.

[197] A Nerka w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 88.

3.3. Art. 4 pkt 3. Uwaga 3.
Ograniczenie przetwarzania
a *ograniczenie przyszłego przetwarzania*

Podkreślenia wymaga, że w przepisie występują dwa rodzaje ograniczenia. Jedno ograniczenie, definiowane w przepisie, to: „ograniczenie przetwarzania" danych osobowych. Drugie ograniczenie, występujące w przepisie to: „ograniczenie (...) przyszłego przetwarzania" danych osobowych. Pierwsze – ograniczenie przetwarzania – to oznaczenie, o którym mowa w przepisie. Drugie – ograniczenie przyszłego przetwarzania – to czynności, które odbędą się w przyszłości na tych danych, które obecnie są poddawane ograniczeniu przetwarzania.

4. Art. 4 pkt 3. Podsumowanie
w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 3 RODO definiuje ograniczenie przetwarzania, zatem zgodnie z dyrektywą języka prawnego[198], każdy kto interpretuje RODO powinien rozumieć pojęcie „ograniczenie przetwarzania" tak jak jest ono w komentowanym przepisie zdefiniowane.

  ADO, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „ograniczenie przetwarzania" tak jest ono zdefiniowane w art. 4 pkt. 3 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „ograniczenie przetwarzania" zgodnie z definicją języka prawnego znajdującą się w omawianym przepisie.

5. Art. 4 pkt 3. Konkretyzacja zasad

Pojęcie „ograniczenie przetwarzania" ma pewien, choć nieoczywisty, związek z konkretyzacją zasad. Ograniczenie przetwarzania może prowadzić do ograniczenia przyszłego przetwarzania, które z kolei pomaga zrealizować: zasadę zgodności z prawem, zasadę ogra-

[198] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

niczenia celu, zasadę minimalizacji danych, zasadę prawidłowości, zasadę ograniczenia przechowywania, zasadę poufności.

6. Art. 4 pkt 3. Postulaty de lege ferenda
6.1 Art. 4 pkt 3. Postulat 1.
Doprecyzowanie treści przepisu

Z uwagi (3.1. Art. 4 pkt 3. Uwaga 1. Zakres znaczenia pojęcia „ograniczenie przetwarzania".) wynika niewątpliwie wniosek, że definicja ograniczenia przetwarzania nie jest jasna. Z definicji ograniczenia przetwarzania, branej pod uwagę łącznie z art. 18 RODO wynika, że dopiero dogłębna analiza art. 18 RODO pozwala tak naprawdę pojąć istotę ograniczenia przetwarzania. W powołanym w uwadze *3.1. Art. 4 pkt 3. Uwaga 1. Zakres znaczenia pojęcia „ograniczenie przetwarzania* poglądzie P. Litwińskiego, P. Barty i M. Kaweckiego, widzę ślad tej myśli. Wskazani autorzy twierdzą, że nieporozumieniem jest sprowadzenie ograniczenia przetwarzania li tylko do oznaczenia danych. Ograniczenie przetwarzania zdefiniowane w art. 4 pkt 3 RODO, to jednak właśnie tylko oznaczenie danych. Faktem jest, że założenie, że ograniczenie przetwarzania sprowadza się tylko do oznaczenia danych osobowych, jest błędne, ale wiadomo to nie z art. 4 ust. 3 RODO ale z art. 18 RODO.

W związku z powyższym, uważam, że definicja ograniczenia przetwarzania powinna w sposób nieco dokładniejszy oddawać istotę ograniczenia przetwarzania i to o czym piszą P. Litwiński, P. Barta i M. Kawecki, że ograniczenie przetwarzania to nie tylko oznaczenie danych osobowych.

W związku z tym postuluję nowelizację art. 4 pkt 12 RODO poprzez zastąpienie słów: „**ograniczenia ich przyszłego przetwarzania**" słowami „realizacji obowiązków wynikających z art. 18 RODO". Zwizualizowanie nowelizacji za pomocą metod graficznych prowadzi do przedstawienia zaproponowanej nowelizacji w następujący sposób: „„„ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ~~ograniczenia ich przyszłego przetwarzania~~ **realizacji obowiązków wynikających z art. 18 RODO**" (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.).

Przepis po nowelizacji miałby postać:

„„ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu realizacji obowiązków wynikających z art. 18 RODO".

7. Art. 4 pkt 3. Rozważania historyczne.
7.1. Art. 4 pkt 3. Rozważanie 1.
Odpowiedniki w dawnej legislacji

W Dyrektywie 95/46/WE brak jest odpowiednika art. 4 pkt 3 RODO. Pojęcie ograniczenia przetwarzania jest jednak bliskie znaczeniowo, o ile nie tożsame z pojęciem blokowania danych, które występuje dwukrotnie w Dyrektywie 95/46/WE. Występuje ono w art. 2 lit. b Dyrektywy 95/46/WE i w art. 12 lit b Dyrektywy 95/46/WE (jako *zablokowanie danych*). Zwracają na to uwagę L. A. Bygrave i L. Tosoni, którzy zauważają też, że pojęcie to występowało w niemieckim i we włoskim akcie prawnym dotyczących ochrony danych osobowych.[199]

[199] Por.: L. A. Bygrave, L. Tosoni w: *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 124.

Artykuł 4 pkt 4 RODO

„profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

1. Art. 4 pkt 4. Komentarz

Profilowanie oznacza dowolną, jakąkolwiek, każdą formę przetwarzania danych osobowych, która odbywa siew sposób zautomatyzowany i ma na celu m.in. analizę lub prognozowanie przeprowadzana w zakresie rozmaitych sfer życia konkretnych osób fizycznych

Profilowanie musi się odbywać w sposób zautomatyzowany. Prawodawca nie wyjaśnia niestety co rozumie przez „sposób zautomatyzowany". Zapewne, w dzisiejszej rzeczywistości, przez sposób zautomatyzowany należy rozumieć wykonywanie obliczeń na danych za pomocą algorytmów komputerowych.

Czynność, by była profilowaniem, musi, polegać na wykorzystaniu danych osobowych.

Profilowanie to czynność wykonywana w pewnym konkretnym celu, jeżeli czynność nie jest wykonywana w tym celu, to nie jest profilowaniem.

2. Art. 4 pkt 4. Analiza

Ze słów: „**oznacza dowolną formę (...) przetwarzania danych osobowych**, (...)" wnosimy, że profilowanie oznacza dowolną, jakąkolwiek, każdą formę przetwarzania danych osobowych. Nie jest jasne co należy rozumieć przez „formę przetwarzania danych osobowych", zapewne jednak intencją prawodawcy jest tu wskazanie, że jeżeli czynność spełnia warunki zapisane dalej w przepisie, to nieistotne jest jak w sensie formalnym, technicznym, czynność ta się odbywa.

Ze słów: „(...) **zautomatyzowanego przetwarzania danych osobowych** (...)" wnosimy, że profilowanie musi się odbywać w sposób zautomatyzowany. Prawodawca nie wyjaśnia niestety co rozumie przez „sposób zautomatyzowany". Zapewne, w dzisiejszej rzeczywistości, przez sposób zautomatyzowany należy rozumieć wykonywanie obliczeń na danych za pomocą algorytmów komputerowych.

Ze słów wytłuszczonych w przepisie: „(...) **które polega na wykorzystaniu danych osobowych** (...)" wnosimy, czynność, by była profilowaniem, musi, oprócz spełnienia innych zawartych w przepisie warunków, polegać na wykorzystaniu danych osobowych. Jeżeli czynność rozpatrywana jest bardzo bliska profilowaniu, ale w jej toku nie są wykorzystywane dane osobowe, to czynność ta profilowaniem nie jest.

Ze słów wytłuszczonych w przepisie: „(...) **wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej**, (...)" wnosimy, że profilowanie to czynność wykonywana w pewnym konkretnym celu, jeżeli czynność nie jest wykonywana w tym celu, to nie jest profilowaniem.

Ze słów: „(...) w s**zczególności do** (...)" wnosimy, że użycie tego zwrotu oznacza iż cele profilowania, podane dalej w przepisie to cele przykładowe. Jeżeli zatem czynność o cechach wymienionych w przepisie jest wykonywana w innym celu, niż cele podane w przepisie, po słowach: *w szczególności*, to czynność taka też jest profilowaniem.

Ze słów wytłuszczonych w przepisie: „(...) **w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się**" dowiadujemy się jakie mogą być, wspomniane wyżej, przykładowe cele profilowania. Przykładowymi celami profilowania mogą być zatem:

- analiza aspektów dotyczących efektów pracy osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących efektów pracy osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących sytuacji ekonomicznej osoby fizycznej, której dane są przetwarzane,

- prognoza aspektów dotyczących sytuacji ekonomicznej osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących zdrowia osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących zdrowia osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących osobistych preferencji osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących osobistych preferencji osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących zainteresowań osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących zainteresowań osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących wiarygodności osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących wiarygodności osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących zachowania osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących zachowania osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących lokalizacji osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących lokalizacji osoby fizycznej, której dane są przetwarzane,
- analiza aspektów dotyczących przemieszczania się osoby fizycznej, której dane są przetwarzane,
- prognoza aspektów dotyczących przemieszczania się osoby fizycznej, której dane są przetwarzane.

Jak widać przykładowe cele profilowania to analiza lub prognozowanie przeprowadzane w zakresie rozmaitych sfer życia konkretnych osób fizycznych.

3. Art. 4 pkt 4. Uwagi
3.1. Art. 4 pkt 4. Uwaga 1.
Rodzaje profilowania

Profilowanie może mieć różne odmiany, na co zwracają słusznie uwagę P. Litwiński, P. Barta, M. Kawecki. [200]

Profilowanie w oparciu o **profile indywidualne** – profilowanie prowadzone w oparciu o prawdziwe dane osobowe konkretnej osoby.

Profilowanie w oparciu o **profile statystyczne** – profilowanie prowadzone w oparciu o dane statystyczne, które mogą być prawdziwe dla danej osoby, ale pewności nie ma.

Profilowanie w oparciu o **profile predykcyjne** – profilowanie prowadzone w oparciu o obserwacje zachowania konkretnych osób.

Profilowanie w oparciu o **profile jawne** – profilowanie prowadzone w oparciu o dane dostarczone przez konkretną osobę, której profilowanie dotyczy.

Profilowanie można również dzielić na profilowanie bezpośrednie i na profilowanie pośrednie. Jest to podział wskazany przez B. Fishera.[201]

Profilowanie bezpośrednie – profilowanie, które prowadzone jest w oparciu o dane dostarczone przez konkretną osobę, której profilowanie dotyczy. Jak widać profilowanie to tożsame jest z profilowaniem w oparciu o profile jawne.

Profilowanie pośrednie – profilowanie prowadzone w oparciu o dane uzyskane z innych źródeł niż od osoby, której dane dotyczą.

---

[200] Zwracają na to uwagę P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 205, za M Ciechomską. M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych,* Europejski Przegląd Sądowy 2017, Nr 5, s. 205.

[201] B. Fisher w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 89.

3.2. Art. 4 pkt 4. Uwaga 2.
Profilowanie jako przetwarzanie danych osobowych

Profilowanie w oparciu o profile indywidualne jest czynnością przetwarzania danych osobowych.

Profilowanie w oparciu o profile statystyczne. Wydaje się, że ten rodzaj profilowania nie jest przetwarzaniem danych osobowych. Profilowanie w ten sposób to czynność prowadzona na informacjach, które mogą być czyimiś danymi osobowymi, ale mogą też nimi nie być. Z ostrożności, administrator powinien traktować takie profilowanie jak czynność na danych, jednak wątpliwość, czy to jest naprawdę czynność na danych – pozostaje. Jeśli nie jest to czynność na danych, to taka czynność nie jest profilowaniem w rozumieniu analizowanego przepisu.

Profilowanie w oparciu o profile predykcyjne jest czynnością przetwarzania danych osobowych.

Profilowanie w oparciu o profile jawne jest czynnością przetwarzania danych osobowych.

3.3. Art. 4 pkt 4. Uwaga 3.
Profilowanie jako wytwarzanie danych osobowych

W dziedzinie profilowania zachodzi ciekawe zjawisko, otóż profilowanie może doprowadzić do uzyskania nowych danych osobowych. Przedsiębiorca-administrator profiluje osoby fizyczne i uzyskuje w ten sposób dane osobowe tych osób dotyczące. Można wręcz powiedzieć, że przedsiębiorca-administrator je wytwarza. W takiej sytuacji przedsiębiorca powinien mieć świadomość, że posiada informacje dotyczące osoby fizycznej, jednak nie pozyskał tych informacji od tej osoby. W takiej sytuacji przedsiębiorca powinien zrealizować art. 14 RODO.[202]

3.4. Art. 4 pkt 4. Uwaga 4.
Rola zautomatyzowanego przetwarzania danych osobowych

Zautomatyzowane przetwarzanie danych osobowych, jakim jest profilowanie pozwala na dopasowanie oferty handlowej jak również usługi świadczonej przez organ publiczny do potrzeb czy do specyfiki

[202] Podobnie: L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 99.

danej osoby fizycznej. Uwagę na to zwraca P. Fajgielski, który dodaje, że zjawisko to skutkuje gromadzeniem coraz większej ilości danych osobowych.[203] Autor ten, w innym miejscu pisze również o tym, że zautomatyzowne przetwarzanie danych pozwala na *(...) niejawną analizę aktywności osób i tworzenie tzw. profili osobowościowych (...)*[204]. Co ciekawe, właśnie w gromadzeniu dużej ilości danych wskazany autor dostrzega powód tworzenia przepisów , których celem jest ochrona osób, których dane dotyczą. O ile nie jestem przekonany o doniosłości wskazanego przez P. Fajgielskiego łańcucha wynikań, o tyle istnieje on zapewne i dowodzi doniosłości zjawiska zautomatyzowanego przetwarzania danych osobowych.[205]

4. Art. 4 pkt 4. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

- Artykuł 4 pkt 4 RODO definiuje profilowanie, zatem zgodnie z dyrektywą języka prawnego[206], każdy kto interpretuje RODO powinien rozumieć pojęcie „profilowanie" tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „profilowanie" tak jest ono zdefiniowane w art. 4 pkt. 4 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „profilowanie" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 4. Konkretyzacja zasad

Związek pojęcia „profilowanie" z zasadami jest i nie jest bliski.

- Nie jest bliski, bo wydaje się, że sama czynność profilowania nie konkretyzuje żadnej z zasad.
- Jest bliski ponieważ profilowanie jest przetwarzaniem danych osobowych. Sama informacja, że profilowanie jest przetwarzaniem da-

[203] P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*. Warszawa 2019. s. 15.

[204] P. Fajgielski, *op. cit.* s. 24.

[205] P. Fajgielski, *op. cit.* s. 15.

[206] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

nych osobowych nie jest szczególnie sensacyjna, pewna istotność pojawia się jednak kiedy uświadamiamy sobie, że przetwarzanie musi odbywać się zgodnie z zasadami dotyczącymi przetwarzania danych osobowych a skoro tak jest to i profilowanie, jako czynność na danych, musi odbywać się zgodnie z zasadami dotyczącymi przetwarzania danych osobowych.

Odnoszę się poniżej do profilowania w kontekście kolejnych zasad z art. 5 RODO.

5.1 art. 4 pkt 4. Realizacja zasad

Profilowanie powinno być realizowane w sposób, który sprzyja realizacji zasad w sposób opisany poniżej.

Realizacji **zasady zgodności z prawem**, poprzez przystąpienie do profilowania po ustaleniu w oparciu o jaką przesłankę dopuszczalności przetwarzania danych osobowych to profilowanie prowadzone będzie. Piszę tu o art., 6 RODO i odpowiednio o art. 9 RODO, oczywiście ze stosownymi uzupełnieniami.

Realizacji **zasady rzetelności**, poprzez informowanie osób, których dane dotyczą o fakcie profilowania. Jeżeli administrator danych nie zbiera danych w związku z profilowaniem, to nie realizuje art., 13 RODO ani art. 15 RODO, jednak realizuje art. 15 RODO. Jeżeli administrator przewiduje profilowanie w momencie zbierania danych osobowych, to informuje osobę, której dane dotyczą o tym, że przewiduje profilowanie jak również o tym, ze go nie przewiduje, co wynika z art. 13 ust. 1 lit. f RODO i z art. 14 ust. 2 lit. g RODO.

Realizacji **zasady przejrzystości** poprzez informowanie osób, których dane dotyczą o szczegółach przetwarzania danych osobowych, w tym o profilowaniu.

Realizacji **zasady ograniczenia celu**, poprzez informowanie osób, których dane dotyczą o celu profilowania, co pozwala osobom, których dane dotyczą na sprawne korzystanie z prawa do wniesienia sprzeciwu, wynikającego z art., 21 ust. 1 RODO i z prawa do żądania bycia zapomnianym i do, żądania ograniczenia przetwarzania.

Realizacji **zasady minimalizacji** poprzez informowanie osób, których dane dotyczą o fakcie profilowania, co pozwala osobom,

których dane dotyczą, na kontrolę przetwarzania danych osobowych przez administratora (art. 17 RODO, art. 18 RODO, art. 21 RODO).

Realizacji **zasady prawidłowości**, poprzez informowanie osób, których dane dotyczą o fakcie profilowania, przez co osoby te mogą kontrolować czy dane osobowe, które zostały uzyskane w wyniku profilowania są prawidłowe.

Realizacji **zasady ograniczenia przechowywania danych** poprzez informowanie osób, których dane dotyczą o fakcie profilowania, na kontrolowanie okresu przechowywania dotyczących ich danych osobowych. uzyskanych w wyniku profilowania.

6. Art. 4 pkt 4. Postulaty de lege ferenda

6.1 Art. 4 pkt 4. Postulat 1.
Usuniecie niezrozumiałej części przepisu i zastąpienie jej

Zgodnie z przepisem: *„**profilowanie**” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które (...)*. Nie jest dla mnie jasne dlaczego prawodawca ujął przepis niejasno, skoro mógł jaśniej. Postuluję aby początek przepisu brzmiał: „„**profilowanie**” oznacza zautomatyzowane przetwarzanie danych osobowych, które (…)”.

Uważam, ze należy uprościć przepis i jednocześnie usunąć z niego zwrot, który w całości, w mianowniku brzmi: „dowolna forma zautomatyzowanego przetwarzania danych osobowych”. Jeśli chodzi o „przetwarzanie danych osobowych”, to wiadomo co te słowa oznaczają. Jeśli chodzi o „zautomatyzowane przetwarzanie danych osobowych”, ze wskazaniem na „zautomatyzowane” to tak do końca nie wiadomo gdzie kończy się przetwarzanie zautomatyzowane a zaczyna to drugie – niezautomatyzowane. Prawdziwy problem ze zrozumieniem pojawia się kiedy chcemy zrozumieć zwrot „forma zautomatyzowanego przetwarzania danych osobowych” lub „dowolna forma zautomatyzowanego przetwarzania danych osobowych”. Oczywiście zinterpretujemy to jako „każde zautomatyzowane przetwarzanie danych osobowych” lub „zautomatyzowane przetwarzanie danych osobowych” – co postuluję wyżej, jednak czy prawodawca nie mógł tego przepisu napisać jasno?

W związku z powyższym postuluję aby początek przepisu brzmiał: „„profilowanie” oznacza ~~dowolną formę zautomatyzowanego przetwarzania~~ **zautomatyzowane przetwarzanie** danych osobowych,

które (…)”.(Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Przepis po nowelizacji miałby postać:

„profilowanie” oznacza zautomatyzowane przetwarzanie danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Artykuł 4. pkt 5 RODO

„pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

1. Art. 4. pkt 5. Komentarz

Pseudonimizacja danych osobowych to jedna z wielu możliwych czynności przetwarzania danych osobowych. Cel tej czynności wynika z dalszej części przepisu.

Pseudonimizacja to przetworzenie danych osobowych wykonywane w pewien szczególny, opisany w przepisie sposób. Pseudonimizacją jest jedynie czynność wykonywana właśnie w ten sposób.

Celem pseudonimizacji jest takie przetworzenie, danych osobowych by nie można było tych danych przypisać konkretnej żyjącej osobie fizycznej, ale jedynie bez użycia dodatkowych informacji. O informacjach tych jest dalej mowa w przepisie. Inaczej - celem pseudonimizacji jest taka zmiana danych osobowych, by nie było wiadomo kogo te dane dotyczą, oczywiście przy jednoczesnym zachowaniu pozostałych, wynikających z przepisu warunków.

Celem pseudonimizacji jest takie przetworzenie danych osobowych, by można było te spseudonimizowane dane przypisać konkretnej osobie fizycznej z użyciem (przy użyciu) dodatkowych informacji.

Wskazane, dodatkowe informacje, bez których nie można przypisać spseudonimizowanych danych osobie fizycznej, muszą spełniać pewne, określone w przepisie, warunki.

- Po pierwsze informacje te „są przechowywane osobno”.
- Po drugie informacje te „są objęte środkami technicznymi i organizacyjnymi”, opisanymi dalej w przepisie.

Nakaz osobnego przechowywania danych oznacza przechowywanie danych gdziekolwiek, o ile przechowujący jest w stanie uzasadnić, że przechowuje je osobno.

Celem objęcia tych danych środkami technicznymi i organizacyjnymi jest uniemożliwienie przypisania tych danych (pseudonimu) zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

2. Art. 4. pkt 5. Analiza

Ze słów: „**oznacza przetworzenie danych osobowych** (...)" wnosimy, że pseudonimizacja danych osobowych to jedna z wielu możliwych czynności przetwarzania danych osobowych. Cel tej czynności wynika z dalszej części przepisu.

Ze słów: „**oznacza przetworzenie danych osobowych w taki sposób** (...)" wnosimy, że pseudonimizacja to przetworzenie danych osobowych wykonywane w pewien szczególny, opisany dalej w przepisie sposób. Należy podkreślić, ze pseudonimizacją jest jedynie czynność wykonywana właśnie w ten, opisany w przepisie sposób.

Ze słów: „(…) **w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą** (...)" wynika, że celem pseudonimizacji jest takie przetworzenie danych osobowych, „by nie można ich było już przypisać konkretnej osobie, której dane dotyczą", oczywiście przy jednoczesnym zachowaniu pozostałych, wynikających z przepisu warunków. Celem pseudonimizacji jest zatem takie przetworzenie, danych osobowych by nie można było tych danych przypisać konkretnej żyjącej osobie fizycznej. Jeszcze bardziej skracając należy stwierdzić, że celem pseudonimizacji jest taka zmiana danych osobowych, by nie było wiadomo kogo te dane dotyczą, oczywiście przy jednoczesnym zachowaniu pozostałych, wynikających z przepisu warunków.

Ze słów: „(…) **bez użycia dodatkowych informacji** (...)", wynika, że celem pseudonimizacji jest takie przetworzenie, danych osobowych by nie można było tych danych przypisać konkretnej żyjącej osobie fizycznej, ale jedynie bez użycia dodatkowych informacji. O informacjach tych jest dalej mowa w przepisie. Celem pseudonimizacji nie jest zatem takie przetworzenie danych osobowych, by w ogóle nie można

było tych danych przypisać konkretnej żyjącej osobie fizycznej. Gdyby danych po przetworzeniu nie można było w żaden sposób przypisać osobie fizycznej, to byłaby to nie pseudonimizacja a anonimizacja. Celem pseudonimizacji jest takie przetworzenie danych osobowych, by można było te spseudonimizowane dane przypisać konkretnej osobie fizycznej z użyciem (przy użyciu) dodatkowych informacji.

Ze słów: „(...) **informacji, pod warunkiem że takie dodatkowe informacje są** (...)" wynika, że wskazane wyżej, dodatkowe informacje, bez których nie można przypisać spseudonimizowanych danych osobie fizycznej, muszą spełniać pewne, określone dalej w przepisie, warunki.

Ze słów: „(...) **pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi** (...)" wynika jakie warunki muszą spełniać dodatkowe informacje bez których nie można przypisać spseudonimizowanych danych konkretnej osobie fizycznej.
Po pierwsze informacje te „są przechowywane osobno".
Po drugie informacje te „są objęte środkami technicznymi i organizacyjnymi", opisanymi dalej w przepisie.

Jeśli chodzi o **osobne przechowywanie danych**, to niestety z przepisu nie wynika co tak naprawdę należy zrobić, by go, w tym zakresie, zrealizować. Nakaz osobnego przechowywania danych może oznaczać przechowywanie danych poza bazą danych, w której przechowywane są spseudonimizowane dane, nakaz osobnego przechowywania danych może oznaczać przechowywanie danych dyskiem fizycznym, na którym przechowywane są spseudonimizowane dane, nakaz osobnego przechowywania danych może oznaczać przechowywanie danych poza dyskiem logicznym, na którym przechowywane są spseudonimizowane dane, nakaz osobnego przechowywania danych może oznaczać przechowywanie danych poza siecią fizyczną, w której przechowywane są spseudonimizowane dane, nakaz osobnego przechowywania danych może oznaczać przechowywanie danych poza siecią logiczną, w której przechowywane są spseudonimizowane dane.

Nadużyciem byłoby napisanie, że **nakaz osobnego przechowywania danych** może oznaczać cokolwiek, lub, że nakaz osobnego przechowywania danych może oznaczać przechowywanie danych gdziekolwiek. To byłoby nadużyciem, ale nie jest już nadużyciem na-

pisanie, że nakaz osobnego przechowywania danych oznacza przechowywanie danych gdziekolwiek, o ile przechowujący jest w stanie uzasadnić, że przechowuje je osobno.

Nad problemem osobnego przechowywania dodatkowych informacji, o których mowa w przepisie zastanawia się K. Witkowska-Nowakowska. Autorka ta dane dodatkowe nazywa danymi służącymi do reidentyfikacji. Ja jestem zwolennikiem używania określenia „odwrócenie pseudonimizacji" ponieważ występuje ono w motywie 85 Preambuły RODO (ang. *reversal of pseudonymisation*), to jednak tylko uwaga marginalna. Dalej wskazana autorka pisze: *Oznacza to, że dane spseudonimizowane i dane potrzebne do reidentyfikacji nie mogą być razem przekazywane bądź przechowywane ani fizycznie, ani technicznie w tym samym miejscu, np. w tej samej szafie czy na tej samej stacji roboczej z jednym kontem użytkownika* [207]. Wskazana autorka dokonuje tu pewnych założeń, a mianowicie, że przechowywanie danych służących do odwrócenia pseudonimizacji w tej samej szafie to już nie jest przechowywanie „osobno". Intencja autorki jest zacna, jednak przykład z szafą może prowadzić na manowce.

Jak bowiem spojrzeć na sprawę, jeżeli dane służące do odwrócenia pseudonimizacji są w innej szafie, jednak stojącej tuż obok szafy z danymi? Pytanie jest, wbrew pozorom, poważne.

Jak spojrzeć na sprawę jeżeli dane służące do odwrócenia pseudonimizacji znajdują się w tej samej szafie co dane spseudonimizowane, jednak na innej półce? I to pytanie jest, poważne.

Jak spojrzeć na sprawę jeżeli dane służące do odwrócenia pseudonimizacji są co prawda w tej samej szafie co dane spseudonimizowane jednak na innym nośniku?

Jak spojrzeć na sprawę jeżeli dane służące do odwrócenia pseudonimizacji są co prawda w na tej samej stacji roboczej jednak dostępne są z kont innych użytkowników? Czy dane na osobnych nośnikach na tej samej półce są bardziej czy mniej osobno niż dane na jednym nośniku ale dostępne dla dwóch użytkowników?

Jak spojrzeć na sprawę jeżeli dane służące do odwrócenia pseudonimizacji są co prawda w na innych stacjach roboczych jednak dostępne

[207] K. Witkowska-Nowakowska w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz,* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 205.

są z konta tego samego użytkownika, funkcjonującego w obydwu stacjach roboczych?

Długo tak można wywodzić. Zacytowane zdanie wskazuje jakby jego autorka wiedziała co to znaczy „przechowywane osobno" i wiedzą tą się z czytelnikami jej części Komentarza dzieliła. Uważam, że niestety autorce tylko się wydaje, że wie. Autorka nie wie, ja nie wiem, nikt nie wie – nie wiemy ponieważ prawodawca nam tej wiedzy nie udzielił.

Jeśli chodzi o drugą część omawianego obowiązku, o słowa: *i są objęte środkami technicznymi i organizacyjnymi* wynika, że dodatkowe informacje bez których nie można przypisać spseudonimizowanych danych konkretnej osobie fizycznej muszą być objęte środkami technicznymi i organizacyjnymi, które spełniają opisane dalej w przepisie warunki. Zwracam uwagę, że między środkami technicznymi a środkami organizacyjnymi, widnieje spójnik *i*. Oznacza to, że warunki, które opisano dalej w przepisie, muszą zostać spełnione zarówno przez środki techniczne, jak i przez środki organizacyjne. Na pozór, sformułowaniu temu nie sposób niczego zarzucić, niestety przy bliższym wejrzeniu, pozór ten pryska. Przede wszystkim, nie wiadomo właściwie gdzie przebiega granica między środkami technicznymi a środkami organizacyjnymi. W rzeczywistości informatyki komputerowej można spróbować tę granice zarysować, może środki techniczne to środki mające miejsce wewnątrz sprzętu komputerowego, zaś środki organizacyjne to środki mające miejsce poza tym sprzętem. Może. Jakim bowiem środkiem, technicznym czy organizacyjnym, jest odłączenie komputera od sieci www, czy wyłączenie mu zasilania? Nie wiem tego, a co gorsza, mam świadomość, że można uzasadnić, zarówno, że jest to środek techniczny jak i że jest to środek organizacyjny.

Wydaje się, że z praktycznego punktu widzenia, można przyjąć pewne założenie, można otóż przyjąć, że środki techniczne, to wszelkie zabezpieczenia techniczne, zaś środki organizacyjne to czynności podejmowane przez ADO w tym celu aby te pierwsze były stosowane, na przykład szkolenia i audyty przestrzegania narzuconych przez ADO metod ochrony danych. Można też na rzecz spojrzeć inaczej i uznać, że środki techniczne to zabezpieczenia techniczne

Ze słów wytłuszczonych w przepisie: „oznacza przetworzenie danych osobowych (…) objęte **środkami technicznymi i organizacyjnymi**

uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;" wynika jaki jest cel objęcia środkami technicznymi i organizacyjnymi informacji bez których nie można przypisać danych konkretnej osobie. Celem objęcia tych danych środkami technicznymi i organizacyjnymi jest uniemożliwienie przypisania tych danych (pseudonimu) zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

3. Art. 4. pkt 5. Uwagi

3.1. Art. 4. pkt 5. Uwaga 1. Odwracalność pseudonimizacji

Podkreślić należy, że pseudonimizacji ma charakter odwracalny[208]. Wynika to wprost z motywu 26 Preambuły RODO, w którym czytamy: „Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej.". Czynność analogiczna do pseudonimizacji, jednak o charakterze nieodwracalnym nie jest pseudonimizacją. Ze względu na odwracalność pseudonimizacji nie można jej traktować jako usunięcia danych.[209]

3.2. Art. 4. pkt 5. Uwaga 2. Dane spseudonimizowane jako dane osobowe

Należy zwrócić uwagę na fakt, że dane spseudonimizowane to nadal dane osobowe.[210] Piszę o tym w komentarzu do art. 4 pkt 1 RODO w uwadze *3.2. Art. 4 pkt 1. Uwaga 2. Dane spseudonimizowane*. Podobny pogląd z trafnym odwołaniem do wyroku TSUE, prezentuje K. Witkowska-Nowakowska.[211]

---

[208] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 207, również: K. Witkowska-Nowakowska, *op. cit.* s. 204.

[209] K. Wygoda w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 89.

[210] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 207.

[211] K. Witkowska-Nowakowska, *op. cit*. s. 206-207.

3.3. Art. 4. pkt 5. Uwaga 3.
Pseudonimizacja a szyfrowanie

Pseudonimizacja skutkuje tym, że podmiot, który nie posiada klucza do odwrócenia pseudonimizacji, nie wie kogo dotyczą spseudonimizowane dane.

Szyfrowanie skutkuje tym , że podmiot, który nie posiada klucza do odszyfrowania, nie wie kogo dotyczą zaszyfrowane dane.
Jak widać skutek pseudonimizacji i szyfrowania jest podobny. Należy zatem zadać sobie pytanie o to czy szyfrowanie to to samo co pseudonimizacji a tylko pod inną nazwą. Otóż nie. Dane spseudonimizowane są nadal czytelne a jedynie nie wiadomo kogo dotyczą. Dane zaszyfrowane są nieczytelne. Jeżeli dane zostaną tak spseudonimizowane, że zostaną również unieczytelnione, to znaczy, że zostały one spseudonimizowane i zaszyfrowane. Analogicznie rzecz widzi K. Wygoda.[212] Podobne stanowisko prezentują[213] P. Litwiński, P. Barta i M. Kawecki. Katarzyna Witkowska-Nowakowska przywołuje pogląd J. Kűhlinga, który twierdzi, że proces pseudonimizacji może przebiegać między innymi przez szyfrowanie[214], jednak wskazana autorka trafnie, choć ostrożnie się od tego poglądu dystansuje.

3.4. Art. 4. pkt 5. Uwaga 4.
Uprawnienie do dokonania pseudonimizacji

Pseudonimizacja to „przetworzenie danych osobowych", należy pamiętać, że z art. 29 RODO i z art. 32 ust. 4 RODO wynika, że osoby, które przetwarzają dane osobowe, powinny mieć uprawnienie do przetwarzania skonstruowane z dwóch etapów. W związku z tym, osoby, które pseudonimizuja dane osobowe, powinny mieć właśnie takie uprawnienie.

4. Art. 4. pkt 5. Podsumowanie
w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

---

[212] K. Wygoda, *op. cit.* s. 91.

[213] P. Litwiński, P. Barta, M. Kawecki, *op. cit.* s. 208.

[214] K. Witkowska-Nowakowska, *op. cit.* s. 206.

- Artykuł 4 pkt 5 RODO definiuje pseudonimizację, zatem zgodnie z dyrektywą języka prawnego[215], każdy kto interpretuje RODO powinien rozumieć pojęcie „pseudonimizacja" tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „pseudonimizacja" tak jest ono zdefiniowane w art. 4 pkt. 5 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „pseudonimizacja" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4. pkt 5. Konkretyzacja zasad

Związek pojęcia „profilowanie" z zasadami nie jest bliski, jednak pewien jest.

Dane spseudonimizowane są nadal danymi osobowymi, więc należy przetwarzać je zgodnie z zasadami z art. 5 RODO.

Sama pseudonimizacja może sprzyjać realizacji wymienionych poniżej zasad.

Zasady zgodności z prawem – jeżeli dane osobowe spseudonimizowane przetwarzane są przez kogoś kto nie został odpowiednio na gruncie RODO uprawniony do przetwarzania, to tak długo jak nie uzyska on dostępu do mechanizmu odwrócenia pseudonimizacji, tak długo można utrzymywać, że w tej sytuacji, ta osoba nie ma dostępu do danych osobowych.

Zasady minimalizacji, ponieważ przetwarzanie danych osobowych spseudonimizowanych w pewnym stopniu faktycznie zmniejsza zakres przetwarzania danych osobowych mimo iż dane spseudonimizowane nie przestają być danymi osobowymi.

Zasady poufności – z tych samych przyczyn co zasad wymienionych wyżej. Osoba, która przetwarza dane osobowe spseudonimizowane, przetwarza dane osobowe, jednak pseudonimizacja danych podnosi poziom realizacji zasady poufności, bowiem osoba przetwarzająca mimo, że przetwarza dane osobowe, to może sama nie wiedzieć kogo one dotyczą. Wiedzieć to może ADO, wiedzieć to może jej

[215] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

przełożony, jednak ona nie. Jeżeli osoba, która przetwarza dane spseudonimizowane, ujawni je niezgodnie z prawem, to odbiorca, który otrzyma je niezgodnie z prawem i tak nie będzie wiedział kogo one dotyczą. Zajdzie tu ciekawa sytuacja, administrator ujawnia dane osobowe, zachodzi naruszenie ochrony danych z art. 4 pkt 12 RODO, jednak nie zachodzi naruszenie praw i wolności osób, których dane dotyczą.

Konkretyzacja wskazanych trzech zasad jest poparta wnioskami z analizy motywu 26 Preambuły RODO.

6. Art. 4. pkt 5. Postulaty de lege ferenda.
6.1 Art. 4. pkt 5. Postulat 1.
Uproszczenie treści przepisu przez usuniecie niejasnego fragmentu dotyczącego osobnego przechowywania danych osobowych

W prowadzonej wyżej analizie *2. Art. 4. pkt 5. Analiza*, zastanawiam się nad osobnym przechowywaniem danych osobowych. By nie powtarzać prowadzonych tam rozważań, tu przypomnę tylko, że nie sposób powiedzieć, kiedy przechowywanie jest osobne. Skoro tak, to słów o osobnym przechowywaniu nie sposób zastosować. Jednocześnie nie wolno ich nie stosować.[216] Prowadzi to do sytuacji, w której słowa o osobnym przechowywaniu danych będą stosowane jakkolwiek, tak tylko by uczynić zadość mętnym słowom przepisu. W ten sposób celem osobnego przechowywania nie staje się zabezpieczenie danych, poufności, prywatności czy czegokolwiek innego a jedynie uczynienie zadość wymogowi zapisanemu w przepisie. Zastosowanie przepisu nabiera więc waloru obrzędowego co, zwłaszcza jeśli zastanowimy się nad tym czego dotyczy przepis, skutkuje ośmieszeniem prawa. Tak być nie powinno. Nie twierdzę, że dane służące do odwrócenia pseudonimizacji powinny być przechowywane razem z danymi spseudonimizowanymi. Nie twierdze, że łatwo jest napisać przepis opisujący technikę tak, by nie popaść w kazuistykę. Twierdzę jednak, ze przepisy są po coś. Mają jakiś cel. Po dziś dzień odwołujemy się do słów Celsusa, z których wynika nakaz by prawo było dobre i sprawiedliwe, by służyło dobru i sprawiedliwości. Jakiemu więc dobru służy przechowywanie skoroszytów z danymi w

[216] L. Morawski, *op. cit*. s. 106.

dwóch szafach a nie w jednej? Jakiemu dobru służy przechowywanie danych na dwóch dyskach na jednej a może na dwóch półkach? Te absurdy można mnożyć. By tego nie czynić, wniosek jest oczywisty.

Postuluję nowelizację art. 4 pkt 5 RODO przez usuniecie słów: *przechowywane osobno i są*.

6.2 Art. 4. pkt 5. Postulat 2. Dalsze uproszczenie treści przepisu przez usunięcie kolejnego niejasnego fragmentu dotyczącego środków technicznych i organizacyjnych

W prowadzonej wyżej analizie *2. Art. 4. pkt 5. Analiza*, zastanawiam się nad tajemniczą różnicą miedzy środkami technicznymi a organizacyjnymi. By nie powtarzać prowadzonych tam rozważań, tu przypomnę tylko, że nie w sposób odpowiedzialny odróżnić środków technicznych od organizacyjnych a co więcej, z uwagi na użycie funktora *i* ADO ma obowiązek zastosować jedne i drugie. Wobec mętności przepisu jego słowa nabierają walorów zaklęcia, które dla celów obrzędowych, po to tylko by zaklęcie wypowiedzieć, wypowiada ADO. Nie jest to dobre.

W związku z tym postuluję nowelizację art. 4 pkt 5 RODO przez usuniecie słów: *technicznymi i organizacyjnymi*.

6.3 Art. 4. pkt 5. Postulat 1+2 =3. Uproszczenie tresci przepisu przez usuniecie obydwu niejasnych fragmentów

W postulacie *6.1 Art. 4. pkt 5. Postulat 1. Uproszczenie treści przepisu przez usuniecie niejasnego fragmentu* i w postulacie *6.2 Art. 4. pkt 5. Postulat 2. Dalsze uproszczenie treści przepisu przez usunięcie kolejnego niejasnego fragmentu* postuluję usunięcie dwóch różnych, niejasnych fragmentów art. 4 pkt 5 RODO. Najlepiej by z przepisu zostały usunięte oba te fragmenty, co spowodowałoby pewne rozjaśnienie jego treści i nie wystawiało by prawa na pośmiewisko. Piszę o pośmiewisku, w odniesieniu do słów *przechowywane osobno*, szerzej rzecz omawiam wyżej w analizie *2. Art. 4. pkt 5. Analiza*.

Postuluję nowelizację art. 4 pkt 5 RODO przez usuniecie słów: *przechowywane osobno i są* i przez usuniecie słów: *technicznymi i organizacyjnymi*. Po zrealizowaniu postulatu przepis miałby postać

zaprezentowaną poniżej. (Czcionką przekreśloną zaznaczam fragmenty, usunięte.)

„„„**pseudonimizacja**” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są ~~przechowywane osobno i są~~ objęte środkami ~~technicznymi i organizacyjnymi~~ uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”.

Artykuł 4 pkt 6 RODO

„zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

1. Art. 4 pkt 6. Komentarz

Należy sądzić, że „zbiór danych" definiowany w przepisie to w istocie „zbiór danych osobowych".

Zbiór danych osobowych to zestaw danych osobowych, zdefiniowany w przepisie.

Zbiór danych osobowych to zestaw tych danych, który jest uporządkowany. Przepis nie precyzuje sposobu uporządkowania, jednak dalej jest w nim mowa o dostępności danych według określonych kryteriów.

Zbiorem w rozumieniu analizowanego przepisu jest zestaw, który jest uporządkowany z użyciem co najmniej dwóch kryteriów.

Dla zbioru danych osobowych nieistotne jest czy uporządkowany zestaw stanowiący zbiór, czyli zbiór, jest scentralizowany, zdecentralizowany czy rozproszony. Zbiór może znajdować się pod jednym adresem, w jednej serwerowni czy archiwum, może pod różnymi adresami, w różnych serwerowniach czy archiwach.

Zbiór może być scentralizowany lub zdecentralizowany lub rozproszony odpowiednio: funkcjonalnie lub geograficznie. Możliwe są tu wszelkie połączenia znaczeniowe między słowami z grupy: „scentralizowany, zdecentralizowany, rozproszony" a słowami z grupy: „funkcjonalnie, geograficznie".

2. Art. 4 pkt 6. Analiza

Ze słów wytłuszczonych w przepisie: „**oznacza** uporządkowany **zestaw danych osobowych** (…)" wnioskujemy, że zbiór danych osobowych to zestaw danych osobowych, który cechują pozostałem określone dalej w przepisie kryteria. Należy zwrócić uwagę, że pojęcie definiowane zostało tu zapisane jako *zbiór danych*. Dalej w definicji mowa jest o zestawie danych osobowych, należy z tego wnioskować, że *zbiór danych* to w istocie „zbiór danych osobowych".

Ze słów wytłuszczonych w przepisie: „**oznacza uporządkowany** zestaw danych osobowych (…)" wnioskujemy, że zbiór danych osobowych to zestaw tych danych, który jest uporządkowany. Przepis nie precyzuje sposobu uporządkowania, jednak dalej jest w nim mowa o dostępności danych według określonych kryteriów.

Ze słów wytłuszczonych w przepisie: „oznacza uporządkowany zestaw danych osobowych **dostępnych według określonych kryteriów** (…)" wnioskujemy, że zbiór danych osobowych to zestaw tych danych, który jest uporządkowany. Prawodawca nie wskazuje na to jakie to miałyby być kryteria. z przepisu możemy wywnioskować, że kryteria to kryteria według których dostępne są dane. Zapewne intencją prawodawcy jest że zestaw danych osobowych jest zbiorem danych osobowych jeżeli dane te uporządkowane są w sposób umożliwiający odszukanie danych o konkretnych wartościach. Należy zwrócić uwagę, na słowo *kryteriów*. Jak widać występuje ono w liczbie mnogiej. W pojedynczej mowa byłaby o kryterium. Wynika z tego, że zbiorem w rozumieniu analizowanego przepisu jest zestaw, który jest uporządkowany z użyciem co najmniej dwóch kryteriów. Szerzej o tym dalej, w uwadze *3.1. Art. 4 pkt 6. Uwaga 1. Kryteria a kryterium*.

Ze słów: „(…) **niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony** (…)" wnioskujemy, że dla zbioru danych osobowych nieistotne jest czy uporządkowany zestaw stanowiący zbiór, czyli zbiór, jest scentralizowany, zdecentralizowany czy rozproszony. Słowa te (scentralizowany, zdecentralizowany, rozproszony) nie są w RODO zdefiniowane. Należałoby je analizować z użyciem słowników. Nie czynię tego świadomie, uważam powiem, że znaczenie tych słów jest powszechnie znane. Wniosek jaki wynika z analizowanego fragmentu przepisu jest dość oczywisty, najlepiej jednak podać go na kilku przykładach. Zbiór może znajdować się w jednej bazie danych, może w kilku, czy większej ilości. Zbiór może tworzyć kilka baz danych, z których w każdej może funkcjonować inne kryterium porządkujące i nadal może być to jeden zbiór. Zbiór może znajdować się w jednym pudełku, skrzynce, szafce aktowej, kartotece – może w większej ilości. Zbiór może znajdować się pod jednym adresem, w jednej serwerowni czy archiwum, może pod różnymi adresami, w różnych serwerowniach czy archiwach.

Ze słów wytłuszczonych w przepisie: „(…) niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony **funkcjonalnie lub geograficznie**” wnioskujemy, że zbiór może być scentralizowany lub zdecentralizowany lub rozproszony odpowiednio: funkcjonalnie lub geograficznie. Możliwe są tu wszelkie połączenia między słowami z grupy: „scentralizowany, zdecentralizowany, rozproszony” a słowami z grupy: „funkcjonalnie, geograficznie”.

Wszelkie zależności dotyczące scentralizowania, zdecentralizowania, rozproszenia, funkcjonalnego, geograficznego – można wyprowadzić z poniższej tabeli, pamiętając przy tym jednak o zasadzie niesprzeczności.

	funkcjonalnie	**geograficznie**
scentralizowany		
zdecentralizowany		
rozproszony		

3. Art. 4 pkt 6. Uwagi
3.1. Art. 4 pkt 6. Uwaga 1.
Kryteria a kryterium

Zbiór danych osobowych to zestaw tych danych, który jest uporządkowany. Dane osobowe w zbiorze są dostępne *według określonych kryteriów*. Jeżeli dane osobowe nie są dostępne według kryteriów to dana rzecz, zjawisko, zestaw nie jest zbiorem danych osobowych. Szczególną uwagę należy poświecić liczbie w jakiej zapisano sposób uporządkowania zbioru. Jest to liczba mnoga: „kryteriów”. Wynika z tego, że jeżeli dane osobowe dostępne są według określonego kryterium, to dana rzecz, zjawisko, zestaw nie jest zbiorem danych osobowych w rozumieniu komentowanego przepisu. Wniosek taki niezależny jest od porównywanych wersji językowych. Przepis stanowi o kryteriach nie zaś o kryterium.

Zakres pojęcia zbioru jest niezwykle istotny dla omawianych zagadnień. Artykuł 2 ust 1. RODO uzależnia stosowanie RODO między innymi od tego czy przetwarzanie danych osobowych dotyczy danych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Jak więc widać pojęcie zbioru danych jest niezwykle istotne. Od zakresu tego pojęcia zależy w wielu sytuacjach czy RODO

znajdzie zastosowanie. Jeżeli przetwarzane są dane które stanowią część zbioru danych to RODO stosuje się do takiego przetwarzania, należy jednak przy tym pamiętać o zakresie pojęcia zbiór danych. Jeżeli dany zestaw danych osobowych nie mieści się w zakresie pojęcia *zbiór danych* to RODO nie stosuje się do przetwarzania danych osobowych w tym zestawie. Innymi słowy, jeżeli dane osobowe przetwarzane są w zestawie, który uporządkowany jest według jednego kryterium, to RODO nie dotyczy takiego przetwarzania. Oczywiście podobnie rzecz się w odniesieniu do danych które co prawda jeszcze nie są przetwarzane w zbiorze czy zestawie ale mają stanowić część takiego zbioru lub zestawu. Jeżeli zatem przetwarzane są dane osobowe, które mają stanowić część zestawu który uporządkowany jest według jednego kryterium to RODO nie ma zastosowania do tego przetwarzania danych.

Prowadzone tu rozważania mogą wydawać się dziwne i prowadzące do ewentualnych naruszeń praw osób których dane dotyczą należy jednak pamiętać że RODO dotyczy nie tylko osób których dane dotyczą ale również administratorów danych, których prawa również należy chronić. Fakt, że RODO nie dotyczy przetwarzania danych osobowych w zestawie uporządkowanym według jednego kryterium może mieć duże znaczenie dla ewentualnej odpowiedzialności administratorów danych jeżeli administrator danych dopuści się naruszenia Ochrony danych osobowych skutkującego naruszeniem praw lub wolności osób fizycznych to grozi mu niezwykle surowa odpowiedzialność Jeżeli jednak administrator danych dopuści się czynności na danych osobowych której nie można zakwalifikować jako naruszenia ochrony danych osobowych ponieważ RODO nie ma zastosowania w danej sytuacji to odpowiedzialność za to zdarzenie administratorowi nie grozi. Można oczywiście zastanawiać się czy tak być powinno, jednak zastanawianie się nad właściwym kształtem przepisu przekracza ramy tych rozważań zaś zastanawiam się nad nim w postulacie *6.1 Art. 4 pkt 6. Postulat 1. Doprecyzowanie treści przepisu*.

Warto zaznaczyć że odmienny pogląd w przedstawionej sprawie prezentuje M. Krzysztofek. autor ten twierdzi[217] że dominujący jest pogląd przeciwny od zaprezentowanego przeze mnie powyżej.

[217] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016, s. 48.

z poglądem zaprezentowanym przeze mnie powyżej można się nie zgadzać zwracam jednak uwagę że komentarz M. Krzysztofka został wydany w 2016 roku kiedy trudno jeszcze było mówić o dominującej opinii w jakiejkolwiek sprawie dotyczącej RODO.

Mimo że nie zgadzam się ze wskazanym autorem to uważam jednak zawarte zacytowania jego zdanie, w którym wyjaśnia on jak rozumie komentowany przepis. Zdanie to brzmi: *(...) posłużenie się to liczbą mnogą nie jest wymogiem ustalenia więcej niż jednego kryterium porządkujące go dane w zbiorze, lecz wskazaniem że dopuszczalne jest posłużenie się różnymi kryteriami*. W cytowanym zdaniu M. Krzysztofka dostrzegam ślad jakiejś lotnej myśli autora, która jednak niestety w momencie przenoszenia na papier czy wręcz w momencie jej redagowania, uległa niestety przekłamaniu lub spłyceniu. Wskazany autor wywodzi że dzięki temu, że w przepisie mowa jest o kryteriach administrator może stosować różne kryteria. Z tym że administrator może stosować różne kryteria w pełni się zgadzam, tyle tylko że gdyby administrator stosował więcej niż jedno kryterium jednak byłyby one takie same to trudno byłoby powiedzieć że administrator stosuje różne kryteria.

Pogląd zgodnie z którym dla istnienia zbioru wystarczy jedno kryterium prezentuje M. Sakowska-Baryła,[218] w sposób, który każe dopatrywać się w jej stanowisku, śladu poglądów M. Krzysztofka, acz autorka wskazuje na literaturę wyrosłą jeszcze na gruncie poprzedniej regulacji, co dziwić nie może, bo i poglądy M. Krzysztofka na owym gruncie wyrosły.

3.2. Art. 4 pkt 6. Uwaga 2.
Zbiór danych osobowych a zbiór nośników z danymi osobowymi

Ze względu na niejasną definicję zbioru danych należy zastanowić się nad jednym jeszcze problemem może się otóż zdarzyć sytuacja w której dane osobowe zapisane są w sposób nieuporządkowany na nośnikach, które przechowywane są w sposób uporządkowany. Mariusz Krzysztofek jako przykład takiej sytuacji podaje[219] nagrania z kamer monitoringu przechowywane w sposób uporządkowany chro-

[218] M. Sakowska-Baryła w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 94-95.

[219] M. Krzysztofek, *loc. cit.*

nologicznie. Wskazany autor używa tego przykładu w innym jeszcze celu którym ja zajmuję się niżej przykład taki jest jednak idealny dla ilustracji sytuacji, w której kryteria wyszukiwawcze porządkują nośniki nie zaś dane. Kiedy przyglądamy się takiej sytuacji po raz pierwszy to oczywiste wydaje się że zbiór nośników nie stanowi zbioru danych osobowych. Innymi słowy wydaje się, że nie można utożsamić zbioru nośników danych ze zbiorem danych. Dłuższe zastanowienie się nad problemem prowadzi do wniosku że sytuacja wcale nie jest taka oczywista, że jeżeli, tak jak w przykładzie M. Krzysztofka uporządkowano nośniki zawierające nieuporządkowane dane, to może taki zbiór nośników danych jest jednocześnie rodzajem zbioru danych. Wydaje się że tak nie jest pewien jednak niepokój pozostaje.

Mariusz Krzysztofek twierdzi,[220] że dla odróżnienia zestawu od zbioru kluczowa jest *Rzeczywista sprawna dostępność poszukiwanych danych osobowych*. Tu właśnie wskazany autor posługuje się przykładem, który zainspirował mnie do odróżnienia zbioru nośników od zbioru danych osobowych. Wskazany autor nie zastanawia się nad tym rozróżnieniem a różnicę miedzy zestawem a zbiorem widzi w sprawnej dostępności, której w zbiorze nośników zawierających nieuporządkowane dane nie widzi. Ja jej też nie widzę, argument M. Krzysztofka wydaje się racjonalny, tyle że jednak nijak nie wynikający z komentowanego przepisu.

3.3. Art. 4 pkt 6. Uwaga 3.
Forma danych w zbiorze

Niezwykle ciekawą, choć po wypowiedzeniu oczywistą, konstatację znajdziemy w komentarzu P. Litwińskiego, P. Barty i M. Kaweckiego, którzy zauważają, że: *Dane osobowe zawarte w zbiorze danych mogą być wyrażone w dowolny sposób, np. słowem, dźwiękiem, obrazem*[221].

[220] M. Krzysztofek, *loc. cit.*

[221] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 209.

3.4. Art. 4 pkt 6. Uwaga 4.
Ilość danych w zbiorze

Ciekawe rozważania prowadzą,[222] w Komentarzu, P. Litwiński, P. Barta i M. Kawecki w odniesieniu do ilości danych w zbiorze. Wskazani autorzy najpierw odnoszą się do poglądu J. Barty, P Fajgielskiego i R. Markiewicza z 2004 roku, z którego wynika, że nie może istnieć zbiór zawierający pojedyncza informacje o osobie.

Następnie wskazani autorzy odnoszą się do poglądu M. Sakowskiej zgodnie z którym, wedle słów wskazanych autorów: *ze zbiorem danych osobowych możemy mieć do czynienia już wówczas, gdy w zbiorze tym znajdują się dane jednej osoby*. Poglądu M. Sakowskiej nie uważam tu za rozstrzygający bowiem dane mogą być danymi jednej osoby, ale tych danych może być więcej niż jedna.

Własny pogląd P. Litwińskiego, P. Barty i M. Kaweckiego najlepiej oddaje zdanie: *W definicji zbioru danych osobowych użyte zostało pojęcie danych osobowych w liczbie mnogiej, co nakazuje przyjąć, że w skład zbioru danych muszą wchodzić co najmniej dwie informacje*.[223]

Poglądy każdego ze wskazanych autorów nie są pozbawione podstaw. Żaden jednak ze wskazanych autorów nie zwrócił uwagi na pewne zjawisko. Artykuł 2 ust. 1 RODO uzależnia stosowanie RODO między innymi od tego czy administrator przetwarza dane osobowe w sposób inny niż zautomatyzowany i jednocześnie te dane osobowe mają stanowić część zbioru danych. Widzimy zatem że prawodawca wiele uzależnia od tego czy dane osobowe mają stanowić części zbioru danych czy nie. W tym momencie należy wyobrazić sobie zbiór danych o którego powstaniu zdecydował administrator, do którego to zbioru jednak nie zdążono włączyć jeszcze żadnych danych. W trakcie działania administratora, który podjął decyzję o stworzeniu zbioru w pewnym momencie pojawiają się dane osobowe, które mają zostać włączone do zbioru. Skoro mają one zostać włączone do zbioru to RODO dotyczy przetwarzania tych danych osobowych. Następnie należy wyobrazić sobie, że administrator włącza do zbioru najpierw jed-

[222] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *loc. cit.* wskazują na: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 392.

[223] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *op. cit.* s. 210.

ną a następnie drugą daną. Jeżeli administrator włączył dane jednocześnie sytuacja wygląda nieco inaczej. Łatwo jednak można wyobrazić sobie sytuację, że administrator najpierw włącza jedną daną do zbioru. Sytuację taką można łatwo sobie wyobrazić tym bardziej, że w praktyce administratora, dane które mają stanowić część zbioru danych mogą pojawić się niejednocześnie. Najpierw w praktyce administratora pojawia się jedna taka dana, administrator włącza ją do zbioru. Administrator włącza ją do zbioru, w którym wcześniej nic nie było czyli administrator włącza ją do pustego zbioru. Wynika z tego że zbiór danych osobowych nie dość że może zawierać tylko jedną daną, to może on w ogóle nie zawierać danych. Dzieje się to w momencie kiedy żadna jeszcze dana nie została do zbioru włączona.

Pojawia się tu pewna ciekawostka. Jak wywiodłem wyżej, możliwe jest istnienie zbioru danych osobowych w którym nie ma jeszcze żadnych danych osobowych. Wydaje się jednak że niemożliwe jest istnienie zbioru, w którym znajduje się jedna tylko dana osobowa. Nie wynika to wcale z argumentów podanych przez wskazanych wyżej autorów, wynika to z czego innego. Otóż, co wywiodłem w uwadze *3.7. Art. 4 pkt 1. Uwaga 7. Dane osobowe a dana osobowa*, do definicji danych osobowych, dane osobowe mogą występować co najmniej po dwie. Niemożliwe jest występowanie jednej danej osobowej, ponieważ albo nie wiadomo byłoby co jest jej treścią, albo kogo ona dotyczy. Skoro najmniejsza możliwa ilość danych osobowych to dwie dane osobowe, to w takim razie najmniejsza możliwa ilość danych osobowych w zbiorze danych osobowych to również dwie dane osobowe.

Warto odnotować pogląd L. Kępy, wyrosły na żyznym gruncie UODO97. Autor ten pisze: „Dane osobowe ze względu na ich ilość, strukturę i kryteria dostępności dzieli się na:
- pojedyncze,
- w zestawach,
- w zbiorach.” [224].

To zestawienie jest poprawne, przez co warte odnotowania. Niestety dalej cytowany autor pisze: *Zestaw danych to po prostu pewna ilość danych osobowych w nieuporządkowanej formie (...)*.[225]

[224] L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 36.

[225] L. Kępa, *loc. cit.*

Dalej autor cytuje ustawowa definicję zbioru danych a jeszcze dalej pisze: *Z definicji ustawowej wynika, że dla istnienia zbioru musi się pojawić zestaw danych i określone kryteria dostępu (struktura). Za zestaw danych o charakterze osobowym rozumie się po prostu dane osobowe w pewnej ilości*.[226] O ile zgadzam się, że zbiór to zestaw plus kryteria dostępu, o tyle, przyznam, niepokoją mnie powtarzane słowa o „pewnej ilości danych". Chce się tu aż zapytać: „Pewnej czyli jakiej?". Publikacja L. Kępy ma charakter poradnikowy, została jednak ładnie napisana, tym bardziej brak mi poglądu autora na temat ilości danych w zbiorze lub zestawie.

3.5. Art. 4 pkt 6. Uwaga 5. Niemożność stworzenia jednoelementowego zbioru danych osobowych

Można wyobrazić sobie jedną sytuację, w której istnieje zbiór zawierający jedną tylko daną osobową. Jest to sytuacja, kiedy zbiór z założenia zawiera, a właściwie ma zawierać, dane osobowe dotyczące jednej tylko osoby. Administrator danych może założyć taki zbiór, zdecydować, że będą się w nim znajdować dane jednej tylko, konkretnej, oznaczonej osoby fizycznej. Kiedy do zbioru zostanie wprowadzona jedna informacja, to można dowodzić, ze to jest właśnie sytuacja zbioru, który zawiera jedną daną. Przykład jest, przyznaję to szczerze, wymyślony, jednak jest on możliwy w rzeczywistości. Dostrzegam tu jednak pewien problem. Jest to otóż przykład, w którym zbliżamy się do zjawiska zbioru danych osobowych zawierającego jedną daną, jednak zjawiska tego nie osiągamy. Nie osiągamy, ponieważ jedna dana znajdująca się w zbiorze, to w istocie dwie dane. Jeżeli na przykład jest to pomiar którejś z wartości spirometrycznych, zapisany w zbiorze tych wartości, mającym zawierać wyniki jednaj tylko osoby, to ten pomiar, ta jedna wartość spirometryczna, ta jedna dana osobowa to w istocie dwie dane. Dwie, ponieważ znamy wartość i wiemy kogo ona dotyczy, szerzej o tym, że niemożliwa jest „jedna dana osobowa" piszę w uwadze *3.7. Art. 4 pkt 1. Uwaga 8. Dane osobowe a dana osobowa*.

[226] L. Kępa, *loc. cit.*

4. Art. 4 pkt 6. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 6 RODO definiuje zbiór danych, zatem zgodnie z dyrektywą języka prawnego[227], każdy kto interpretuje RODO powinien rozumieć pojęcie „zbiór danych" tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „zbiór danych" tak jest ono zdefiniowane w art. 4 pkt. 6 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „zbiór danych" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4. pkt 5. Konkretyzacja zasad

Związek pojęcia *zbiór danych* z zasadami jak i z całym RODO jest ważny i bardzo bliski. Wynika on z art. 2 ust. 1 RODO. Jeżeli administrator przetwarza dane w sposób inny niż zautomatyzowany i dane te nie stanowią części zbioru lub nie mają stanowić części zbioru a jedynie stanowią część zestawu danych lub mają stanowić część zestawu danych to RODO nie ma zastosowania do danego przetwarzania danych osobowych. Jak więc widać zakres pojęcia *zbiór danych* ma znaczny wpływ na to czy do danego przetwarzania RODO ma zastosowanie czy nie.

Jeżeli RODO nie ma zastosowania do danego przetwarzania danych osobowych to oczywiste jest że zastosowania tego nie ma do danego przetwarzania danych osobowych całe RODO w tym oczywiście również zasady dotyczące przetwarzania danych osobowych z art. 5 RODO.

[227] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

6. Art. 4 pkt 6. Postulaty de lege ferenda
6.1 Art. 4 pkt 6. Postulat 1.
Doprecyzowanie treści przepisu

W uwadze *3.1. Art. 4 pkt 6. Uwaga 1. Kryteria a kryterium*. wyjaśniłem jak wiele zależy od tego że dla uporządkowania zestawu danych tak aby stał się zbiorem konieczne są dwa kryteria porządkujące, nie wystarczy zaś jedno. Przedstawione tam rozumowanie wynika z obecnej treści przepisu, nie oznacza to jednak, że treść ta jest poprawna. Obecna treść przepisu, uzależniająca istnienie zbioru danych od dwóch kryteriów porządkujących zestaw, jest, w pewnym sensie, krzywdząca dla osób których dane dotyczą. Skoro przetwarzanie danych w zestawie porządkowaniem przy pomocy jednego tylko kryterium lub mających się znaleźć w takim zestawie nie skutkuje obowiązkiem stosowania RODO to może się zdarzyć że podmiot będzie przetwarzał dane osobowe właśnie w takim zestawie po to tylko by przetwarzania tego nie dotyczyły przepisy RODO. Przeciwdziałać temu można w jeden tylko sposób a mianowicie nowelizując komentowany przepis.

W związku z powyższym postuluję nowelizację art. 4 pkt 6 RODO poprzez dodanie słów: „określonego kryterium lub" między słowami: *według* a *określonego kryterium*.

Przepis po nowelizacji miałby postać:

„„**zbiór danych**" oznacza uporządkowany zestaw danych osobowych dostępnych według określonego kryterium lub określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;" (Czcionką podkreśloną zaznaczam słowa dodane.)

Artykuł 4 pkt 7 RODO

„administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

1. Art. 4 pkt 7. Komentarz

Administratorem danych może być każdy z podmiotów wymienionych w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków.

- Administratorem danych może być osoba fizyczna.
- Administratorem danych może być osoba prawna.
- Administratorem danych może być organ publiczny.
- Administratorem danych może być jednostka.
- Administratorem danych może być inny podmiot.
- Administratorem może być każdy podmiot lub osoba.

Warunkiem by wymieniony podmiot był administratorem (danych osobowych) jest, by ten podmiot samodzielnie lub wspólnie z innymi ustalał cele i sposoby przetwarzania danych osobowych.[228]

Jeśli chodzi o podmioty publiczne, działające w zamkniętych ramach prawa administracyjnego, to podmioty te nie ustalają celów przetwarzania danych osobowych. Cele te ustala prawodawca.

Administrator może cele i sposoby przetwarzania danych osobowych ustalać samodzielnie, oraz administrator może cele i sposoby przetwarzania danych osobowych ustalać wspólnie z innymi admi-

[228] Podobnie: M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Część I ZAGADNIENIA OGÓLNE ORAZ PROCES PRZETWARZANIA DANYCH OSOBOWYCH W JEDNOSTKACH ORGANIZACYJNYCH POMOCY SPOŁECZNEJ. 4.Administrator danych osobowych,* Warszawa 2019, Lex.

nistratorami. Przepis odnosi się tu do zjawiska współadministrowania, opisanego w art. 26 RODO.

Jeżeli cele i sposoby przetwarzania danych osobowych są określone w prawie UE lub w prawie państwa członkowskiego, to również w prawie UE lub w prawie państwa członkowskiego może zostać wyznaczony administrator danych osobowych, oraz, że w prawie UE lub w prawie państwa członkowskiego mogą zostać określone kryteria wyznaczenia administratora danych osobowych.

2. Art. 4 pkt 7. Analiza

Ze słów: „**oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, (…)" wynika, że administratorem danych może być każdy z podmiotów wymienionych w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków.
Administratorem danych może być osoba fizyczna.
Administratorem danych może być osoba prawna.
Administratorem danych może być organ publiczny.
Administratorem danych może być jednostka.
Administratorem danych może być inny podmiot.

Jak widać z powyższego wyliczenia, administratorem może być każdy podmiot lub osoba.

Ze słów wytłuszczonych w przepisie: „oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, **który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych** (…)" wnioskujemy, że warunkiem by wymieniony wyżej podmiot lub osoba był administratorem danych osobowych jest, by ten podmiot lub osoba samodzielnie lub wspólnie z innymi ustalał cele i sposoby przetwarzania danych osobowych. Jeśli chodzi o podmioty publiczne, działające w zamkniętych ramach prawa administracyjnego, to podmioty te nie ustalają celów przetwarzania danych osobowych. Cele te ustala prawodawca. Co więcej, sposoby przetwarzania danych osobowych w podmiotach publicznych, również bardzo często, przynajmniej w pewnym zakresie, ustala prawodawca. Nie sposób przyjąć, że prawodawca jest administratorem danych osobowych w podmiotach publicznych, należy więc przyjąć że podmiot publiczny jest administratorem danych jeżeli

ustala sposoby przetwarzania danych osobowych. Takie rozwiązanie jest najprostsze, pomija się tu jednak kwestię ustalania celów. Można udać, że problemu tego nie ma. Można uznać, że prawodawca się tu pomylił. Można wreszcie uznać, że racjonalny prawodawca przyjął założenie, że o ile, w odniesieniu do podmiotu publicznego, prawodawca ustala cele przetwarzania danych ogólnie – tworząc przepisy, o tyle podmioty publiczne ustalają szczegółowe cele przetwarzania danych osobowych – stosując przepisy. Trzecia z podanych interpretacji jest najbardziej przychylna wobec prawodawcy, nie można jednak ukrywać, że przepis nie jest napisany perfekcyjnie.

Nie od rzeczy jest tu zacytować P. Litwińskiego, P. Bartę i M. Kaweckiego, którzy trafnie zauważają w definicji administratora *Dwa konstytutywne elementy tego pojęcia: ustalanie celów przetwarzania danych osobowych oraz ustalanie sposobów przetwarzania danych*.[229]

Znaczący, dla prowadzonych tu rozważań pogląd wyraził M. Gumularz, autor ten stwierdza: *Można powiedzieć w uproszczeniu, że nie ma procesu przetwarzania danych, w którym nie byłoby administratora danych, chociaż przypisanie tego statusu może rodzić wątpliwości*.[230] Na pewno zgadzam się z drugą częścią myśli M. Gumularza, prawdą jest bowiem, że czasem trudno ustalić kto jest administratorem danych. Nie jestem w pełni przekonany czy zgadzam się z pierwszą częścią cytowanej myśli. Być może moja częściowa wątpliwość wynika z tego, że sam M. Gumularz sygnalizuje, że myśl jego jest pewnym uproszczeniem. Mirosław Gumularz twierdzi, że *nie ma procesu przetwarzania danych, w którym nie byłoby administratora danych*, czyli jeżeli ktoś robi coś z danymi, to zawsze gdzieś w tle jest administrator. Mam tu pewną wątpliwość. Wyobraźmy sobie faktury, które należało zniszczyć, ich wystawca miał je zniszczyć, nie zniszczył jednak – nie zdążył. Złodziej ukradł faktury, po czym je porzucił. Kto jest administratorem? Może nadal wystawca, może złodziej, może nikt. Przykład jest celowo wymyślony tak, by utrudniał odpowiedź,

[229] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 217.

[230] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział III. GŁÓWNI AKTORZY RODO. 1. Administrator danych. 1.1. Informacje ogólne,* Warszawa 2018, Lex.

ale właśnie w takich sytuacjach okazuje się czasem, że trudne przypadki skutkują dobrym prawem, że strawestuję myśl H. L. A. Harta.

Ciekawa jest uwaga B. van Alsenoya, który twierdzi,[231] że kluczowym elementem bycia administratorem jest element rzeczywistego wpływu tego podmiotu na przetwarzanie danych.

Ze słów wytłuszczonych w przepisie: „oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala** cele i sposoby przetwarzania danych osobowych; (…)" wnioskujemy, że administrator danych może cele i sposoby przetwarzania danych osobowych ustalać samodzielnie, oraz, że administrator danych może cele i sposoby przetwarzania danych osobowych ustalać wspólnie z innymi administratorami. Przepis odnosi się tu do zjawiska współadministrowania, opisanego w art. 26 RODO. Wnioskujemy to z faktu, że art. 26 RODO zaczyna się od słów: *Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami*.

Ze słów wytłuszczonych w przepisie: „(…) **jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania**;" wnioskujemy, że jeżeli cele i sposoby przetwarzania danych osobowych są określone w prawie UE lub w prawie państwa członkowskiego, to również w prawie UE lub w prawie państwa członkowskiego może zostać wyznaczony administrator danych osobowych, oraz, że w prawie UE lub w prawie państwa członkowskiego mogą zostać określone kryteria wyznaczenia administratora danych osobowych. Zwracam uwagę, na fakt, że możliwość wyznaczenia administratora w prawie, uzależniono od tego, że również cele i sposoby przetwarzania są wyznaczone w prawie.

[231] B. van Alsenoy, *Data protection law in the EU: Roles, responsibilities and liability,* Intersentia 2019, s. 55.

3. Art. 4 pkt 7. Uwagi
3.1. Art. 4 pkt 7. Uwaga 1.
Kto może być administratorem

Analiza definicji administratora, zwłaszcza słów: „**oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, (…)" prowadzi do wniosku, że administratorem może być każdy podmiot lub osoba.[232] Pragnę zwrócić uwagę na fakt, że nie jest konieczne by administrator posiadał zdolność do czynności prawnych[233] lub osobowość prawną.

Warto w tym miejscu zastanowić się nad jednym problemem. A mianowicie czy czynności z zakresu RODO to czynności prawne. Czy umowa powierzenia przetwarzania to naprawdę umowa. Jeśli umowa powierzenia przetwarzania nie jest umową, to czym jest? Zjawiskiem sui generis? Chyba nie. Czy upoważnienie do przetwarzania danych osobowych to pełnomocnictwo do wykonania czynności czy coś zupełnie innego? Odpowiedź na te pytania nie jest łatwa, staram się jej udzielać w odpowiednich miejscach niniejszej książki i książek towarzyszących.

3.2. Art. 4 pkt 7. Uwaga 2.
Kto może być administratorem, ciąg dalszy

Analiza definicji administratora może prowadzić do pochopnego wniosku, że w administracji bardzo trudno jest wskazać administratora na gruncie komentowanego przepisu. Lektura komentowanego przepisu wskazuje zrazu na fakt że administratorem jest podmiot który *ustala cele i sposoby przetwarzania danych osobowych*. W tym miejscu pojawia się wątpliwość: kto jest administratorem w administracji samorządowej jak i rządowej skoro organy administracji działają na podstawie i w granicach prawa. Z działania organów administracji na podstawie i w granicach prawa wynika że przynajmniej cele przetwarzania danych osobowych przez organy administracji, określone są w przepisach, co budzi wątpliwość czy organy admini-

[232] Podobnie: B. van Alsenoy, *Data protection law in the EU: Roles, responsibilities and liability,* Intersentia 2019, s 54-55.

[233] Podobnie: P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 222.

stracji są administratorami danych skoro nie określają celów przetwarzania danych.

Kiedy uświadomimy sobie że w komentowanym przepisie jest przecież mowa o określaniu celów i sposobów przetwarzania danych w prawie to okazuje się, że problem ze wskazaniem administratorów w administracji rządowej i samorządowej znika. Z przepisów prawa wynikają obowiązki organów administracji tym samym z przepisów prawa wynikają cele przetwarzania danych osobowych. Z komentowanego przepisu absolutnie nie wynika że jeżeli prawo decyduje o celach przetwarzania danych to prawo musi również decydować o tym kto jest administratorem. Komentowany przepis stanowi jedynie że w prawie może zostać wyznaczony administrator lub kryteria jego wyznaczenia. Może zostać wyznaczony. RODO pozostawia kwestię wyznaczenia administratora lub określenia kryteriów jego wyznaczenia do decyzji prawodawców krajowych lub prawodawcy unijnego. Jeżeli prawodawcy ci nie wskażą administratora lub kryteriów jego wyznaczenia to administratora trzeba wskazać na gruncie przepisów RODO i absolutnie nie stoi temu na przeszkodzie fakt że cele przetwarzania danych przez podmiot, który zamierzamy wskazać jako administratora zostały określone w przepisach prawa.

Problem administratora danych w administracji omawiam wyżej rozważając przy tej okazji kwestie celów przetwarzania danych. Omawiany przepis stanowi również o sposobach przetwarzania danych. Administrator to ten kto określa cele lub sposoby lub za którego cele i sposoby zostały określone w prawie Unii lub w prawie krajowym. Wydaje się, że jeśli chodzi o sposoby przetwarzania danych to nie ma tutaj problemu interpretacyjnego, ponieważ za sposoby przetwarzania danych można uznać po prostu rozliczne przepisy postępowań zgodnie z którymi to przepisami administratorzy mają obowiązek realizować swoje obowiązki materialne.

Z problemem administratora którego obowiązki zostały uregulowane w przepisach prawa zmagają się P. Litwiński, P. Barta i M. Kawecki. Twierdzą oni że w przypadku takich administratorów należy inaczej rozumieć *przesłankę decydowania o celach i sposobach przetwarzania danych osobowych*[234]. Twierdzą oni dalej, że: *swoboda w zakresie osobowych jest wyznaczana przez właściwe przepisy prawa*

[234] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *op. cit.* s. 223.

określające realizowane przez nie zadania[235]. Lektura cytowanego zdania w pierwszej chwili budzi sprzeciw wydaje się bowiem że jeżeli administrator ma decydować o celach i środkach przetwarzania danych to powinien móc on rzeczywiście decyzję w tej kwestii podejmować w sposób swobodny nie zaś związany przepisami prawa. Po chwili sprzeciw ten jednak wydaje się nieracjonalny, kiedy uświadomimy sobie że wiele decyzji podejmowanych, i to nie tylko przez podmioty ze sfery prawa publicznego, podejmowanych jest w ramach pewnej swobody wyznaczonej przepisami. Mogę się ze wskazanymi autorami tu zgodzić, acz zgoda ta ma charakter częściowy i roboczy. Wskazani autorzy dwukrotnie jeszcze na tej samej stronie swojego Komentarza wywodzą tezę sprowadzającą się do tego że administrator ze sfery prawa publicznego czy to decyduje *o celach i sposobach przetwarzania danych* osobowych w *granicach zakreślonych* przepisami czy to administrator ze sfery prawa publicznego jedynie konkretyzuje cele wskazane przepisami.[236]

Tak czy inaczej wskazani autorzy zdają się robić dobrą minę do złej gry i na siłę szukają sposobu wyjaśnienia dzięki któremu można uzasadnić, że administrator ze sfery prawa publicznego który tak naprawdę nie decyduje o celach i sposobach przetwarzania danych, w istocie jednak decyduje o tych celach i sposobach, tyle że w sposób ograniczony, nieswobodny, czy też nie tyle decyduje ile je konkretyzuje. Świadomie piszę o uzasadnieniu na siłę uważam bowiem że administratorzy z dziedziny prawa publicznego w istocie o niczym w zakresie przetwarzania danych nie decydują. Jeżeli na przykład człowiek przysyła do takiego administratora podanie, to wtedy administrator ten ma związane z tym podaniem pewne obowiązki, nie ma on przed sobą decyzji dotyczącej określenia celów i sposobów postępowania z danymi dostarczonymi w podaniu. Celem działań administratora jest załatwienie sprawy, sposoby określone są w przepisach proceduralnych, administrator tak naprawdę o niczym nie decyduje.

Ciekawy wniosek dla określania kto jest administratorem danych wynika z wypowiedzi M. Bochenka. Autor ten definiuje administratora danych w sposób następujący: *Administrator danych osobowych (ADO) – reprezentowany przez dyrektora ...., podejmującego*

[235] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *loc. cit.*

[236] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *loc. cit.*

czynności administratora danych osobowych[237]. Pomijam niedoskonałość tej definicji, nie jest moim celem polemika z jej autorem, swoje zdanie w kwestii znaczenia definicji wyraziłem wyżej w niniejszym podrozdziale. Tu zwracam jedynie uwagę na fakt, że cytowany autor stwierdził, że administrator jest przez dyrektora jedynie reprezentowany. Drugi wartościowy wniosek wypływający z wypowiedzi M. Bochenka jest taki, że dyrektor podejmuje czynności administratora danych, jednak sam nim nie jest.

Ciekawa jest również jedna jeszcze wypowiedź M. Bochenka, który zrazu pisze: *Nie można jednak nie zauważyć, że to OPS, wykonując ustawowe zadania z zakresu np. świadczeń rodzinnych, funduszu alimentacyjnego, pomocy materialnej dla uczniów (stypendia i zasiłki szkolne), samodzielnie lub wspólnie z innymi podmiotami (m.in. wójt gminy) ustala cele i sposoby przetwarzania danych przedmiotowych danych osobowych*[238] – z tej wypowiedzi nie dowiadujemy się wiele, poza tym, że jej autor umie dokonać subsumpcji, jednak dalej ten sam autor pisze: *Wszystko to w efekcie oznacza, że to OPS w ramach konkretnych postępowań samodzielnie ustala cele i sposoby przetwarzania danych osobowych w rozumieniu art. 4 pkt 7 RODO*[239].

Drugi z zacytowanych poglądów M. Bochenka jest niezwykle doniosły, zwłaszcza w świetle pierwszego. Pierwszy jest po prostu relacją stanu prawnego, w drugim, jego autor przejawia własny, oryginalny, wartościowy pogląd. Uogólniając ten pogląd można stwierdzić, że podmiot publiczny jest administratorem ponieważ ustala cele i sposoby (…) w ramach konkretnych postępowań. Czyli ogólnie celem podmiotu jest wydawanie decyzji w takiej to a takiej kategorii spraw – to nie czyni go administratorem, jednak szczególnie, w konkretnej sprawie, podmiot ustala cele i sposoby …, co czyni go administratorem.

[237] M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Kto jest administratorem niżej wskazanych zbiorów danych – wójt czy GOPS?* Warszawa 2019, Lex.

[238] M. Bochenek, *loc. cit.*

[239] M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Część I ZAGADNIENIA OGÓLNE ORAZ PROCES PRZETWARZANIA DANYCH OSOBOWYCH W JEDNOSTKACH ORGANIZACYJNYCH POMOCY SPOŁECZNEJ. 4. Administrator danych osobowych,* Warszawa 2019, Lex.

3.3. Art. 4 pkt 7. Uwaga 3.
Administrowanie danymi a posiadanie danych

Ciekawą konstatację znaleźć można w Komentarzu P. Litwińskiego, P. Barty i M. Kaweckiego, którzy trafnie zauważają, że administrator nie musi posiadać danych, że administrator sprawuje władztwo nad danymi, sprawuje faktyczną kontrolę nad przetwarzaniem danych.[240] Dodam tu tylko, że możliwa jest sytuacja, w której administrator nie dość, że nie posiada danych osobowych, to prawie wcale się z nimi nie styka. Wystarczy wyobrazić sobie sytuację biznesową, w której administrator powierza przetwarzanie danych rozmaitym zleceniobiorcom, a tam gdzie nie powierza przetwarzania tam po prostu zleca wykonanie usług związanych z przetwarzaniem danych, jednak nie mających charakteru przetwarzania danych osobowych w imieniu administratora. Zleceniobiorcy zbierają dla administratora zamówienia, podpisują umowy w imieniu administratora, obsługują pozyskiwanie towarów, wysyłają towary do kupujących. Administrator nie styka się z danymi, jednak poprzez swoje know-how decyduje o celach przetwarzania danych osobowych a poprzez wybór zleceniobiorców decyduje o środkach przetwarzania danych osobowych.

Ciekawym uzupełnieniem może być tu uwaga T. Izydorczyka, który stwierdza, że: *Bycie ADO to okoliczność faktyczna. Zlecający organizację konkursu oraz agencja przyjmująca zlecenie nie mogą się umówić, kto będzie administratorem danych.*[241]. Tomasz Izydorczyk pisze tu o byciu administratorem w realiach konkursów, takowych bowiem realiów dotyczy jego artykuł, jednak cytowane stwierdzenie ma charakter uniwersalny, a z uwagi na swoją hasłowość, (zwłaszcza pierwsze z cytowanych zdań) warte jest zacytowania. Z drugiej strony, nie należy zapominać o elemencie władczym po stronie administratora, na co zwraca uwagę A. Sobczyk[242] Do poglądów A. Sobczyka odnoszę się również niżej, w uwadze *3.5. Art. 4 pkt 7. Uwaga 9. Organ władzy publicznej jako administrator*.

---

[240] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *op. cit.* s. 217.

[241] T. Izydorczyk, ADO w konkursach i loteriach marketingowych. ABI Expert 1(2). s. 41-43.

[242] A. Sobczyk, *RODO. Rozproszona władza publiczna,* Kraków 2019, s. 58.

3.4. Art. 4 pkt 7. Uwaga 4.
Administrator, podmiot przetwarzający, odbiorca

Administrator, podmiot przetwarzający i odbiorca to podmioty zdefiniowane w sąsiadujących ze sobą w przepisach RODO. Każde z tych pojęć doczekało się oczywiście osobnego omówienia. W tym miejscu publikacji, żeby ułatwić odróżnienie administratora od pozostałych dwóch podmiotów omawiam rzecz w skrócie i w pewnym uproszczeniu.

Administrator to podmiot który decyduje o celach i środkach przetwarzania danych osobowych.

Odbiorca to podmiot któremu ujawnia się dane osobowe, bardzo często odbiorca staje się lub w momencie ujawnienia już jest, nowym administratorem ujawnionych danych.

Należy zwrócić uwagę, że administrator przetwarza dane osobowe w oparciu o właściwą dla siebie podstawę prawną. Następnie administrator danych w oparciu o odpowiednią podstawę prawną ujawnia dane osobowe odbiorcy. Jeżeli przetwarzanie danych osobowych przez odbiorcę mieści się w zakresie RODO, to odbiorca staje się nowym administratorem. Oczywiście odbiorca by móc zgodnie z prawem przetwarzać dane osobowe, które ujawnił mu pierwotny administrator, musi posiadać odpowiednią ku temu podstawę prawną. Należy zwrócić uwagę że odbiorca ma własną podstawę prawną do przetwarzania danych osobowych inną niż podstawa prawna z której korzysta pierwotny administrator. Może się oczywiście zdarzyć że są to te same przepisy RODO lub te same przepisy szczególne.

Podmiot przetwarzający przetwarza dane osobowe w imieniu administratora. Co do zasady podmiot przetwarzający przetwarza dane osobowe na podstawie umowy powierzenia przetwarzania. Może się zdarzyć, że podmiot przetwarzający przetwarza dane osobowe w imieniu administratora mimo że nie łączy go z administratorem umowa powierzenia przetwarzania co jest rozwiązaniem niewłaściwym jednak czasem spotykanym. Szerzej piszę o tym w omówieniu art. 4 pkt 8 RODO, w uwadze *3.7. Art. 4 pkt 8. Uwaga 7. Bezumowne powierzenie przetwarzania danych osobowych a prowadzenie cudzych spraw bez zlecenia*.

Pomijając tę nietypową sytuację kiedy podmiot przetwarzający przetwarza dane osobowe w imieniu administratora jednak bez umowy powierzenia, podstawą prawną do przetwarzania danych osobowych przez podmiot przetwarzający jest właśnie umowa powierzenia

przetwarzania łącząca podmiot przetwarzający z administratorem. Umowa powierzenia przetwarzania zawarta między administratorem a podmiotem przetwarzającym reguluje relacje między tymi dwoma podmiotami, tworzy po stronie podmiotu przetwarzającego uprawnienie do przetwarzania danych osobowych. Jeżeli jednak chcemy prześledzić całą podstawę prawną przetwarzania danych osobowych przez podmiot przetwarzający, to podstawa ta składa się z dwóch elementów. Pierwszy z nich to podstawa prawna przetwarzania danych przez administratora, drugi z nich to umowa łącząca administratora z podmiotem przetwarzającym.

Jeśli chodzi o przetwarzanie danych osobowych w imieniu administratora, to należy zwrócić uwagę na art. 28 ust. 19 RODO. Z przepisu tego wynika, że jeżeli podmiot przetwarzający przetwarza dane osobowe w innym celu niż wynika to z umowy z administratorem, lub w inny sposób, to w zakresie tego przetwarzania, podmiot ten jest administratorem. Artykuł 28 ust 10 jest niestety napisany niejasno, stanowi on bowiem, że *(...) jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania*. Ja rozumiem ten przepis tak jak wskazałem wyżej. Niestety pozwala on również na inną interpretację, trudno bowiem powiedzieć co tak naprawdę oznaczają słowa o naruszeniu RODO przy określaniu celów i sposobów przetwarzania. Uważam jednak, że zwłaszcza w zakresie celów przetwarzania, jeżeli podmiot przetwarzający przetwarza dane w mniejszej liczbie celów niż ustalił to z administratorem lub jeżeli podmiot przetwarzający przetwarza dane osobowe w węższym zakresie niż to ustalił z administratorem to nie sposób uznać, że staje się on administratorem.[243]

3.5. Art. 4 pkt 7. Uwaga 5.
Administrator, a osoba kierująca administratorem

Definicja administratora jest daleka od precyzji. Istotą jej treści jest konstatacja, że administratorem może być każdy kto decyduje o celach i sposobach przetwarzania danych. Ustalając takie znaczenie definicji, żyjemy przez chwilę w mylnym przeświadczeniu, że wiemy

[243] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział III. GŁÓWNI AKTORZY RODO. 1.Administrator danych. 1.1.Informacje ogólne,* Warszawa 2018, Lex.

kto jest administratorem, kiedy jednak z poziomu przepisu przechodzimy na poziom jego stosowania w praktyce, czyli kiedy dokonujemy subsumpcji, to okazuje się, że w konkretnych przypadkach niekoniecznie wiemy kto jest administratorem. Czy administratorem jest jednostka czy administratorem jest podmiot czy osoba nim kierująca? Należy przyjąć, że administratorami są podmioty, nie zaś osoby nimi kierujące. Wskazuję poniżej pewną ilość przykładów, które mogą przybliżyć zagadnienie.

Jednoosobowa działalność gospodarcza – administratorem jest osoba prowadząca te działalność, ale dlatego, że w tej formie prawnej działania, podmiot w zasadzie nie istnieje.

Spółka cywilna – administratorem jest spółka, acz można spotkać się w praktyce z poglądem, że administratorami są wspólnicy działający w warunkach współadministrowania.

Spółka jawna, spółka z ograniczoną odpowiedzialnością, spółka komandytowa, spółka akcyjna – administratorem jest spółka.

Szkoła publiczna – administratorem jest szkoła, nie dyrektor.

Szkoła wyższa – administratorem jest szkoła, nie rektor, nie senat.

Gmina – administratorem jest gmina i administratorem jest wójt we współadministrowaniu (analogicznie powiat)

Ośrodek pomocy społecznej – administratorem jest ośrodek. Ten sam pogląd wyraża M. Bochenek, zwracając przy tym uwagę na fakt, że „że operacje na danych osobowych w ośrodku pomocy społecznej (OPS) są wykonywane przez kierownika/dyrektora jako kierującego jednostką sektora finansów publicznych – podmiotem publicznym, która jest administratorem danych osobowych (ADO).”[244].

Pogląd zgodnie z którym to spółka jest administratorem nie zaś wspólnicy spółki prezentują autorzy poradnika dla radców prawnych i adwokatów, w którym znajdujemy słowa: *jeżeli radca prawny lub adwokat wykonuje zawód w spółce osobowej lub spółce cywilnej, za administratora danych osobowych przetwarzanych w ramach wykonywania zawodu radcy prawnego należy uznać samą spółkę osobową lub spółkę cywilną, a nie radcę prawnego bądź adwokata będącego wspólnikiem, partnerem albo komplementariuszem takiej spółki. Decyzje co do celów i sposobów przetwarzania danych osobowych podejmowane są w ramach spółki, a nie na szczeblu indywidualnego*

[244] M. Bochenek, *loc. cit.*

radcy prawnego czy adwokata wykonującego w niej zawód[245]. Zacytowany tu pogląd odnosi się do działalności radcowskiej i adwokackiej, nie ma jednak powodu by uważać, że do innej nie. Autorzy cytatu pogląd swój, z którym się zgadzam, wspierają odwołaniem do stanowiska PUODO i do wyroku WSA w warszawie.

Ciekawy pogląd w tej kwestii prezentuje M. Gumularz, który twierdzi, że w obrocie cywilnoprawnym *to nie organ jednostki występuje jako podmiot praw i obowiązków, ale jednostka samorządu terytorialnego jako taka*[246], więc *administratorem danych osobowych przetwarzanych w związku z występowaniem jednostki samorządu terytorialnego w obrocie cywilnoprawnym (np. dane osobowe dłużników) będzie jednostka samorządu terytorialnego, a nie jej organ*[247]. Przyznam, że mam tu wątpliwość. Zgadzam się, że w obrocie cywilnoprawnym, administratorem danych jest jednostka samorządu terytorialnego, uważam jednak, że również poza tym obrotem, kiedy jednostka realizuje swoje obowiązki w sferze imperium, wtedy również nie organ jednostki ale jednostka jest administratorem danych. Nie dostrzegam realnej możliwości uzasadnienia poglądu M. Gumularza.

3.5. Art. 4 pkt 7. Uwaga 6.
Podmiot przetwarzający a odbiorca

Kolejną rzeczą na którą należy tu zwrócić uwagę jest odpowiedź na pytanie o to czy podmiot przetwarzający jest odbiorcą. Uważam że podmiot przetwarzający nie jest odbiorcą. PUODO uważa, że podmiot przetwarzający jest odbiorcą.[248] Z ostrożności należy (niestety) zgadzać się z błędnym stanowiskiem PUODO. Tym niemniej przedstawiam poniżej swoje stanowisko.

---

[245] *Poradnik dla radców prawnych i adwokatów. Ogólne rozporządzenie o ochronie danych (RODO)*. X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka, s. 27.

[246] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział. V. PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH. 1. Podstawy (warunki) przetwarzania danych osobowych zwykłych. 1.3. Zawarcie i realizacja umowy,* Warszawa 2018, Lex.

[247] M. Gumularz, *loc. cit.*

[248] Urząd Ochrony Danych Osobowych, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*. Brak daty, miejsca wydania, autora publikacji. s. 8. Publikacja dostępna ze strony: https://uodo.gov.pl/pl/383/214. (dostęp: 2020.08.10. godz. 16.33.)

Uważam że pogląd zgodnie z którym podmiot przetwarzający nie jest odbiorcą można uzasadnić na kilka sposobów.

Pierwszym argumentem stojącym za stanowiskiem, że podmiot przetwarzający nie jest odbiorcą, jest zakaz wykładni synonimicznej[249]. Nie wolno otóż interpretować dwóch różnych pojęć w jednym akcie prawnym tak że znaczą one to samo. Zakaz wykładni synonimicznej jest argumentem jak najbardziej na miejscu jednak nie jest on argumentem przesądzającym, można bowiem wysnuć stanowisko zgodnie z którym podmiot przetwarzający nie jest tożsamy z odbiorcą natomiast zakres pojęcia: „odbiorca" mieści w sobie zakres pojęcia: „podmiot przetwarzający". Innymi słowy odbiorcy stanowią duży zbiór do którego między innymi należą podmioty przetwarzające.

Drugim argumentem stojącym za stanowiskiem, że podmiot przetwarzający nie jest odbiorcą, jest różniąca te podmioty podstawa prawna przetwarzania danych osobowych. Odbiorca przetwarza dane osobowe w oparciu o własną podstawę prawną zwłaszcza odbiorca stający się administratorem. Podmiot przetwarzający przetwarza dane osobowe w oparciu o podstawę prawną administratora i umowę powierzenia przetwarzania.

Trzecim argumentem stojącym za stanowiskiem, że podmiot przetwarzający nie jest odbiorcą, jest to, że odbiorca czasem, choć nie zawsze może stać się administratorem. Jeżeli odbiorca znajduje się w zakresie RODO i jeżeli przetwarzanie danych osobowych przez odbiorcę znajduje się w zakresie RODO, to odbiorca automatycznie staje się administratorem. Podmiot przetwarzający nigdy automatycznie administratorem się nie staje. Możliwe są sytuacje kiedy podmiot przetwarzający staje się administratorem na przykład z mocy prawa lub niezgodnie z prawem, są to jednak sytuacje absolutnie wyjątkowe, kiedy to rola administratora nakłada się na rolę podmiotu przetwarzającego.

[249] M Zirk-Sadowski w: *System Prawa Administracyjnego* Red: R Hauser, Z Niewiadomski, A Wróbel, *Tom IV. Wykładnia w prawie administracyjnym.* L. Leszczyński, B. Wojciechowski, M. Zirk-Sadowski, Warszawa 2012, s. 200.

3.5. Art. 4 pkt 7. Uwaga 7.
Rozróżnienie
między administratorem a podmiotem przetwarzającym
jako zagrożenie odpowiedzialnością

Niezwykle istotna jest różnica między administratorem danych (osobowych) a podmiotem przetwarzającym. Różnica ta jest o tyle istotna, że, jeżeli podmiot jest jednym bądź drugim, to powinien być w stanie ustalić czy jest administratorem czy podmiotem przetwarzającym. Jeżeli podmiot któremu udostępniane są dane osobowe jest podmiotem przetwarzającym, to podstawowe jego obowiązki w zakresie ochrony danych wynikają z umowy powierzenia przetwarzania, którą podpisał z administratorem. Jeżeli podmiot któremu udostępniane są dane jest nowym administratorem, to po prostu spoczywają na nim obowiązki administratora.

W tym właśnie miejscu może pojawić się problem. Problem może pojawić się wtedy, jeżeli podmiot któremu udostępnione są dane mylnie przyjmuje, że jest podmiotem przetwarzającym podczas gdy w istocie jest administratorem danych.

Mylne uznanie się przez podmiot za podmiot przetwarzający nie zaś za administratora danych może się zdarzyć szczególnie wtedy kiedy między administratorem a podmiotem któremu udostępniane, ujawniane są dane osobowe podpisana zostaje umowa powierzenia przetwarzania. Należy podkreślić że umowa powierzenia przetwarzania nie ustanawia między stronami umowy relacji, którą można określić jako: „administrator/podmiot przetwarzający". Podmiot przetwarzający zdefiniowany jest w artykule 4 pkt 8 RODO i definicja tego podmiotu w żaden sposób nie jest związana z umową powierzenia przetwarzania. Jeżeli zatem administrator udostępni dane innemu podmiotowi, który staje się nowym administratorem i jednocześnie podpisze z tym podmiotem umowę powierzenia przetwarzania to taki podmiot – (nowy) administrator nie staje się w wyniku podpisania tej umowy podmiotem przetwarzającym. Podmiot taki – (nowy) administrator może jednak uważać, że skoro podpisano z nim umowę powierzenia przetwarzania to w wyniku podpisania tej umowy stał się podmiotem przetwarzającym, w związku z czym nie spoczywają na nim obowiązki które spoczywają na administratorze danych. Pierwszym obowiązkiem którego nowy administrator uważający że jest podmiotem przetwarzającym nie realizuje jest obowiązek informacyj-

ny wynikający z artykułu 14 RODO. Opisany tu problem może skutkować odpowiedzialnością administracyjną i cywilną po stronie (nowego) administratora który uważa jest podmiotem przetwarzającym.

Szerzej zagadnienia te opisuję w omówieniu definicji podmiotu przetwarzającego.

3.5. Art. 4 pkt 7. Uwaga 8.
Dane niepożądane przez administratora

Ciekawym problemem praktycznym jest problem posiadania przez administratora danych, których administrator posiadać nie chce. Nie chce posiadać, zebrał je przypadkowo, wbrew swej woli. Można próbować postawić sobie pytanie, czy w takiej sytuacji podmiot, któremu narzucono przetwarzanie danych osobowych jest wobec tych danych administratorem. Najczęstszym, jak się wydaje przykładem praktycznym jest sytuacja, w której podmiot posiada publicznie dostępną skrzynkę poczty elektronicznej i dostaje tam zarówno informacje oczekiwane, pożądane, takie jakich cel przyświecał założeniu tej skrzynki, jak i inne – przypadkowe, spam.

Problem nad którym się tu zastanawiamy jest następujący: podmiot posiada publicznie dostępny adres poczty elektronicznej, czy podmiot ten jest administratorem wszystkich danych osobowych znajdujących się w jego skrzynce pocztowej. Na pewno zagadnieniu należy przyjrzeć się przez pryzmat definicji administratora. Dla zagadnienia istotny jest ten fragment definicji, który mówi o tym iż administrator to podmiot który ustala cele i sposoby przetwarzania danych. Pytanie postawione na wstępie należy zatem przełożyć na następujące pytanie: „Czy podmiot, który posiada publicznie dostępną skrzynkę poczty elektronicznej decyduje o celach i sposobach danych osobowych znajdujących się w tej skrzynce?”. Pytanie to składa się z dwóch elementów. Są one jak poniżej.

- Czy podmiot, który posiada publicznie dostępna skrzynkę poczty elektronicznej decyduje o celach przetwarzania danych osobowych znajdujących się w tej skrzynce?
- Czy podmiot, który posiada publicznie dostępna skrzynkę poczty elektronicznej decyduje o sposobach przetwarzania danych osobowych znajdujących się w tej skrzynce?

Odpowiedź na drugie z pytań jest łatwiejsza, niż na pierwsze. Udzielam jej najpierw dla jasności wywodu. Podmiot korzysta z konkretnego rozwiązania technicznego i organizacyjnego tym samym podmiot decyduje o sposobach przetwarzania danych. Sam wybór dostawcy usługi poczty elektronicznej wydaje się być decyzją o sposobie przetwarzania danych. Decyzjami o sposobie przetwarzania danych są również decyzje dotyczące technicznych aspektów przechowywania danych, takich jak czas przechowywania stosowanie lub nie skanerów antywirusowych, rozwiązań antyspamowych etc.

Odpowiedź na pierwsze pytanie nie jest niestety oczywista i zawiera w sobie pewien element ocenny. Dla jasności powtórzmy pytanie: *Czy podmiot, który posiada publicznie dostępna skrzynkę poczty elektronicznej decyduje o celach przetwarzania danych osobowych znajdujących się w tej skrzynce?*

Poniżej wypunktowuję kolejne elementy prowadzące do ostatecznego wniosku.

- Podmiot posiada skrzynkę poczty elektronicznej.
- Celem przetwarzania danych osobowych znajdujących się w tej skrzynce jest, na przykład, zbieranie zamówień od klientów. Dla prowadzonego rozumowania cel przetwarzania danych osobowych znajdujących się w skrzynce, założony przez administratora, nie jest istotny istotne jest, że administrator jakiś cel zakłada.
- Podmiot jest świadom, że w tej skrzynce mogą znaleźć się zarówno wiadomości poczty elektronicznej realizujące cel założony przez administratora, jak i inne wiadomości poczty elektronicznej. Podmiot jest tego świadom, ponieważ taka jest natura rzeczy, inaczej po prostu nie jest, jeżeli podmiot posiada publicznie dostępny, publicznie ujawniany adres poczty elektronicznej to musi liczyć się z tym, że znajdzie się tam korespondencja nie tylko od osób od których chciałby żeby się ona tam znalazła, ale również od innych osób. Jest to zjawisko o charakterze analogicznym do praw fizyki.
- Podmiot posiada zatem skrzynkę poczty elektronicznej, w której wymieszane są wiadomości poczty elektronicznej przetwarzane w celu założonym przez ten podmiot i inne wiadomości poczty elektronicznej, przetwarzane w celu, który staram się w niniejszym rozumowaniu ustalić.
- Podmiot potrzebuję jedynie tych wiadomości poczty elektronicznej, których zbieranie założył. Faktem jest jednak, że podmiot zbiera

również inne wiadomości poczty elektronicznej, czyni to ponieważ taka jest natura rzeczy, tak działają publicznie dostępne skrzynki poczty elektronicznej, jeżeli zatem podmiot chce zapoznać się z treścią konkretnych wiadomości poczty elektronicznej, które zgodne są z założonym przez niego celem przetwarzania danych, to podmiot ten musi oddzielić te wiadomości od pozostałych wiadomości poczty elektronicznej. Tym samym podmiot musi oddzielić niechciane wiadomości od chcianych, niepożądane od pożądanych. Manewrem przeprowadzonym jedynie w warstwie językowej byłoby opisanie tej sytuacji w drugą stronę, a mianowicie, że podmiot oddziela interesujące go, chciane, pożądane informacje poczty elektronicznej od niechcianych, wobec chcianych decyduje o celu ich przetwarzania, a niechciane - jako niechciane - usuwa.

Należy jednak zwrócić uwagę, że rozdzielenie wiadomości na chciane i niechciane, pożądane i niepożądane, zgodne z celem założonym przez podmiot i niezgodne z celem założonym przez podmiot, to po prostu rozdzielenie tych wiadomości na dwie grupy. Pierwotnym celem przetwarzania danych jest zebranie wiadomości chcianych i niechcianych, a następnie rozdzielenie tych danych (w opisywanych wypadku tych wiadomości poczty elektronicznej) na dwie grupy. Jeżeli więc zapytamy o cel, w jakim przetwarzane są dane osobowe niechciane, niepożądane przez administratora, to odpowiedź jest bardzo prosta. Dane te przetwarzane są po to, żeby oddzielić od nich dane pożądane. Celem założonym przez administratora jest przetwarzanie tych danych. Chce on przetwarzać, zebrać dane pożądane, jednak nie ma możliwości realnej, aby administrator przetwarzał - zebrał te dane - bez zebrania pozostałych. Tym samym, jeżeli administrator podejmuje decyzję, że celem przetwarzania danych jest zbieranie pożądanych informacji, to jednocześnie podejmuje on decyzję, że równocześnie celem przetwarzania danych jest wyłuskanie informacji pożądanych spośród niepożądanych i oddzielenie niepożądanych od pożądanych.

Wydaje się, że nadużyciem byłoby stwierdzenie, że zbieranie danych osobowych pożądanych jest celem o którym administrator decyduje, zaś oddzielenie ich od niepożądanych i zapewne dalsze zniszczenie niepożądanych, jest celem o którym administrator nie decyduje.

Na zjawisko danych niepożądanych przez administratora czyli danych co do których może istnieć wątpliwość, czy administrator - czy dany podmiot jest w istocie administratorem tych danych, można, a nawet uważam, że należy spojrzeć przez pryzmat praw i wolności osób których te dane dotyczą.

Dla porządku, należy najpierw spojrzeć na takie dane osobowe przez pryzmat przepisów zakresowych, czyli przez pryzmat art. 1 RODO, art. 2 RODO, art.3 RODO. Nie chcę dokonywać tu streszczenia wskazanych przepisów, przepisy omawiam drobiazgowo w odpowiednich miejscach niniejszej publikacji, w tym miejscu ograniczam się zatem jedynie do zwrócenia uwagi na pewne, wynikające z nich szczegóły, które są istotne dla opisywanej sytuacji i dla kategorii sytuacji do sytuacji tej analogicznych.

Spojrzenie na stan faktyczny przez pryzmat art. 1 RODO każe stwierdzić, że RODO chroni prawo do ochrony danych osobowych, przysługujące osobom, których dane dotyczą. Niezależnie od tego, czy osoby te przysyłają do administratora korespondencję przez tego administratora oczekiwaną i pożądaną, czy przesyłają do administratora korespondencję przez niego nieoczekiwaną i niepożądaną.

Spojrzenie przez pryzmat art. 2 RODO każe stwierdzić, że przetwarzanie danych osobowych mające postać zbierania tych danych, poprzez zbieranie korespondencji zawierającej te dane, wydaje się realizować dwa warunki z art. 2 ust. 1 RODO. Gromadzenie danych w skrzynce poczty elektronicznej, najpierw na serwerze pocztowym (a następnie zapewne lokalnie) należy zakwalifikować jako przetwarzanie danych osobowych w sposób zautomatyzowany. Odpowiedzi na to, czy jest to przetwarzanie w sposób częściowo, czy całkowicie zautomatyzowany nie udzielam tu świadomie, zarówno ze względu na brak prawnego substratu do udzielenia tej odpowiedzi, jak i ze względu na nieistotną treść tej odpowiedzi dla przedmiotu namysłu.

Wspomniane gromadzenie danych w skrzynce poczty elektronicznej, skutkuje włączaniem tych danych do zbioru danych osobowych i to do zbioru posiadającego kilka kryteriów wyszukiwawczych, bowiem zasoby poczty elektronicznej można zwykle przeszukiwać na różny sposób, z tym, że twierdzenie o włączaniu do zbioru jest poprawne, o tyle, o ile utożsamiamy wiadomość poczty elektronicznej z danymi osobowymi. Jest to oczywiście pewne uproszczenie, należy jednak pamiętać, że dane osobowe zwykle znajdują się w dokumentach. Między dokumentem zawierającym dane osobo-

we a danymi osobowymi zachodzi istotna różnica ontologiczna, jednak stanowisko, zgodnie z którym zbiór wiadomości poczty elektronicznej nie jest zbiorem danych osobowych uważam za błędne i mające na celu głównie obejście art. 2 ust. 1 RODO. Gdyby nawet uznać, że zbiór wiadomości poczty elektronicznej nie jest zbiorem danych osobowych, to i tak gromadzenie danych osobowych mieści się w materialnym zakresie stosowania RODO, z uwagi na automatyzm tej czynności, co opisałem wyżej w niniejszym podrozdziale.

Dla porządku, patrząc przez pryzmat art. 3 RODO, przyjmuję, że zbieranie wiadomości poczty elektronicznej niechcianych, wiadomości niepożądanych - zawierających dane osobowe, zachodzi, dla potrzeb tego przykładu, w związku z działalnością prowadzoną przez administratora na terenie Unii.

Osobie której dane dotyczą, w tym wypadku nadawcy wiadomości poczty elektronicznej przysługuje cały szereg praw na gruncie RODO. Przede wszystkim osoba taka ma prawo oczekiwać, że jej dane będą przetwarzane przez administratora w sposób zgodny z prawem (zasada zgodności z prawem). Nie sposób dopatrzeć się niezgodności z prawem w tym, że administrator posiada skrzynkę poczty elektronicznej, na którą doręczane są różne wiadomości poczty elektronicznej, taka jest bowiem specyfika tego rozwiązania technicznego, że administrator zbiera tam wiadomości chciane i niechciane.

Jeżeli administrator jest podmiotem publicznym, to zwykle zbiera te wiadomości w oparciu o art. 6 ust. 1 lit. e RODO, jeżeli administrator jest podmiotem prywatnym, to zwykle zbiera te wiadomości w oparciu o art. 6 ust. 1 lit. f RODO. Użyłem tu słowa: „zwykle", ponieważ możliwe jest również zbieranie wiadomości poczty elektronicznej, rozumiane jako przetwarzanie danych osobowych, w oparciu o inne podstawy prawne, które jednak z uwagi na tematykę niniejszego wywodu pomijam. Zebrawszy wiadomości zgodnie z art. 6 ODO, administrator, tym samym, realizuje zasadę zgodności z prawem. Jedynym celem zbierania tych wiadomości jest zbieranie jakichkolwiek wiadomości poczty elektronicznej, tych pożądanych i tych niepożądanych przez administratora, można więc, z powodzeniem, uznać, że celem zbierania wiadomości niepożądanych jest, po prostu, zbieranie wiadomości poczty elektronicznej, w szczególności wiadomości pożądanych przez administratora, tak by móc jedne od drugich oddzielić, patrzę tu oczywiście na problem przez pryzmat realizacji zasady ograniczenia celu.

Po oddzieleniu wiadomości pożądanych, administrator nie powinien dalej przetwarzać, w tym przechowywać, niepożądanych wiadomości poczty elektronicznej. Ten sam wniosek wynika z zasady minimalizacji, administratorowi wolno jest zebrać niepożądane wiadomości poczty elektronicznej dopóki zbieranie to jest niezbędne w kontekście zbierania wiadomości pożądanych, kiedy jednak administrator pożądane wiadomości oddzieli od niepożądanych, to nie powinien już wiadomości niepożądanych posiadać, powinien zatem je usunąć. Jeśli chodzi o zasadę ograniczenia przechowywania, to po realizacji celu, czyli po oddzieleniu informacji pożądanych od informacji niepożądanych, administrator nie powinien dalej niepożądanych informacji przetwarzać. Z punktu widzenia zasady poufności, administrator powinien zadbać o to, żeby osoby, które dokonują czynności oddzielenia informacji pożądanych od informacji niepożądanych, były do tego uprawnione. Z punktu widzenia zasady integralności, administrator powinien zadbać o to, by usunięcie danych niepożądanych nie zagroziło integralności danych pożądanych.

W świetle powyższych rozważań, widać, jak wiele obowiązków administrator powinien spełnić, w związku z przetwarzaniem danych osobowych w treści niepożądanych informacji poczty elektronicznej. Zwracam uwagę, że obowiązki te jedynie zasygnalizowałem i to jedynie na poziomie zasad, bez przechodzenia na poziom przepisów szczegółowych RODO. Każdy z obowiązków leżących po stronie administratora koreluje z uprawnieniem leżącym po stronie osoby, której dane dotyczą. Naruszenie tych obowiązków automatycznie skutkuje naruszeniem uprawnień, czyli praw osób których dane dotyczą, co w skrajnej sytuacji mogłoby skutkować odpowiedzialnością cywilną po stronie administratora, w kontekście ewentualnej szkody niemajątkowej w wyniku naruszenia przepisów RODO (art. 82 RODO), może też oczywiście skutkować odpowiedzialnością administracyjną, co jest swoistym truizmem więc myśli tej dalej nie rozwijam.

3.5. Art. 4 pkt 7. Uwaga 9.
Organ władzy publicznej jako administrator

Ciekawym problemem, nad którym warto się zastanowić jest problem, który streszczony został w tytule podrozdziału, a mianowicie kto jest administratorem danych osobowych w przypadku organów władzy publicznej.

Nie wykluczam, że zasygnalizowany problem jest jedynie problemem interpretacyjnym, jednak nawet jeżeli tak właśnie jest, a nawet zwłaszcza wtedy, nad problemem tym zastanowić się należy.

Źródłem ewentualnego problemu interpretacyjnego jest brzmienie dwóch przepisów, pierwszy to art. 4 pkt 7 RODO, który w zakresie istotnym dla wywodu stanowi, że administrator to podmiot, który: *samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (...)*. Drugi przepis to przepis Konstytucji RP, który stanowi, że: *Organy władzy publicznej działają na podstawie i w granicach prawa*[250]. Jak widać, przynajmniej na pierwszy rzut oka, przepisy te mogą rodzić wątpliwości co do tego kto jest administratorem danych w administracji i czy takowi w ogóle w administracji występują.

Zestawmy poniżej:

- administrator danych ustala cele i sposoby przetwarzania danych osobowych (RODO) i jednocześnie
- organ władzy publicznej działa na podstawie i w granicach prawa (Konstytucja RP).

Ze względu na treść art. 4 pkt 7 RODO i art. 7 Konstytucji RP, należy postawić pytanie wskazane poniżej.

- Czy organ władzy publicznej może być administratorem danych?

Pytanie to pojawia się wskutek analizy wskazanych przepisów, skoro bowiem organ działa na podstawie prawa, to być może nie może być on administratorem danych, skoro administrator decyduje o celach i sposobach przetwarzania danych. Organ nie decyduje, organ działa na podstawie prawa, w związku z tym (może, nad czym zastanawiam się niżej) organ, żaden organ, administratorem nie jest.

Nie chcę wdawać się tu w rozważania nad ewentualną różnicą między organem władzy a organem administracji. Nie wdaję się w nie tym bardziej, że art. 6 KPA stanowi, że *Organy administracji pu-*

[250] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. Dz.U. 1997 nr 78 poz. 483 ze zm. Art. 7.

blicznej działają na podstawie przepisów prawa[251]. Wywodzenie dla prowadzonych tu rozważań, wniosków z różnicy miedzy organem władzy publicznej a organem administracji uważam za niecelowe, więc wywodu takiego nie prowadzę.

Nadal nieodpowiedziane pozostaje zatem pytanie wskazane poniżej.

- Czy organ władzy publicznej (organ administracji) może być administratorem danych?

Wyżej w uwadze *3.5. Art. 4 pkt 7. Uwaga 5. Administrator, a osoba kierująca administratorem* piszę, że *Należy przyjąć, że administratorami są podmioty, nie zaś osoby nimi kierujące*, mam jednak świadomość, że jest to pewien postulat, czego zresztą nie ukrywam, w warstwie językowej pisząc *Należy przyjąć, że (...)*.

Jeżeli przyjmie się, że administratorem jest podmiot, nie osoby nim kierujące, to można próbować udzielić odpowiedzi na powracające tu pytanie. Można wywodzić, że skoro administratorem jest podmiot, nie zaś organ, to problem „kto jest administratorem danych osobowych w przypadku organów władzy publicznej" nie istnieje. Nie istnieje, ponieważ Konstytucja RP dotyczy organu, a skoro administratorem jest podmiot, którego organ jest organem, to problemu nie ma. Wywód ten prowadzę, ponieważ jest możliwy, może nawet czasem wywód taki sprawę wyjaśnia, uważam go jednak za bałamutny. Uważam tak ponieważ, na przykład w ministerstwie (jakimkolwiek) administratorem danych jest minister (tak przynajmniej jest sygnalizowane na stronach ministerstw w Polsce i z tym się zgadzam). W ministerstwie nie ma podmiotu, którego minister byłby organem i który to podmiot byłby administratorem danych, ale już na przykład w gminie podmiot taki jest, jest nim (oczywiście) gmina.

Nadal nieodpowiedziane pozostaje zatem pytanie wskazane poniżej.

- Czy organ władzy publicznej (organ administracji) może być administratorem danych?

[251] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Dz.U. 1960 nr 30 poz. 168 ze zm. t.j. Dz. U.2020 poz. 256 ze zm. Art. 6.

Warto w kwestii będącej tu przedmiotem rozważań, skorzystać z publikacji A. Sobczyka.

Z poglądów A. Sobczyka wynika (takie odnoszę wrażenie), że autor ten uważa, że w sytuacji, w której na podmiocie publicznym (takiego określenia używa A. Sobczyk) spoczywają obowiązki nałożone przepisami prawa, podmiot taki nie jest administratorem danych. Wnioskuję o tym z następujących słów A. Sobczyka: *Zanim przejdziemy do RODO, zatrzymajmy się nad kolejnym poziomem regulacji prawnej dotyczącej ochrony danych osobowych bez zastosowania rozporządzenia unijnego. Tym razem chodzi o relacje z podmiotami publicznymi w wąskim tego słowa znaczeniu, czyli ze strukturami państwa*[252]. Dalej niestety A. Sobczyk pisze, że *(...) władze publiczne nie mogą gromadzić danych przesłanych przez obywatela bez wezwania (np. nieproszone podanie o zatrudnienie)*. Jak widać, A. Sobczyk używa tu jako przykładu „nieproszonego podania o zatrudnienie", retorycznym pozostanie pytanie dlaczego A. Sobczyk ograniczył przykład do „nieproszonego podania o zatrudnienie", skoro przecież każde podanie jest „nieproszone", jeżeli przez „nieproszone" rozumieć dostarczanie danych (podań, skarg – czegokolwiek) bez wezwania. Jak pogląd A. Sobczyka ma się do KPA czy, zwłaszcza, do przepisów kancelaryjnych, które nakazują gromadzenie korespondencji – trudno powiedzieć.

Dalej jeszcze, A. Sobczyk pisze: *Istnieje całe spektrum sytuacji, w których RODO nie ma zastosowania, choć dane osobowe są oczywiście chronione. Dotyczy to przede wszystkim danych, które podmiot danych ujawnia samodzielnie na podstawie przysługującej mu autonomii informacyjnej lub poprzez wspólną decyzję uprawnionego lub odbiorcy. Co więcej, każdy element zachowania przez podmiot autonomii lub współautonomii, czy to do celów, czy sposobów przetwarzania, ma ten skutek że RODO nie ma zastosowania*[253]. Jak widać, A. Sobczyk robi tu kolejny krok w kierunku wyłączenia stosowania RODO w pewnych sytuacjach. Już nie tylko obowiązki w zakresie przetwarzania danych, wynikające z innych podstaw niż z RODO, wyłączają stosowanie RODO, ale stosowanie RODO wyłącza już samo to, że osoba, której dane dotyczą, z własnej woli, dostar-

[252] A. Sobczyk RODO, Rozproszona władza publiczna. Kraków 2019. s. 54.

[253] A. Sobczyk RODO, *loc. cit*.

cza dane administratorowi. Można więc zrekonstruować tu prawdopodobny pogląd A. Sobczyka, że skoro osoba, której dane dotyczą, dostarcza dane podmiotowi, to ta osoba, nie zaś podmiot, do którego dane są dostarczane decyduje o celach przetwarzania danych.

Uważam, że poglądy A. Sobczyka, które po części zasygnalizowałem powyżej, zawierają pewien podstawowy błąd u założenia. Otóż można uogólnić, że A. Sobczyk uważa, że jeżeli podmiot nie w pełni decyduje o celach i sposobach przetwarzania danych osobowych, to podmiot taki nie jest administratorem danych osobowych. Podmiot nie decyduje o celach przetwarzania danych osobowych:

- jeżeli jest podmiotem publicznym, na który prawo nakłada obowiązki,
- jeżeli jest podmiotem prywatnym, na który prawo nakłada obowiązki,
- jeżeli osoby, których dane dotyczą, z własnej woli dostarczają podmiotowi dane, których dostarczenie podmiot akceptuje,
- jeżeli osoby, których dane dotyczą, z własnej woli dostarczają podmiotowi dane, których dostarczenia podmiot nie akceptuje.

Podmiot nie byłby w takim razie administratorem danych, ponieważ nie realizuje przepisu, zgodnie z którym administrator „(…) ustala cele (…) przetwarzania danych osobowych (…)". W tym miejscu należy zadać sobie podstawowe pytanie. Pytanie o to czy możliwe jest, by prawodawca,

- który tworzył art. 4 pkt 7 RODO i
- który tworzył art. 2 RODO i
- który tworzył art. 6 ust. 1 RODO,

przy tworzeniu art. 4 pkt 7 RODO, zapomniał jednocześnie o treści art. 6 ust. 1 RODO albo przy tworzeniu art.6 ust 1 RODO, zapomniał jednocześnie o treści art. 4 pkt 7 RODO.

Można w związku z tym postawić dwie tezy. Zaznaczam, że zgadzam się tylko z jedną z nich, dokładnie – z drugą, z wymienionych, jednak tezy stawiam dwie, ponieważ postawienie ich jest możliwe, z uczciwości naukowej nie chcę zatem udawać, że widzę możliwość postawienia tylko jednej z nich.

- Pierwsza teza jest taka, że prawodawca przy pisaniu jednego przepisu zapomniał o drugim.

.

- Druga teza jest taka, że prawodawca przy pisaniu jednego przepisu nie zapomniał o drugim.

Pierwsza z tez wydaje się nie do zaakceptowania. Nie do zaakceptowania ponieważ kłóci się z zasadą racjonalnego prawodawcy. Wydaje się, że niestety tezie tej hołduje A. Sobczyk. Mogę nawet zaryzykować twierdzenie, że cała książka jego, z której cytaty tu zamieszczam, jest przeciągłym i (czego absolutnie wskazanemu autorowi nie odmawiam) niezwykle kompetentnym poszukiwaniem i wskazywaniem innych niż RODO przepisów, które chronią osoby fizyczne, w kontekście przetwarzania danych osobowych, które ich dotyczą. Mam nawet wrażenie, że A. Sobczyk dostrzega potrzebę ochrony danych osobowych i z niezwykłą biegłością i znawstwem wskazuje cały szereg przepisów, które chronią prawa osób, których dane dotyczą i które jednocześnie stosowane są, zdaniem cytowanego autora, zamiast przepisów RODO. podczas gdy ja uważam, że przepisy te stosowane są obok RODO, nie zaś zamiast.

Zwracam szczególną uwagę na zasadę racjonalnego prawodawcy, uważam bowiem, że **prawidłowa jest teza druga**, teza, którą dla porządku powtarzam: „prawodawca przy pisaniu jednego przepisu nie zapomniał o drugim". Inaczej, szerzej ujmując, prawodawca przy tworzeniu przy tworzeniu art. 4 pkt 7 RODO, nie zapomniał jednocześnie o treści art. 6 ust.1 RODO, zaś od niejako drugiej strony patrząc, prawodawca przy tworzeniu art. 6 ust. 1 RODO, nie zapomniał jednocześnie o treści art. 4 pkt 7 RODO.

Rozkładając rozumowanie na fragmenty: prawodawca, który tworzył definicję administratora, pamiętał przy tym o warunkach zgodności z prawem przetwarzania danych osobowych, które to warunki zapisane są w art. 6 ust. 1 RODO.

Prawodawca wiedział zatem, że normalne jest, że w zakresie przetwarzania danych osobowych normalne jest, że zachodzą czasem zjawiska wymienione przeze mnie poniżej.

- Że osoba, której dane dotyczą wyraża czasem zgodę na przetwarzanie tych danych (art. 6 ust. 1 lit. a RODO).
- Że podmioty zawierają umowy i że w związku z tym przetwarzanie danych osobowych bywa do wykonania tych umów niezbędne (art. 6 ust. 1 lit. b RODO).

- Że na administratorach ciążą czasem obowiązki prawne, do wykonania których niezbędne jest przetwarzanie danych osobowych (art. 6 ust. 1 lit. c RODO).
- Że przetwarzanie danych osobowych bywa czasem niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO).
- Że przetwarzanie danych osobowych bywa czasem niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO).
- Że przetwarzanie danych osobowych bywa czasem niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą (art. 6 ust. 1 lit. f RODO).

Innymi słowy, prawodawca, który stworzył definicję administratora wiedział, przy okazji tworzenia tej definicji, że w dziedzinie przetwarzania danych osobowych zachodzą pewne zjawiska, kategorie zdarzeń. Wiedział o tym i dlatego ujął te kategorie zdarzeń w ramy art. 6 ust. 1 RODO. Jednocześnie ten sam prawodawca, który ujął pewne kategorie zdarzeń w ramy art. 6 ust. 1 RODO znał treść definicji administratora danych. Te pozornie banalne wnioski wysnuwam z domniemania racjonalności prawodawcy. Lech Morawski wskazuje, że domniemanie to stanowi *niezbędne założenie każdej interpretacji przepisów prawnych (...)*[254]. Analogiczny pogląd odnajdujemy w dużo wcześniejszej publikacji J. Wróblewskiego. Jerzy Wróblewski pisze o normodawcy racjonalnym, *którego skonstruowane „przeżycia psychiczne mają stanowić właściwe znaczenie normy prawnej*.[255] *W ten sposób z jednej strony unika się nieokreśloności związanych*

[254] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 169.

[255] Przypis J. Wróblewskiego umieszczony w odpowiednim miejscu tekstu cytowanego w wywodzie głównym: *A. Hagerstrom pisze, że wykładnia jest zgodna z intencją prawodawcy wówczas, gdy znaczenie interpretowanej normy odpowiada intuicyjnemu jej ujęciu i jednocześnie pozostaje w ramach tekstu, oraz podkreśla, że zazwyczaj ten prawodawca jest konstruowany jako rozsądny (reasonable) prawodawca (A. Hagerstrom: Inquiries into the Nature*, *s. 354, 204, 241).* J. Wróblewski.

z badaniem realnych przeżyć jakiegoś normodawcy, z drugiej zaś strony od ścisłości reguł, według których konstrukcja fikcyjnego normodawcy przebiega, zależy stałość otrzymywanego w ten sposób znaczenia norm prawnych.[256]. Jak widać z zacytowanego poglądu, „racjonalny prawodawca" to pewna koncepcja, koncepcja, która umożliwia ustalanie znaczenia przepisów.

Skoro prawodawca jest racjonalny, to przepisy przezeń tworzone również (zapewne) takowe są. Wszystko wskazuje zatem na to, że definicję administratora danych należy interpretować przez pryzmat art. 6 ust. 1 RODO. Jest to sensowne nie tylko z uwagi na racjonalność prawodawcy, ale również, po prostu ze względu na treść definicji administratora danych i z uwagi na treść art. 6 ust. 1 RODO. Część wprowadzająca tego przepisu stanowi, że: *Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:*. I tu właśnie kryje się klucz do ustalenia zależności między definicją administratora danych a art. 6 ust. 1 RODO. Otóż z art. 6 ust. 1 RODO wynika kiedy przetwarzanie jest zgodne z prawem. Przetwarzanie jest zatem zgodne z prawem w warunkach wskazanych w art. 6 ust. 1 RODO.

Zwracam jednak uwagę na jeszcze jeden element, art. 6 ust. 1 RODO, wskazuje kiedy przetwarzanie danych osobowych jest zgodne z prawem, jednak istotne jest również kto owe dane przetwarza. Odpowiedzialność za przestrzeganie przepisów RODO spoczywa na administratorze danych, co wynika z art. 5 ust. 2 RODO. Administrator danych to podmiot wskazany w art. 4 pkt 7 RODO. Administrator to podmiot wskazany w art. 4 ust. 7 RODO, ale z poszanowaniem dla treści art. 6 RODO. Innymi słowy, nic nie stoi na przeszkodzie, by administratorem danych był podmiot, którego możliwość podejmowania decyzji w przedmiocie celów przetwarzania jest ograniczona przez okoliczności, do których odnosi się art. 6 ust. 1 RODO, w tym, pośrednio przez art. 7 Konstytucji RP.

Dla porządku odpowiadam poniżej na pytanie zadane na początku podrozdziału. Pytanie to brzmi jak poniżej.

- Czy organ władzy publicznej może być administratorem danych?

Odpowiedź na nie brzmi: „Organ władzy publicznej może być administratorem danych".

[256] J. Wróblewski *Zagadnienia teorii wykładni prawa ludowego*. Warszawa 1959, s. 162-163.

Można zadać jeszcze jedno, objaśniające pytanie.

- Czy fakt, że organ władzy publicznej działa na podstawie prawa nie stanowi przeszkody, by organ taki był administratorem danych, skoro administrator decyduje o celach przetwarzania danych osobowych, zaś działanie na podstawie prawa uniemożliwia pełne decydowanie o celach przetwarzania danych osobowych?

Odpowiedź na nie brzmi: fakt, że organ władzy publicznej działa na podstawie prawa nie stanowi przeszkody by taki organ był administratorem danych.

- Działanie na podstawie prawa uniemożliwia pełne decydowanie o celach przetwarzania danych osobowych, jednak do ograniczeń w swobodzie podejmowania decyzji odsyła art. 6 ust. 1 RODO i jednocześnie,
- artykuł 6 ust. 1 RODO określa warunki zgodnego z prawem przetwarzania danych osobowych i jednocześnie,
- art. 5 ust. 2 RODO nakłada obowiązki z zakresu RODO na administratora danych i jednocześnie,
- administrator danych jest zdefiniowany w art. 4 ust. 7 RODO i jednocześnie,
- warunki z art. 6 ust. 1 RODO mają charakter wyjściowy, warunki te poprzez art. 5 ust. 2 RODO odnoszą się do definicji administratora danych, która tym samym nie stoi na przeszkodzie by podmiot w niej zdefiniowany był administratorem, przy jednoczesnym poszanowaniu warunków z art. 6 ust. 1 RODO.

Na rozważane wyżej zagadnienia można spojrzeć w jeszcze jeden sposób, nie rozwijam tego spojrzenia, bowiem wnioski z rozważań byłyby analogiczne do wyprowadzonych powyżej – dopuszczających by podmiot publiczny był administratorem danych. Co więcej, uważam, że prowadzone wyżej rozważania są niczym innym, jak ujętym w słowa spojrzeniem przez pryzmat logiki. Spojrzenie to prezentuję poniżej. Problem, nad którym zastanawiam się w niniejszym podrozdziale to kwestia koniunkcji. Uważam, że koniunkcja nie zachodzi jedynie między art. 7 Konstytucji RP i art. 4 pkt 7 RODO, ale również, a nawet przede wszystkim, koniunkcja zachodzi miedzy art. 6 ust. 1 RODO i art. 5 ust. 2 RODO w zw. z (czyli też koniunkcja) art. 5 ust. 1 RODO i z art. 4 ust. 7 RODO i z art. 7 Konstytucji RP. Istotne jest by zauważyć istnienie dłuższej ze wskazanych koniunkcji.

Kiedy tę koniunkcję spostrzeżemy, pozostaje jedynie ubrać wnioski ze spostrzeżenia w słowa.

4. Art. 4 pkt 7. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 7 RODO definiuje **administratora**, zatem zgodnie z dyrektywą języka prawnego[257], każdy kto interpretuje RODO powinien rozumieć pojęcie ***administrator*** tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie ***administrator*** tak jest ono zdefiniowane w art. 4 pkt. 7 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że administrator będzie rozumiał znaczenie pojęcia „**administrator**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 7. Konkretyzacja zasad

Administrator danych, zdefiniowany w komentowanym przepisie ma bardzo poważny związek z zasadami dotyczącymi przetwarzania danych osobowych, zapisanymi w art. 5 RODO.
Otóż z art. 5 ust. 2 RODO wynikają dwie zasady.

Pierwsza to **zasada odpowiedzialności administratora**. Odsyłam do komentarza do tej zasady stanowiącego pierwszą cześć komentarza do art. 5 ust. 2 RODO[258]. Tu jedynie przypominam, że zasada odpowiedzialności oznacza, że administrator ma obowiązek realizować art. 5 ust. 1 RODO, czyli zasady dotyczące ochrony danych osobowych. Zasady o których tu mowa, należy realizować poprzez re-

[257] L. Morawski *op. cit.* s. 93-99, zwłaszcza 95.

[258] Będącego częścią publikacji, wydawanej równolegle z niniejszą, a to: J. Rzymowski, *RODO – GDPR. Przetwarzanie danych osobowych. Zasady. Zgodność z prawem*, Łódź. 2021..

alizację przepisów szczególnych RODO. Administrator jest więc odpowiedzialny za przestrzeganie przepisów RODO.

Druga to **zasada rozliczalności**. Odsyłam do komentarza do tej zasady stanowiącego drugą cześć komentarza do art. 5 ust. 2 RODO. Tu jedynie przypominam, że zasada rozliczalności oznacza, że administrator ma obowiązek wykazania przestrzegania przepisów art. 5 ust. 1 RODO czyli zasad, przy czym narzędziem wykazania realizacji zasad jest wykazanie realizacji przepisów, administratora ma zatem obowiązek wykazania realizacji przepisów RODO.

6. Art. 4 pkt 7. Postulaty de lege ferenda

6.1 Art. 4 pkt 7. Postulat 1.
Doprecyzowanie definicji administratora

Nieznośną dla praktyków jest sytuacja, w której nie są w stanie ustalić kto jest administratorem w danej sytuacji. W uwadze (3.5. Art. 4 pkt 7. Uwaga 5. Administrator, a osoba kierująca administratorem.) odnosze się do tego problemu, prezentuję swoje stanowisko, w sposób niestety dość kazuistyczny, nie ukrywam jednak, że jest to moje stanowisko. Możliwe są i inne. W zwiazku z tym dobrze by było gdyby prawodawca tak zmienił definicję administratora by łatwiej niż obecnie było ustalić kto jest administratorem. Przyznam, że nie mam, w przypadku komentowanego przepisu, sprecyzowanej propozycji nowelizacji. Potrzebę nowelizacji jednak widzę, dla przyczyn zaprezentowanych wyżej w tym postulacie. Prezentuję poniżej kilka propozycji postulatów nowelizacyjnych, co do tresci których jestem przekonany, jednak jeśli chodzi o formę proponowanej nowelizacji, to nie jest ona doskonała, mimo tego prezentuję swoje stanowisko, choćby jako zachętę dla innych badaczy. Propozycje nowelizacyjne umieszczam w cudzysłowach i podkreślam.

„W przypadku osoby prawnej, administratorem jest ta osoba prawna, nie zaś osoba lub osoby nią kierujące lub sprawujące w niej funkcje.“ – Administratorem jest spółka nie zarząd spółki.

„W przypadku kiedy organ publiczny jest organem podmiotu publicznego, administratorem jest ten podmiot“. – Administratorem jest gmina nie wójt, nie rada gminy, nie urząd gminy.

„W przypadku kiedy organ publiczny nie jest organem podmiotu publicznego, administratorem jest ten organ publiczny". – Administratorem jest minister nie ministerstwo.

„W przypadku jednostki lub innego podmiotu, administratorem jest taka jednostka lub podmiot nie zaś osoba lub osoby nimi kierujące lub sprawujące w nich funkcje". - Administratorem jest stowarzyszenie - nie prezes lub zarząd, administratorem jest szkoła - nie dyrektor szkoły, administratorem jest ośrodek pomocy społecznej - nie kierownik ośrodka, administratorem jest uczelnia - nie rektor.

Artykuł 4 pkt 8 RODO

„podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

1. Art. 4 pkt 8. Komentarz

Przepis definiuje podmiot przetwarzający.

Należy zwrócić szczególną uwagę na fakt, że w komentowanej definicji zdefiniowano podmiot przetwarzający, jednak w żaden sposób nie powiązano definicji z art. 28 RODO, zatytułowanym: „Podmiot przetwarzający". Oczywiście „podmiot przetwarzający" o którym mowa w komentowanym przepisie i „podmiot przetwarzający", o którym mowa w art. 28 RODO, to ten sam podmiot, ten sam podmiot przetwarzający, co wynika z dyrektywy języka prawnego[259].

W art. 28 RODO zawarto przepisy doprecyzowujące definicję podmiotu przetwarzającego, a przede wszystkim przepisy ustanawiające obowiązki podmiotu przetwarzającego, mimo tego, jeżeli podmiot spełnia warunki wynikające z komentowanego przepisu to jest podmiotem przetwarzającym, niezależnie od tego, czy podmiot ten spełnia również warunki z art. 28 RODO.

- Podmiotem przetwarzającym, może być każdy podmiot lub osoba.[260]
- Podmiotem przetwarzającym może być osoba fizyczna.
- Podmiotem przetwarzającym może być osoba prawna.
- Podmiotem przetwarzającym może być organ publiczny.
- Podmiotem przetwarzającym może być jednostka.
- Podmiotem przetwarzającym może być inny podmiot.

Warunkiem by podmiot lub osoba był podmiotem przetwarzającym jest, by ten podmiot lub osoba przetwarzał dane osobowe w imieniu administratora.

---

[259] L. Morawski, *loc. cit*.

[260] Podobnie: P. Litwiński, P. Barta, M. Kawecki. w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 225-226.

Przetwarzanie danych osobowych w imieniu administratora decyduje o tym czy podmiot, który te dane przetwarza jest podmiotem przetwarzającym.

Umowa powierzenia przetwarzania nie decyduje o tym, czy podmiot jest podmiotem przetwarzającym czy nie. Jeżeli nie zawarto umowy powierzenia przetwarzania i podmiot przetwarza dane osobowe w imieniu administratora, to jest on podmiotem przetwarzającym, mimo niezawarcia umowy powierzenia przetwarzania.

Jeżeli zawarto umowę powierzenia przetwarzania i podmiot nie przetwarza danych osobowych w imieniu administratora a jedynie we własnym imieniu, to nie jest on podmiotem przetwarzającym.

2. Art. 4 pkt 8. Analiza

Ze słów wytłuszczonych: „**podmiot przetwarzający**" **oznacza**" wynika, że przepis definiuje podmiot przetwarzający. Podmiotem przetwarzającym jest zatem podmiot zdefiniowany w przepisie. Należy zwrócić szczególną uwagę na fakt, że w komentowanej definicji zdefiniowano podmiot przetwarzający, jednak w żaden sposób nie powiązano tej definicji z art. 28 RODO, zatytułowanym: *Podmiot przetwarzający*. Oczywiście „podmiot przetwarzający" o którym mowa w komentowanym przepisie i „podmiot przetwarzający", o którym mowa w art. 28 RODO, to ten sam podmiot, ten sam podmiot przetwarzający, co wynika z dyrektywy języka prawnego[261].

W art. 28 RODO zawarto przepisy doprecyzowujące definicję podmiotu przetwarzającego, a przede wszystkim przepisy ustanawiające obowiązki podmiotu przetwarzającego, mimo tego, jeżeli podmiot spełnia warunki wynikające z komentowanego przepisu to jest podmiotem przetwarzającym, niezależnie od tego, czy podmiot ten spełnia również warunki z art. 28 RODO. Szerzej w uwadze *3.7. Art. 4 pkt 8. Uwaga 7. Bezumowne powierzenie przetwarzania danych osobowych a prowadzenie cudzych spraw bez zlecenia*.

Ze słów wytłuszczonych w przepisie: „**oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, który przetwarza dane osobowe w imieniu administratora" wynika, że podmiotem przetwarzającym może być każdy z podmiotów wymienionych

[261] L. Morawski, *loc. cit.*

w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków.
Podmiotem przetwarzającym może być osoba fizyczna.
Podmiotem przetwarzającym może być osoba prawna.
Podmiotem przetwarzającym może być organ publiczny.
Podmiotem przetwarzającym może być jednostka.
Podmiotem przetwarzającym może być inny podmiot.

Jak widać z powyższego wyliczenia, podmiotem przetwarzającym, podobnie jak administratorem, może być każdy podmiot lub osoba.[262]

Ze słów wytłuszczonych w przepisie: „oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, który przetwarza dane osobowe w imieniu administratora**" wynika, że warunkiem by wymieniony wyżej podmiot lub osoba był podmiotem przetwarzającym jest, by ten podmiot lub osoba przetwarzał dane osobowe w imieniu administratora.

Przetwarzanie danych osobowych w imieniu administratora danych jest konstytutywne dla bycia podmiotem przetwarzającym, jednak trudno czasem ustalić czy podmiot, który przetwarza dane osobowe, przetwarza je w swoim imieniu czy przetwarza je w imieniu administratora. Szerzej w uwadze *3.2. Art. 4 pkt 8. Uwaga 2. Problemy z odróżnieniem administratora danych od podmiotu przetwarzającego*.

Należy zwrócić baczną uwagę na fakt, że przetwarzanie danych osobowych w imieniu administratora nie musi oznaczać sytuacji, w której administrator zbiera dane a następnie powierza ich przetwarzanie podmiotowi przetwarzającemu. Taka sytuacja jest możliwa, co więcej, jest ona często spotykana, jednak nie jest to jedyna możliwa sytuacja. Przetwarzanie danych osobowych w imieniu administratora danych może też oznaczać zbieranie w imieniu administratora danych. Administrator (danych) może być administratorem (danych) których administrator (danych) nie posiada, danych które zostaną dopiero zebrane, ale ich zebranie administrator danych powierzył podmiotowi przetwarzającemu.

[262] Podobnie: P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 225-226.

3. Art. 4 pkt 8. Uwagi
3.1. Art. 4 pkt 8. Uwaga 1. Co odróżnia administratora (danych) od podmiotu przetwarzającego

Zwracam uwagę na ogromne podobieństwo przepisów definiujących administratora danych osobowych i podmiot przetwarzający. Przepisy te cytuję poniżej w tabeli, zestawiając elementy wspólne dla obu przepisów i elementy odróżniające.

„**administrator**" oznacza	„**podmiot przetwarzający**" oznacza
osobę fizyczną	osobę fizyczną;
lub prawną,	lub prawną,
organ publiczny,	organ publiczny,
jednostkę	jednostkę
lub inny podmiot,	lub inny podmiot,
	który przetwarza dane osobowe
	w imieniu administratora
który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;	
jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;	

Z zaprezentowanego porównania wynika pewien uderzający wniosek. Administrator ustala cele i sposoby przetwarzania, ale dla jego bytu jako ADO nie jest konieczne by przetwarzał dane. Administrator może zatem ustalić cele i sposoby, po czym nie zetknąć się nawet z danymi osobowymi, których jest administratorem.

Jeśli chodzi o podmiot przetwarzający, to jest odwrotnie. Podmiot przetwarzający nie ustala celów i sposobów przetwarzania danych osobowych. Podmiot przetwarzający *przetwarza dane osobowe*

w imieniu administratora, jak widać, dla bytu podmiotu przetwarzającego konieczne jest by przetwarzał dane osobowe w imieniu administratora, nie wystarczy nawet by się z nimi tylko zetknął.

Prawodawca zapomniał tu o pewnym zjawisku, które w realiach dzisiejszego obrotu jest możliwe. Może się zdarzyć, że administrator danych nie przetwarza danych, jednak powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu i jednocześnie wyraża zgodę na dalsze powierzenie. W tym samym stanie faktycznym, podmiot przetwarzający nie przetwarza danych, jednak podpowierza przetwarzanie danych podmiotowi przetwarzającemu drugiego stopnia. Z komentowanego przepisu wynika, że podmiot przetwarzający to (poza pozostałymi warunkami) podmiot, który przetwarza dane osobowe.

W związku z powyższym, jeżeli podmiot, z którym zawarto umowę przetwarzania sam nie przetwarza danych osobowych, zaś ich przetwarzanie podpowierza podmiotowi przetwarzającemu drugiego stopnia, to podmiot z którym zawarto umowę przetwarzania, nie jest podmiotem przetwarzającym. To wynika z definicji. Podmiot przetwarzający musi przetwarzać dane, jeśli nie przetwarza, bo dane przetwarza podmiot przetwarzający drugiego stopnia, to podmiot między administratorem danych, a podmiotem przetwarzającym drugiego stopnia, nie jest podmiotem przetwarzającym pierwszego stopnia. Pozostaje zatem pytanie, **kim w takim razie ten podmiot jest**.

- Stroną trzecią chyba nie jest, bo jednak ma zwykle prawo dostępu do danych (dlaczego piszę, że zwykle, wynika to z prowadzonych niżej rozważań),
- podmiotem przetwarzającym nie jest bo nie przetwarza danych osobowych.
- Podmiotem przetwarzającym drugiego stopnia nie jest tym bardziej, ponieważ nie przetwarza danych osobowych i ponieważ podmiotem takim jest kto inny i ponieważ (sic!) przetwarzanie powierzył mu administrator danych nie zaś podmiot przetwarzający.

Wykonałem tu swoisty, intelektualny manewr okrążający, ustaliłem kim nie jest podmiot, z którym zawarto umowę powierzenia przetwarzania, który jednak nie przetwarza danych, jednak właśnie okrążyłem problem, nie wiem bowiem nadal kim ów podmiot jest.

Wnioski, których możliwość tu dostrzegam są trzy, jednak tylko jeden z nich uważam za właściwy a mianowicie pogląd drugi, a mianowicie, ze podmiot taki jest pełnomocnikiem administratora.

Podmiot taki jest stroną trzecią. Strona trzecia zdefiniowana jest w art. 4 ust. 10 RODO, do którego odsyłam, tu jedynie, dla potrzeb wywodu zwracam uwagę, że strona trzecia to ktoś poza łańcuchem przetwarzania danych osobowych. Językowa wykładnia art. 4 ust. 10 RODO prowadzi do wniosku, że podmiot taki jest stroną trzecią. Uważam to za błędną interpretację i widzę tu potrzebę odejścia od wykładni językowej z uwagi na jej absurdalny wniosek.

Podmiot taki jest pełnomocnikiem administratora danych. Pełnomocnik taki, w zakresie swego pełnomocnictwa ma wyłącznie zawarcie umowy podpowierzenia. W takim wypadku umowa powierzenia staje się pełnomocnictwem do zawarcia umowy podpowierzenia. Pogląd ten jest kuszący. Umowa powierzenia jest pełnomocnictwem do zawarcia umowy podpowierzenia a podmiot, z którym zawarto umowę powierzenia jest pełnomocnikiem.

Uważam, że należy tu jeszcze wyróżnić **dwie sytuacje**.

Pierwsza – administrator w umowie powierzenia nakazuje pod–miotowi z którym ją zawiera, aby ten zawarł umowę podpowierzenia i aby dane przetwarzał podmiot przetwarzający, z którym zawarto umowę podpowierzenia. Podmiot, z którym administrator danych zawarł umowę powierzenia jest tu **pełnomocnikiem administratora** czyli **stroną trzecią**.

Druga – administrator w umowie powierzenia nie nakazuje podmiotowi z którym ją zawiera, aby ten zawarł umowę podpowierzenia i aby dane przetwarzał podmiot przetwarzający, z którym zawarto umowę podpowierzenia, jednak administrator danych dopuszcza w umowie powierzenia by podmiot, z którym ją zawiera, zawarł dalszą umowę powierzenia i by dane przetwarzał podmiot przetwarzający, z którym zawarto umowę podpowierzenia.

W **drugiej sytuacji** są **dwie możliwości**.

Pierwsza – podmiot, z którym administrator danych zawarł umowę powierzenia sam przetwarza dane osobowe na podstawie tej umowy. Podmiot, z którym administrator danych zawarł umowę powierzenia jest tu podmiotem przetwarzającym, co nie zaskakuje.

Druga – podmiot, z którym administrator danych zawarł umowę powierzenia sam nie przetwarza danych osobowych na podstawie tej umowy, natomiast zawiera umowę podpowierzenia. Podmiot, z którym administrator danych zawarł umowę powierzenia jest tu **pełnomocnikiem administratora** czyli **stroną trzecią**.

Podmiot taki jest podmiotem przetwarzającym. Przyjmując taką interpretację lekceważymy dosłowne znaczenie definicji strony trzeciej. Z jednej strony, nie chciałbym tego robić. Nie chciałbym lekceważyć językowego znaczenia definicji strony trzeciej. Wyżej, w niniejszej uwadze *3.1. Art. 4 pkt 8. Uwaga 1. Co odróżnia administratora danych od podmiotu przetwarzającego* założyłem, że strona trzecia to ktoś kto nie ma prawa dostępu do danych. Opisywany podmiot spełnia ten warunek, opisywany podmiot można uznać za stronę trzecią, jeśli nie ma on dostępu do danych, bo tak umownie ustalił z administratorem danych (Sytuacja Druga Możliwość Druga). Można, co napisałem wyżej w niniejszym akapicie, zlekceważyć znaczenie definicji strony trzeciej i uznać, że podmiot, który podpowierzył przetwarzanie danych i sam ich nie przetwarza jest jednak podmiotem przetwarzającym. Przyjmując tak, lekceważymy też niestety definicję podmiotu przetwarzającego, przechodząc do porządku nad faktem, że podmiot, który podpowierzył i sam nie przetwarza danych, właśnie nie przetwarza danych, czyli nie jest podmiotem przetwarzającym.

Wydaje się, że wiele uprościłaby nowelizacja komentowanego przepisu, tak by nie było wątpliwości, że podmiot, który podpowierza przetwarzanie danych i sam ich nie przetwarza, nadal jest podmiotem przetwarzającym.

Ciekawą uwagę na temat powierzenia przetwarzania danych osobowych napotkać można u M. Gumularza. Autor ten pisze, że: *(...) powierzenie danych to taka sytuacja, gdy administrator danych dopuszcza do przetwarzania danych osobowych w jego imieniu podmiot (tzw. procesor) spoza jego personelu.*[263] Wskazany autor nie ustrzegł się tu niestety przed popełnieniem pewnego błędu, a mianowicie pisze on o powierzeniu danych podczas gdy powinien był napisać o powierzeniu przetwarzania danych. Pomijając jednak ten błąd, ufam, że jedynie językowy - nie chce mi się bowiem wierzyć iżby M. Gumularz nie rozumiał istoty zagadnienia, samo cytowane zdanie niesie w sobie pewną prawdę. Rzeczywiście, kiedy administrator powierza przetwarzanie danych to dopuszcza on by podmiot przetwarzający, czyli przecież ktoś inny niż administrator, przetwarzał dane osobowe.

[263] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział. III. GŁÓWNI AKTORZY RODO. 3. Kolejne podmioty w łańcuchu przetwarzania danych: osoby upoważnione oraz podmioty przetwarzające. 3.2.Powierzenie. 3.2.1. Powierzenie danych a udostępnienie danych i współadministrowanie,* Warszawa 2018, Lex.

W ciekawych bardzo wywodach M. Gumularza na temat powierzenia brak jest elementu, z którego wynikałoby, że umowa powierzenia przetwarzania nie decyduje o tym czy relacja powierzenia przetwarzania zachodzi czy nie. Nie wykluczam, że wskazany autor uważa to za cos tak oczywistego, że o tym nie pisze. Tym niemniej M. Gumularz czujnie przypomina o tym że umowa powierzenia powinna zostać zawarta w formie pisemnej, w tym elektronicznej, co wynika z art. 28 ust. 9 RODO. *3.15. Art. 4 pkt 8. Uwaga 15. Powierzenie przetwarzania – forma umowy.* Zgadzam się z M. Gumularzem, że *(...) RODO nie wymaga w tym przypadku zachowania formy elektronicznej zgodnie z Kodeksem cywilnym (...)*. Przemawia do mnie argumentacja M. Gumularza, zgodnie z którą konieczność autonomicznej wykładni RODO, w oderwaniu od przepisów krajowego prawa cywilnego wynika z faktu, że poszczególne kraje UE, w sposób autonomiczny regulują kwestie formy czynności prawnych. Argumentacja przemawia, jednak problem formy, faktycznej formy, w której strony zawierają taką umowę, pozostaje otwarty. Potwierdzenie takiej umowy podpisem elektronicznym, najlepiej kwalifikowanym, wydaje się zasadne, z tym, że to właśnie wskazana wyżej forma elektroniczna w rozumieniu Kodeksu cywilnego.

Obserwacje wskazują, że umowy takie zawierane są często przez przystąpienie, lub z wykorzystaniem dokumentów elektronicznych, jednak bez potwierdzania podpisem elektronicznym.

3.2. Art. 4 pkt 8. Uwaga 2. Problemy z odróżnieniem administratora danych od podmiotu przetwarzającego

Wyżej w analizie *2. Art. 4 pkt 8. Analiza* piszę, że *(...) trudno czasem ustalić czy podmiot, który przetwarza dane osobowe, przetwarza je w swoim imieniu czy przetwarza je w imieniu administratora*. Dla lepszego rozpatrzenia problemu należy wyobrazić sobie umowę, w której występują dwa podmioty. (Pomijam tu powierzenie na podstawie innego niż umowa instrumentu i powierzenie bezumowne.) Pierwszy z nich to zleceniodawca. Drugi z nich to zleceniobiorca. Zleceniodawca jest administratorem danych. Pozostaje ustalić kim jest zleceniobiorca. Czy odbiorcą – nowym administratorem danych, czy podmiotem przetwarzającym. Jak wiadomo z przepisu, podmiot przetwarzający przetwarza dane w imieniu administratora. Jeżeli zatem

zleceniobiorca przetwarza dane osobowe w imieniu administratora to jest podmiotem przetwarzającym. Jeżeli natomiast zleceniobiorca przetwarza dane osobowe we własnym imieniu to jest administratorem, nowym administratorem, odbiorcą – administratorem.

Lektura przepisu i żonglowanie jego słowami prowadzą do wniosku, że odróżnienie podmiotu przetwarzającego od nowego administratora jest proste i nie przysparza trudności, niestety tak nie jest. Praktyka uczy, że często trudno jest odróżnić administratora od podmiotu przetwarzającego. Ciężko jest te podmioty rozróżnić, ponieważ w relacji miedzy zleceniodawcą a zleceniobiorcą, zleceniobiorca jest zainteresowany przetwarzaniem danych jedynie dlatego, że istnieje ta relacja. Zleceniobiorca przetwarza dane osobowe w związku z wykonywaniem przez niego umowy zlecenia. Zleceniobiorca przetwarza dane osobowe, ponieważ łączy go ze zleceniodawcą umowa, gdyby umowy nie było, to tych danych osobowych, których administratorem jest dany administrator – zleceniodawca, zleceniobiorca by nie przetwarzał, ponieważ nie byłby zleceniobiorcą. Odróżnienie zatem podmiotu przetwarzającego od nowego administratora jedynie na tej podstawie, że podmiot przetwarza dane osobowe w imieniu administratora, czyli nie w swoim, jest trudne, może prowadzić do mylnych wniosków, co więcej może dać wynik fałszywie negatywny lub fałszywie pozytywny. By tego uniknąć należy posłużyć się inną metodą. Metodę tę opisuję w uwadze *3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie przetwarzania jako zlecenie czynności na danych osobowych.*

Jak piszę wyżej: *Przetwarzanie danych osobowych w imieniu administratora danych jest konstytutywne dla bycia podmiotem przetwarzającym 2. Art. 4 pkt 8. Analiza*. Zawarcie umowy jest obowiązkiem administratora. Należy się zgodzić z M. Gumularzem, który ładnie podsumował to w zdaniu: *Niezawarcie umowy powierzenia lub zawarcie umowy o błędnej treści może być oceniane m.in. przez pryzmat art. 83 ust. 4 RODO, prowadząc do odpowiedzialności zarówno po stronie administratora, jak i procesora*[264].

[264] M. Gumularz, *loc. cit*.

3.3. Art. 4 pkt 8. Uwaga 3. Konieczność odróżnienia administratora danych od podmiotu przetwarzającego

W sytuacji, w której występuje zleceniobiorca/administrator danych i zleceniodawca, konieczne jest precyzyjne ustalenie czy zleceniobiorca jest administratorem/odbiorcą czy podmiotem przetwarzającym. Doniosłość problemu oddaje tu zdanie, które znaleźć można na stronie brytyjskiego organu ochrony danych – ICO, brzmi ono w języku polskim: *Zrozumienie roli w odniesieniu/relacji do danych osobowych, które się przetwarza jest decydujące dla zapewnienia zgodności z RODO i odpowiedniego traktowania osób fizycznych*.[265]

Należy pamiętać, że jeśli zleceniodawca zleca zleceniobiorcy wykonanie zlecenia i w związku z tym zleceniem ujawnia zleceniobiorcy dane, to nie zawsze oznacza to, że zachodzi powierzenie. Powierzenie zachodzi albo nie zachodzi, zależnie od tego, czy zleceniobiorca przetwarza dane w imieniu zleceniodawcy (powierzenie zachodzi) czy w swoim (powierzenie nie zachodzi).

Należy pamiętać, że napisanie umowy powierzenia nie statuuje relacji powierzenia. Nieco trywializując, można powiedzieć, że można napisać i podpisać nie jedną a sto umów powierzenia a powierzenia jak nie ma tak nie ma. Co więcej umowy te są niebezpieczne, zwłaszcza dla zleceniobiorcy. Są niebezpieczne ponieważ wskutek podpisania takich umów, zleceniobiorca mylnie uważa, że jest podmiotem przetwarzającym, podczas gdy jest on administratorem. Jeżeli administrator uważa, że jest podmiotem przetwarzającym to nie realizuje obowiązków administratora. Wystarczy wymienić art. 13 RODO i art. 14 RODO. Niezrealizowanie tych przepisów, w sytuacji braku zwolnień (dla uproszczenia wywodu, zostawiam tu zwolnienia na boku), grozi odpowiedzialnością administracyjną i cywilną. Oczywiste jest, że administrator danych, który uważa, że jest podmiotem przetwarzającym nie realizuje art. 13 RODO lub (odpowiednio) art. 14 RODO, właśnie dlatego, że uważa, że jest podmiotem przetwarzającym. Uważa to mylnie, niczego to jednak nie zmienia w jego sytuacji prawnej. Z tego choćby względu, odróżnienie podmiotu przetwarzającego od administratora jest takie ważne. O problemach z opisanym odróż-

[265] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ dostęp: 2019.09.07, godz. 9.20. Tłum.: Jakub Rzymowski

nieniem piszę w uwadze *3.2. Art. 4 pkt 8. Uwaga 2. Problemy z odróżnieniem administratora danych od podmiotu przetwarzającego*, metodę odróżnienia opisuję w uwadze *3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie przetwarzania jako zlecenie czynności na danych osobowych*.

3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie przetwarzania jako zlecenie czynności na danych osobowych

Dla odróżnienia podmiotu przetwarzającego od administratora/odbiorcy, należy przeprowadzić pewne, rozumowanie. Rozumowanie to prowadzę przy założeniu, że powierzenie przetwarzania zachodzi na podstawie umowy. Pomijam tu inny instrument prawny, o którym jest również, jak i o umowie, mowa w art. 28 ust. 3 RODO.

Powierzenie przetwarzania jest umową.

Powierzenie przetwarzania jest umową o świadczenie usług.

Do umów o świadczenie usług należy stosować przepisy o zleceniu. Wynika to z art. 750 K.C.[266]

Można zatem powiedzieć, że powierzenie przetwarzania danych osobowych to umowa zlecenia. Jest to pewnym uproszczeniem, jednak uproszczenie to nie narusza w żaden sposób prowadzonego rozumowania i jednocześnie ogromnie je upraszcza.

Przetwarzanie można z powodzeniem utożsamić z czynnością na danych. i to jest pewnym uproszczeniem, pomijam bowiem kwestię zestawów danych i zestawów czynności, odsyłam do komentarza do art. 4 pkt 2 RODO.

Powierzenie przetwarzania danych osobowych jest to zatem zlecenie czynności na danych.

Dla podkreślenia wniosku, warto powtórzyć go w wersji precyzyjnej, co czynię poniżej.

Powierzenie przetwarzania danych osobowych znaczy to samo co zlecenie czynności na danych osobowych.

Jeżeli zatem administrator/zleceniodawca zleca zleceniobiorcy wykonanie jakichś czynności, to przed udzieleniem odpowiedzi na pytanie o to czy zleceniobiorca (z umowy podstawowej) jest administra-

[266] Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny. Dz.U. 1964 nr 16 poz. 93 ze zm. t. j. Dz.U. 2019 poz. 1145.

torem/odbiorcą, czy podmiotem przetwarzającym, należy zastanowić się nad tym co jest przedmiotem umowy.

Jeżeli przedmiotem umowy jest wykonanie czynności na danych osobowych, to zleceniobiorca (z umowy podstawowej) jest podmiotem przetwarzającym.

Jeżeli przedmiotem umowy jest co innego niż wykonanie czynności na danych, to zleceniobiorca jest administratorem/odbiorcą. Należy przy tym pamiętać, że często zleceniodawca przekazuje zleceniobiorcy jakieś dane osobowe, bowiem bez tego przekazania wykonanie umowy zlecenia – umowy podstawowej byłoby niemożliwe, jednak samo przekazanie danych, ich ujawnienie, nie czyni ze zleceniobiorcy podmiotu przetwarzającego. Dane przekazane to po prostu informacje konieczne do wykonania umowy.

3.5. Art. 4 pkt 8. Uwaga 5.
Umowa podstawowa a umowa powierzenia przetwarzania

Powierzenie przetwarzania zwykle zachodzi na podstawie umowy. Dla zajścia powierzenia przetwarzania nie jest jednak konieczne podpisanie umowy powierzenia przetwarzania. Czasem administrator danych i podmiot przetwarzający zawierają umowę, wskutek której strona umowy inna niż administrator staje się właśnie podmiotem przetwarzającym jednak umowa ta nie jest wcale umową powierzenia przetwarzania. Umowa ta jest inna umową, jednak wskutek jej realizacji pojawia się zjawisko powierzenia przetwarzania i zjawisko przetwarzania przez podmiot przetwarzający w imieniu administratora. Dla uproszczenia, w poniższym rozumowaniu, umowę tę, umowę łączącą administratora z podmiotem przetwarzającym, jednak nie będącą umową powierzenia przetwarzania, nazywam umową podstawową. Czasem administrator danych i podmiot przetwarzający zawierają umowę podstawową i umowę powierzenia przetwarzania. Możliwości jest tu więcej, zestawiam je poniżej.

Jeżeli zachodzi zjawisko przetwarzania przez podmiot przetwarzający w imieniu administratora danych, to możliwe są wymienione poniżej sytuacje.[267]

[267] Wyliczenie poniższe jest wersją rozwiniętą i uzupełnioną, udzielonej przeze mnie odpowiedzi na pytanie, jakie zadano mi kiedyś w jednej z grup poświęconych danym osobowych w portalu Facebook. Pytanie zadał mi pan. G. Sterniczuk. Niestety nie odnotowałem daty, miało to miejsce w roku 2019 lub 2020.

Sama umowa powierzenia przetwarzania – sytuacja dziwaczna. Samo powierzenie bez określenia szczegółów, czego ono dotyczy, jest jak czysta powinność u Kelsena, niby zachodzi ale trudno powiedzieć, że wywołuje jakiekolwiek skutki. Nie wywołuje skutków ponieważ na przykład ze słów: „Administrator danych powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu" nie wynika tak naprawdę czego administrator oczekuje od podmiotu przetwarzającego. Nawet więcej, nie wynika z niej czy administrator naprawdę powierza przetwarzanie, czy jedynie tak mu się wydaje i to swoje mylne odczucie zawiera w umowie.

Umowa powierzenia przetwarzania zawierająca elementy umowy podstawowej – sytuacja poprawna. Zawarto umowę powierzenia – zrealizowano art. 28 RODO, wiadomo co jest przedmiotem umowy.

Sama umowa powierzenia przetwarzania nie mająca w sobie nawet słowa o powierzeniu, ale wypełniająca cechy umowy powierzenia (zlecenie czynności na danych) – sytuacja poprawna. Administrator zawiera umowę, której przedmiotem jest przetwarzanie danych osobowych w imieniu administratora. W umowie tej zawarte są wszystkie elementy konieczne dla umowy powierzenia przetwarzania, wynikające z art. 28 RODO.

Umowa podstawowa i umowa powierzenia przetwarzania – sytuacja poprawna nawet bardzo dobra.

Sama umowa podstawowa z zawartymi w niej elementami umowy powierzenia przetwarzania – wersja poprawna, wręcz bardzo dobra.

Sama umowa podstawowa bez umowy powierzenia przetwarzania bez elementów umowy powierzenia przetwarzania – sytuacja niewłaściwa, ponieważ brak jest umowy powierzenia – nie zrealizowano art. 28 RODO, powierzenie i tak zachodzi, oczywiście jeżeli umowa skutkuje przetwarzaniem danych osobowych przez zleceniobiorcę w imieniu zleceniodawcy.

Brak umowy podstawowej i umowy powierzenia przetwarzania (prowadzenie cudzych spraw bez zlecenia, skutkujące pojawieniem się przetwarzania przez prowadzącego cudze sprawy bez zlecenia w imieniu tego, czyje sprawy są prowadzone) – sytuacja niewłaściwa, ponieważ brak jest umowy powierzenia – nie zrealizowano art. 28 RODO, powierzenie, a dokładniej przetwarzanie w imieniu administratora przez podmiot przetwarzający i tak zachodzi.

Leszek Kępa proponuje nieco krótsze zestawienie, które, w pewnym zakresie, pokrywa się z moim zestawieniem. Przytaczam je poniżej, uznając taką wersję za lepszą od wstawienia pozycji zestawienia L. Kępy między pozycje mojego zestawienia, z uwagi na pewną wartość dodaną jaką ma każde z zestawień, kiedy występuje w postaci pierwotnej. Leszek Kępa pisze zatem jak cytuję poniżej.
Zapisy związane z powierzeniem przetwarzania danych osobowych można zawrzeć na kilka sposobów:
- w umowie głównej (jako jej integralna część),
- aneks do umowy głównej (jako „dodatek"),
- odrębna umowa.[268]

3.6. Art. 4 pkt 8. Uwaga 6.
Umowne powierzenie przetwarzania a nieprzetwarzanie danych

Fakt, że podmiot przetwarzający przetwarza dane osobowe wydaje się truizmem, można sobie jednak wyobrazić sytuacje, w której administrator (danych osobowych) podpisał umowę powierzenia przetwarzania z podmiotem przetwarzającym, jednak podmiot ten nie przetwarza danych osobowych w imieniu administratora (o tym niżej). W tej sytuacji wątpliwe jest czy podmiot, z którym podpisano umowę powierzenia przetwarzania jest rzeczywiście podmiotem przetwarzającym.

3.7. Art. 4 pkt 8. Uwaga 7.
Bezumowne powierzenie przetwarzania danych osobowych a prowadzenie cudzych spraw bez zlecenia

Z komentowanego przepisu wynika jeszcze coś. Otóż przepis definiuje podmiot przetwarzający jako *(...) podmiot, który przetwarza dane osobowe w imieniu administratora*, jak więc widać przepis w żaden sposób nie odwołuje się do art. 28 RODO, który ustanawia kolejne warunki dla podmiotu przetwarzającego i określa konieczne, minimalne elementy umowy powierzenia przetwarzania. Można rzec, że definicja podmiotu przetwarzającego i art. 28 dotyczący tego podmiotu, stoją obok siebie. Żaden z dwóch wskazanych przepisów do drugiego wprost nie odsyła. Jednocześnie w art. 28 poważnie doprecyzowano kto może być podmiotem przetwarzającym, oraz w szczegó-

[268] L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 146.

łach określono elementy umowy powierzenia przetwarzania, czyli w pewnym sensie doostrzono definicję podmiotu przetwarzającego.

Można sobie wyobrazić sytuację, w której podmiot przetwarza dane osobowe w imieniu administratora, jednak nie łączy tego podmiotu z administratorem umowa powierzenia przetwarzania ani inny instrument prawny, o którym mowa w art., 28 ust. 3 RODO. W takiej sytuacji i tak między podmiotami zachodzi relacja powierzenia przetwarzania danych osobowych, powstaje ona bowiem nie tyle w wyniku zawarcia umowy powierzenia przetwarzania, ile w wyniku przetwarzania w imieniu administratora danych osobowych. Dostrzegam tu pewną analogię do zjawiska prowadzenia cudzych spraw bez zlecenia. Analogia ta wydaje się być o tyle trafna, że umowa powierzenia przetwarzania danych osobowych to w istocie umowa zlecenia przetwarzania danych osobowych.

Podsumowując, można stwierdzić, że o ile zawarcie umowy powierzenia przetwarzania może ustanowić relację, w której powierzenie przetwarzania zachodzi, o tyle dla ustanowienia takiej relacji, zawarcie umowy nie jest niezbędne. Ładnie ujęła to M. Sakowska-Baryła, która twierdzi, że: *(...) przetwarzanie danych osobowych na zasadzie powierzenia to stan faktyczny, z którym RODO (...) wiąże określone skutki prawne (...). Brak pisemnej umowy lub innego aktu prawnego (...) nie oznacza jednak, że w danym przypadku powierzenie przetwarzania nie wystąpiło*[269]. Zaznaczam, że słowa o „zasadzie powierzenia" są tu zapewne użyte przypadkowo, bowiem powierzenie przetwarzania nie znajduje się w katalogu zasad dotyczących przetwarzania danych osobowych, znajdującym się w art. 5 RODO.

Zawarcie umowy powierzenia przetwarzania danych osobowych jest obowiązkiem wynikającym z RODO jeżeli powierzenie przetwarzania zachodzi lub ma zachodzić. Jeżeli jednak zleceniodawca i zleceniobiorca nie zawrą umowy powierzenia przetwarzania i jednocześnie powierzenie przetwarzania zachodzi, to fakt, że nie zawarli oni umowy powierzenia przetwarzania nie powoduje, że powierzenie przetwarzania nie zachodzi. Powierzenie przetwarzania danych osobowych zachodzi a administrator i podmiot przetwarzający naru-

[269] M. Sakowska-Baryła w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 107.

szają art. 28 RODO[270], w kontekście art. 4 pkt 8 RODO (piszę o kontekście, trudno bowiem wyobrazić sobie naruszenie definicji).

Zestawienie sytuacji, w których powierzenie przetwarzania zachodzi, zaś umowę stosowna zawarto lub nie znajduje się w uwadze *3.5. Art. 4 pkt 8. Uwaga 5. Umowne powierzenie przetwarzania a nieprzetwarzanie danych*.

3.8. Art. 4 pkt 8. Uwaga 8. Niedopuszczalność realizacji własnych celów podmiotu przetwarzającego

Ciekawe zdanie można znaleźć w komentarzu P. Litwińskiego, P. Barty i M. Kaweckiego. Autorzy ci piszą, że podmiot przetwarzający „nie może więc – przetwarzając dane osobowe w imieniu administratora danych – realizować własnych celów przetwarzania danych".[271] W zdaniu tym tkwi ziarno prawdy, jednak mam wobec niego kilka uwag.

Wniosek zawarty w zdaniu, wskazani autorzy wywodzą z faktu, że *przetwarzanie danych osobowych zawsze odbywa się w imieniu administratora danych*. O ile zgadzam się z tym, że przetwarzanie danych osobowych zawsze odbywa się w imieniu administratora danych, o tyle uważam, że fakt, że podmiot przetwarzający nie może realizować własnych celów, budzi moje wątpliwości. Na pierwszy rzut oka wygląda to dobrze, skoro administrator danych powierza przetwarzanie danych, to podmiot przetwarzający przetwarza nie w celu własnym ale w celu, który jest celem administratora. Niestety wygląda to dobrze jedynie do momentu, w którym przechodzimy na przykłady.

Zleceniodawca/administrator (danych) zleca wykonanie czynności na danych, powoduje to, że zleceniobiorca staje się podmiotem przetwarzającym. Należy jednak przy tym pamiętać, że celem zleceniobiorcy jest zwykle realizacja takich zleceń. Można próbować wywieść, że celem zleceniobiorcy jest realizacja zlecenia nie zaś celu zawartego w zleceniu. Inaczej patrząc, zleceniodawca ma własny cel, zleca zleceniobiorcy realizację tego celu „celu zleceniodawcy", zlece-

[270] Podobnie: M. Sakowska-Baryła, *loc. cit.*

[271] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 226.

niobiorca realizuje zlecenie, celem zleceniobiorcy jest realizacja zlecenia, którego z kolei przedmiotem jest realizacja „celu zleceniodawcy". Jeśli tak patrzymy to okazuje się, że występuje „cel zleceniodawcy" i „cel zleceniobiorcy".

Cel zleceniobiorcy to realizacja zlecenia zleceniodawcy, czyli cel zleceniobiorcy ma wobec celu zleceniodawcy charakter metacelu, nadcelu, celu drugiego stopnia, poziomu, rzędu.

Niestety mam świadomość, że rozważania o celu zleceniodawcy i metacelu zleceniobiorcy mają nieco charakter żonglerki słowem a żonglerka przystoi raczej w cyrku niż przy okazji dokonywania wykładni. Uważam te (moje przecież własne) rozważania za żonglerkę, ponieważ należy pamiętać, że czy to „cel zleceniodawcy" czy to „cel zleceniobiorcy" – oba prowadzą do tego samego, do wykonania czynności. Czynności, której wykonanie zleceniodawca zleca zleceniobiorcy.

Dodatkowy problem jest skutkiem tego, że jeżeli administrator/zleceniodawca danych zleca zleceniobiorcy wykonanie jakiejś czynności w sytuacji, w której zleceniobiorca staje się nowym administratorem danych, to przecież zleceniobiorca wykonuje tę czynność dlatego, że zleceniodawca mu ją zlecił, na przykład reprezentuje go w sądzie, leczy jego pracowników, drukuje wizytówki. Co gorsza, co prawda nie jest to czynność na danych, jednak czynność, do której dane są konieczne. Rozplątanie tego węzła może być czasem bardzo trudne, jeżeli rozplątujący go posługuje się tylko kryterium celu. Rozplątanie węzła może być nie dość, że trudne to i niebezpieczne prawnie, ponieważ jeżeli rozplątujący rozplącze go źle, to źle zrealizuje np. obowiązek informacyjny i tym samym naraża się na odpowiedzialność.

Wracając do myśli P. Litwińskiego, P. Barty i M. Kaweckiego, można podsumować, że prawdą jest, że podmiot przetwarzający realizuje cel przetwarzania administratora, jednak ustalenie, że ten a ten cel jest celem administratora, a inny cel jest celem zleceniobiorcy, skoro już nie podmiotu przetwarzającego, to nowego administratora, jest uważam tak trudne, że może być zawodne, przez co jest niebezpieczne.

3.9. Art. 4 pkt 8. Uwaga 9. Krokowa metoda ustalenia czy podmiot jest administratorem danych (odbiorcą) czy podmiotem przetwarzającym

Przetwarzanie danych osobowych w imieniu administratora lub nie w imieniu administratora może nie wystarczyć do ustalenia czy dany podmiot jest administratorem czy podmiotem przetwarzającym, jest tak ponieważ rozstrzygnięcie dylematu interpretacyjnego może być po prostu w danej sytuacji tak trudne, że dla danego rozstrzygającego niemożliwe. O zagrożeniach związanych z mylnym rozróżnieniem między administratorem danych a podmiotem przetwarzającym piszę w uwadze *3.3. Art. 4 pkt 8. Uwaga 3. Konieczność odróżnienia administratora danych od podmiotu przetwarzającego*. Jak zatem widać, oparcie metody służącej do ustalania czy podmiot jest administratorem danych czy podmiotem przetwarzającym, jedynie o to w czyim imieniu dane są przetwarzane, może być zawodne i groźne.

Bardziej niezawodną wydaje się być metoda oparta na tym czy administrator (danych) zleca czynność na danych czy inną czynność, do której wykonania dane osobowe są niezbędne. *3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie przetwarzania jako zlecenie czynności na danych osobowych*.

Kolejną metodą jest metoda oparta o to czy administrator (danych) może skutecznie żądać zwrócenia danych osobowych od podmiotu który jest administratorem danych/odbiorcą lub podmiotem przetwarzającym.[272]

Jeszcze jedna metoda oparta może być o fakt, że podmiot, który badamy pod kątem ustalenia czy jest on administratorem (danych) czy podmiotem przetwarzającym, nie może zwrócić danych pierwotnemu administratorowi, ponieważ prawo mu to uniemożliwia. Przykładem są tu osoby/podmioty wykonujące niektóre zawody czy rodzaje działalności regulowane prawem, takie jak adwokat, doradca podatkowy, notariusz, szpital, przychodnia.

[272] Metodę tę stosuje pewien ze znanych mi praktyków ochrony danych i RODO – Rafał Kosuń z firmy DataLex. Rafała Kosunia znam osobiście, warto wskazać na jego pogląd, z uwagi na trafność poglądu i wygodę w stosowaniu, opartej o pogląd metody, acz metoda ta musi być czasem uzupełniana, o to czy czynność zlecana jest czynnością na danych, czego R. Kosuń ma świadomość.

Mając na uwadze powyższe rozważania można skonstruować metodę służącą do ustalania czy dany podmiot jest administratorem danych czy podmiotem przetwarzającym.

Krok 1.
Czy podmiot przetwarza dane osobowe w imieniu (pierwotnego) administratora czy podmiot przetwarza dane osobowe we własnym imieniu?
Jeżeli podmiot przetwarza dane osobowe w imieniu (pierwotnego) administratora to podmiot ten jest podmiotem przetwarzającym
Jeżeli podmiot przetwarza dane osobowe we własnym imieniu to podmiot ten jest administratorem (odbiorcą).

Krok 1 jest pozornie przesądzający, niestety tylko pozornie, trudno bowiem czasem wręcz zrozumieć w czyim imieniu podmiot przetwarza.
Mając to na uwadze, trzeba mieć świadomość, że
zarówno wynik, w którym zleceniobiorca jest administratorem danych, może być fałszywy,
jak i wynik, w którym zleceniobiorca jest podmiotem przetwarzającym może być fałszywy.

Krok 2.
Czy podmiot lub osoba wykonuje zawód lub działalność uregulowaną prawem w taki sposób, że działa w sposób, który nie dopuszcza przyjmowania wskazówek od zleceniodawcy? Zwykle wiąże się to również z obowiązkiem przechowywania danych po wykonaniu zlecenia i niemożnością zwrócenia tych danych (pierwotnemu) administratorowi.
Jeżeli podmiot lub osoba wykonuje zawód lub działalność uregulowaną prawem w taki sposób, że działa w sposób, który nie dopuszcza przyjmowania wskazówek od zleceniodawcy, to taki podmiot lub osoba jest administratorem (odbiorcą).
Jeżeli podmiot lub osoba nie wykonuje zawodu lub działalności uregulowanej prawem w taki sposób, że działa w sposób, który nie dopuszcza przyjmowania wskazówek od zleceniodawcy, to taki podmiot lub osoba jest administratorem (odbiorcą), lub podmiotem przetwarzającym, lecz w Kroku 2 tego nie ustalono, należy wykonać kroki następne.

Innymi słowy,
twierdząca odpowiedź na pytanie skutkuje wynikiem pozytywnym, który wydaje się być wiarygodny,
przecząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który może być fałszywie negatywny.

Krok 3
Czy administrator zleca przetwarzanie w celu, do realizacji, którego sam nie jest uprawniony, którego nie wolno mu realizować?
Jeżeli administrator zleca przetwarzanie w celu, do realizacji, którego sam nie jest uprawniony, którego nie wolno mu realizować, to zleceniobiorca jest podmiot lub osoba wykonuje zawód lub działalność do realizacji których administrator jest uprawniony, to taki podmiot lub osoba jest administratorem (odbiorcą).
Jeżeli administrator zleca przetwarzanie w celu, do realizacji, którego sam jest uprawniony, który wolno mu realizować, to zleceniobiorca jest podmiotem przetwarzającym.
Innymi słowy,
twierdząca odpowiedź na pytanie skutkuje wynikiem pozytywnym, który wydaje się być wiarygodny,
przecząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który również wydaje się być wiarygodny.

Pomocny może być tu pogląd M. Gumularza, który zwraca uwagę, że: *(...) jeżeli dwa podmioty z sektora publicznego mają swoje samodzielne cele przetwarzania danych związane z realizacją ich samodzielnych zadań, to podmioty te są niezależnymi administratorami danych (a wymiana danych osobowych w tym układzie nie jest powierzeniem danych)*[273]. Problem polega niestety czasem na tym, że trudno jest ustalić czyje cele realizuje dany podmiot. Zwykle podmiot realizuje własne cele.

[273] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym. Rozdział III. GŁÓWNI AKTORZY RODO. 3. Kolejne podmioty w łańcuchu przetwarzania danych: osoby upoważnione oraz podmioty przetwarzające. 3.2. Powierzenie. 3.2.1. Powierzenie danych a udostępnienie danych i współadministrowanie,* Warszawa 2018, Lex.

Krok 4.
Czy administrator może skutecznie żądać zwrócenia danych od podmiotu który jest administratorem danych/odbiorcą lub podmiotem przetwarzającym? Nie wykluczam, że krok 4 tożsamy jest z krokiem 3 aczkolwiek nie mam tu całkowitej pewności.
Jeżeli administrator nie może skutecznie żądać zwrócenia danych od podmiotu który jest administratorem danych/odbiorcą lub podmiotem przetwarzającym, to podmiot ten jest administratorem danych (odbiorcą).
Jeżeli administrator może[274] skutecznie żądać zwrócenia danych od podmiotu który jest administratorem danych/odbiorcą lub podmiotem przetwarzającym, to podmiot ten jest podmiotem przetwarzającym lub administratorem, lecz w Kroku 3 tego nie ustalono, należy wykonać kroki następne.
Innymi słowy,
przecząca odpowiedź na pytanie skutkuje wynikiem pozytywnym, który wydaje się być wiarygodny,
twierdząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który może być fałszywie negatywny.

Krok 5.
Czy administrator zleca wykonanie czynności na danych?
Jeżeli administrator zleca wykonanie czynności na danych, to zleceniobiorca jest podmiotem przetwarzającym.
Jeżeli administrator zleca wykonanie innej czynności niż czynność na danych, to zleceniobiorca jest administratorem danych (odbiorcą).
Innymi słowy,
twierdząca odpowiedź na pytanie skutkuje wynikiem pozytywnym który może być fałszywie pozytywny,
przecząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który wydaje się być wiarygodny.

Podobne spostrzeżenia a mianowicie, ze zleceniobiorca jest podmiotem przetwarzającym, poczynił. L. Kępa, szczególnie podoba

[274] Podobnie: M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Część I ZAGADNIENIA OGÓLNE ORAZ PROCES PRZETWARZANIA DANYCH OSOBOWYCH W JEDNOSTKACH ORGANIZACYJNYCH POMOCY SPOŁECZNEJ. 6.Umowy o powierzeniu przetwarzania danych osobowych,* Warszawa 2019, Lex.

mi się następujące zdanie tego autora: *Zlecenie innemu podmiotowi (firmie) przetwarzania danych osobowych w celu realizacji określonego zadania określa się mianem powierzenia przetwarzania*.[275] Leszek Kępa zwrócił uwagę na ciekawy niuans, powierzenie przetwarzania to zlecenie przetwarzania w celu realizacji zadania, ja dodam, że powierzeniem przetwarzania nie jest zlecenie realizacji zadania w związku z którym zleceniobiorca musi jakieś dane przetworzyć.

Niestety L. Kępa nie ustrzegł się przed pewnym błędem. Autor ten wymienił dwanaście przykładów, z których część to sytuacje, w których zachodzi powierzenie, część to sytuacje, w których zachodzi udostępnienie, po czym stwierdził: *Z przykładów wynika, że umowę powierzenia należy zawierać, jeśli przedmiotem umowy są operacje na danych osobowych*[276] – z czym się zgadzam w pełni, niestety dalej zdanie brzmi *lub gdy zleceniobiorca będzie musiał zapoznawać się z danymi osobowymi, aby wykonać zlecenie*[277], co jest błędem. Błąd ten jest o tyle mniej rażący, że praca L. Kępy powstała w poprzednim stanie prawnym, jednak należy podkreślić, że już z samej definicji podmiotu przetwarzającego wynika, że dostęp do danych nie oznacza konieczności zawarcia umowy powierzenia przetwarzania. Konieczne jest jeszcze przetwarzanie (przez zleceniobiorcę) w imieniu administratora (zleceniodawcy).

Dla potrzeb polemiki z L. Kępą nie chcę powtarzać argumentów, które znajdują się powyżej i poniżej mojej niniejszej wypowiedzi, zaznaczam tylko, że pogląd L. Kępy jest błędny, autor ten podał po prostu źle dobrane przykłady, wymieszał administratorów i podmioty przetwarzające, założył, że podmioty z jego wyliczenia powinny mieć umowę powierzenia przetwarzania, po czym założenie to udowodnił. Wskazany autor niejako wymieszał podmioty przetwarzające z podmiotami, które zależnie od szczegółów zlecenia są podmiotami przetwarzającymi lub nimi nie są i dodał do tego „świadczenie usług doradztwa prawnego", które skutkuje powstanie relacji administrator/administrator. Poszczególne przykłady L. Kępy omawiam w uwagach *3.11. Art. 4 pkt 8. Uwaga 11. Przykładowi odbiorcy,*

[275] L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 144-145.

[276] L. Kępa, *op. cit.* s. 151.

[277] L. Kępa, *loc. cit.*

administratorzy danych, nie podmioty przetwarzające i *3.12. Art. 4 pkt 8. Uwaga 12. Przykładowe podmioty przetwarzające*.

Analogiczny błąd popełnia M. Bochenek. Autor ten opisuje sytuację, w której gminny *ośrodek pomocy społecznej podpisał umowę na świadczenie usług tymczasowego schronienia dla osób bezdomnych z terenu gminy objętej jej działaniem*[278]. Autor ten zastanawia się, czy należy obok wskazanej umowy, zawrzeć umowę powierzenia i pisze, że w *opisanym przypadku występuje konieczność zawarcia umowy powierzenia przetwarzania danych osobowych, ponieważ imię i nazwisko oraz połączenie tych identyfikatorów z informacją, że osoba korzysta z konkretnego świadczenia z pomocy społecznej w danej gminie pozwala na zidentyfikowanie osoby fizycznej*[279]. Drugi zacytowany fragment pokazuje jaką drogą idzie myśl M. Bochenka. Autor ten, jak widać uważa, że skoro człowieka można zidentyfikować, to należy zawrzeć umowę powierzenia i w ogóle nie zastanawia się przy tym nad przedmiotem zawieranej umowy. Pogląd M. Bochenka jest oczywiście błędny, wskazuje go jednak jako przykład tego jak rozumować nie należy. Podkreślenia wymaga, że w przeciwieństwie do poglądu L. Kępy, pogląd M. Bochenka został opublikowany już pod rządami RODO.

W swym mylnym rozumowaniu M. Bochenek jest konsekwentny, dalej rozważa bowiem sytuację, w której *gmina (OPS) zawiera umowę z podmiotem niepublicznym na zakup usługi udzielenia tymczasowego schronienia w placówce prowadzonej przez podmiot niepubliczny*, trafnie zauważa, że gmina *będzie niewątpliwie przekazywać dane osobowe osób korzystających z tej formy pomocy*[280] i kiedy już mam prawniczą nadzieję, że M. Bochenek zauważy, że zlecenie usługi udzielenia tymczasowego schronienia nie jest zleceniem usługi na danych osobowych w imieniu administratora, tylko zleceniem czegoś na kształt usługi hotelowej, M. Bochenek pisze: *Ośrodek pomocy społecznej powinien przede wszystkim uregulować zasady przekazania, przetwarzania i zabezpieczenia przedmiotowych danych przez podmiot niepubliczny (podmiot przetwarzający) w umowie o powierzeniu przetwarzania danych, zawartej z wyłonionym wykonawcą, zgodnie z art.*

[278] M. Bochenek, *loc. cit.*

[279] M. Bochenek, *loc. cit.*

[280] M. Bochenek, *loc. cit.*

28 ust. 3 RODO[281]. Dalej M. Bochenek wywodzi, że do zadań gminy *należy m.in. udzielanie schronienia, zapewnienie posiłku oraz niezbędnego ubrania osobom tego pozbawionym*[282], jednak nawet pisząc o zapewnieniu ubrania, nie zauważa, że (trywializując nieco) kupno spodni i koszuli, nie jest czynnością na danych osobowych w imieniu administratora a w dodatku w ogóle nie jest czynnością na danych osobowych.

Co ciekawe dalej M. Bochenek rozważa czy ośrodek pomocy społecznej *musi zawrzeć umowę powierzenia danych osobowych ze szkołą, do której kieruje wolontariuszy*[283]. Jest to dla mnie tak ciekawe, ponieważ wskazany autor udziela tu odpowiedzi poprawnej, że umowy powierzenia zawierać nie należy, uzasadnia ją jednak w ten sposób, że umowy powierzenia się w tej sytuacji nie zawiera ponieważ *to szkoła ustala cele i zadania*[284] wolontariuszy. Problem polega na tym, że o ile bieżące zadania rzeczywiście ustala szkoła, to przecież cel wolontariatu ustala ośrodek pomocy społecznej, celem tym jest na przykład włączenie społeczne osób wykluczonych. Dalej wskazany autor, omawiając cytowany przykład, błądzi nieco[285] po okolicach art. 28 RODO by w końcu uniknąć zajęcia stanowiska w sprawie, wycofując się z tego, które zajął słowami, że po to by *jednoznacznie odpowiedzieć na pytanie, trzeba zatem określić, który z podmiotów (OPS czy szkoła) samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych* [286]. Oczywiście i w opisanym przykładzie powierzenie nie ma miejsca, ponieważ wolontariat nie jest czynnością na danych.

Pochylenie się nad wskazanymi przykładami i analiza rozważań cytowanych autorów, zwłaszcza M. Bochenka doprowadziła mnie do ciekawego znaleziska. Autor ten (w ogniu omawiania przykładu o wolontariacie w szkole) pisze: *Artykuł 28 RODO nie definiuje pojęcia powierzenia przetwarzania danych, choć zawiera warunki jego skuteczności*[287]. Z cytatu tego wnoszę, że M. Bochenek nie rozumie, że

[281] M. Bochenek, *loc. cit.*

[282] M. Bochenek, *loc. cit.*

[283] M. Bochenek, *loc. cit.*

[284] M. Bochenek, *loc. cit.*

[285] M. Bochenek, *loc. cit.*

[286] M. Bochenek, *loc. cit.*

[287] M. Bochenek, *loc. cit.*

umowa powierzenia przetwarzania nie ustanawia tej relacji, czyli, że nie rozumie on definicji z art. 4 pkt 8 RODO. Definicji, z której wynika, że powierzenie jest albo go nie ma i że o ile umowa powierzenia przetwarzania danych osobowych jest obowiązkiem kiedy powierzenie jest, o tyle kiedy go nie ma, to umowa ta niewiele znaczy. Głównie ze wskazanego tu prawdopodobnego braku zrozumienia wynikają, jak mniemam, poglądy M. Bochenka.

Najbardziej niezawodną wydaje się być metoda oparta na tym czy administrator (danych) zleca czynność na danych czy inną czynność, do której wykonania dane są niezbędne. *3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie przetwarzania jako zlecenie czynności na danych osobowych*. Niestety i tu może pojawić się wynik fałszywie pozytywny. Ma to miejsce, kiedy administrator zleca czynność na danych, co pozornie czyni zleceniobiorcę podmiotem przetwarzającym. Zleceniobiorca nie jest jednak podmiotem przetwarzającym a nowym administratorem, kiedy wykonuje czynność na danych, jednak w imieniu własnym, nie zaś w imieniu administratora danych.

Przykładem może być tu wykonanie badania tomograficznego w podmiocie zewnętrznym wobec zleceniodawcy. Zleceniobiorca wykonuje badanie, podczas wykonywania zlecenia mają miejsce dwie grupy czynności:

pierwsza – wykonanie czynności technicznych, poinformowanie pacjenta o skutkach, przygotowanie pacjenta do badania – przetwarzanie danych osobowych w ogóle nie ma tu miejsca,

druga – zbieranie wyników badania, przechowywanie wyników badania, udostępnianie wyników badania podmiotowi zlecającemu badanie. Są to czynności na danych osobowych, jednak wykonywane nie są one wykonywane w imieniu zleceniodawcy a są one wykonywane w imieniu zleceniobiorcy. Mimo, że są to czynności na danych, to są one wykonywane w imieniu zleceniobiorcy, więc zleceniobiorca jest administratorem danych.

O tym, że czynności są wykonywane w opisanym stanie faktycznym, w imieniu zleceniobiorcy, wiemy z Kroku 2 niniejszej metody etapowej. Skutkiem opisanych tu ustaleń jest Krok 5 i Krok 6. Krok 5 i Krok 6 stanowią dwie wersje tego samego etapu.

Krok 6.
Czy administrator zleca wykonanie czynności na danych w swoim czyli zleceniodawcy czyli administratora imieniu?
Jeżeli administrator zleca wykonanie czynności na danych w swoim czyli zleceniodawcy czyli administratora imieniu, to zleceniobiorca jest podmiotem przetwarzającym.
Jeżeli administrator zleca wykonanie czynności na danych w imieniu zleceniobiorcy, to zleceniobiorca jest administratorem danych (odbiorcą).
Innymi słowy,
twierdząca odpowiedź na pytanie skutkuje wynikiem pozytywnym, który wydaje się być wiarygodny,
przecząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który wydaje się być wiarygodny.

Krok 7.
Czy administrator zleca wykonanie czynności na danych w imieniu zleceniobiorcy?
Jeżeli administrator zleca wykonanie czynności na danych w imieniu zleceniobiorcy, to zleceniobiorca jest administratorem danych (odbiorcą).
Jeżeli administrator zleca wykonanie czynności na danych w swoim czyli zleceniodawcy czyli administratora imieniu, to zleceniobiorca jest podmiotem przetwarzającym.
Innymi słowy,
twierdząca odpowiedź na pytanie skutkuje wynikiem pozytywnym, który wydaje się być wiarygodny,
przecząca odpowiedź na pytanie skutkuje wynikiem negatywnym, który wydaje się być wiarygodny.

Zwracam uwagę, że stosując proponowanej etapowej metodzie ustalania czy podmiot jest administratorem danych czy podmiotem przetwarzającym, trzeba zachowywać ostrożność. Właściwie dopiero Krok 6 i Krok 7 dają wynik, który jest na tyle wiarygodny, ze można go przyjąć jako ostateczny. Uważam, że również Krok 3 daje wiarygodny wynik.

Na metodę krokową można spojrzeć jako na metodę pozwalającą na sformułowanie zwrotu stosunkowego, czyli wypowiedzi o zgodności z przepisem.[288]

3.10. Art. 4 pkt 8. Uwaga 10. Realizacja art. 13 RODO i art. 14 RODO i art. 15 RODO przez podmiot przetwarzający

Uważam, że należy poczynić kilka uwag dotyczących realizacji art. 13 RODO, art. 14 RODO i art. 15 RODO. Zwracam uwagę, że obowiązki wynikające z tych przepisów spoczywają na administratorze danych. Stanowi to zasadę ogólną, może się jednak zdarzyć, że obowiązki realizować będzie podmiot przetwarzający. Niżej omawiam kilka modelowych sytuacji.

Administrator danych zbiera dane osobowe od osoby, której dane dotyczą – obowiązek informowania wynikający z art. 13 RODO spoczywa na administratorze.

Administrator danych pozyskuje dane osobowe nie od osoby, której dane dotyczą – obowiązek informowania wynikający z art. 14 RODO spoczywa na administratorze.

Podmiot przetwarzający w imieniu administratora danych zbiera dane osobowe od osoby, której dane dotyczą – obowiązek informowania wynikający z art. 13 RODO spoczywa na administratorze, jednak najprawdopodobniej realizować ten obowiązek będzie podmiot przetwarzający, ponieważ podawanie informacji wynikających z art. 13 RODO ma się odbywać podczas pozyskiwania tych informacji. Dane osobowe pozyskuje podmiot przetwarzający, więc oczywiste się wydaje, że i podmiot przetwarzający będzie udostępniał informacje wynikające z art. 13 RODO. Możliwe jest oczywiście, że dane osobowe pozyskuje podmiot przetwarzający i jednocześnie w trakcie tego pozyskiwania, administrator danych realizuje osobiście art. 13 RODO. Możliwe jest też, że dane osobowe pozyskuje podmiot przetwarzający i jednocześnie informacje wynikające z art. 13 RODO zostały danej osobie udostępnione wcześniej przez administratora danych. Osoba te informacje posiada, zatem nie udostępnia ich już nikt.

[288] J. Wróblewski, *Zwroty stosunkowe – wypowiedzi o zgodności z normą.* w: J. Wróblewski *Pisma wybrane.* Wybór i wstęp: M. Zirk-Sadowski, Warszawa 2015, s. 100.

Podmiot przetwarzający w imieniu administratora danych zbiera dane osobowe nie od osoby, której dane dotyczą – obowiązek informowania wynikający z art. 14 RODO spoczywa na administratorze. Artykuł 14 ust. 3 RODO ustanawia terminy i warunki ujawniania osobie, której dane dotyczą, informacji o szczegółach przetwarzania danych. Obowiązek ujawniania informacji z art. 14 ust. 1 RODO i z art. 14 ust. 2 RODO spoczywa na administratorze danych, jednak nic nie stoi na przeszkodzie by obowiązek ten był realizowany przez podmiot przetwarzający. Możliwe jest też, że dane osobowe pozyskuje podmiot przetwarzający i jednocześnie informacje wynikające z art. 14 RODO zostały danej osobie udostępnione wcześniej przez administratora (danych). Osoba te informacje posiada, zatem nie udostępnia ich już nikt.

Podobnie sytuacja wygląda jeśli chodzi o realizację obowiązków wynikających z art. 15 RODO, z art. 16 RODO, z art. 17 RODO, z art. 18 RODO, z art. 19 RODO i z art. 20 RODO. Obowiązki wynikające ze wskazanych przepisów spoczywają na administratorze danych, jednak administrator danych może umownie zobowiązać inne podmioty lub osoby do realizacji tych obowiązków.

3.11. Art. 4 pkt 8. Uwaga 11. Przykładowi odbiorcy, administratorzy danych, nie podmioty przetwarzające

Dla zilustrowania prowadzonych powyżej wywodów zamieszczam poniżej przykładowe podmioty, które są administratorami danych i nie są podmiotami przetwarzającymi.

Bank

Administrator, odbiorca, nie podmiot przetwarzający.

Bank przetwarza dane osobowe w oparciu o przepisy sektorowe.

Błądzi M. Bochenek, który twierdzi[289], że jeżeli MOPS wypłaca świadczenia za pośrednictwem banku, to MOPS powinien z bankiem podpisać umowę powierzenia i bank w takiej sytuacji jest podmiotem przetwarzającym. Co ciekawe, wskazany autor nie raz ale dwa razy[290]

[289] M. Bochenek, *loc. cit.*

[290] M Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach. Czy OPS powinien zawrzeć z bankiem umowę o powierzenie prze-*

zaleca zawierać umowę powierzenia z bankiem – błądzi za każdym razem. Między MOPSem a bankiem zachodzi relacja administrator-administrator.

Podmiot świadczący usługę medycyny pracy

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa medycyny pracy nie jest czynnością na danych osobowych. Poza tym podmiot świadczący te usługę, świadczy ja w swoim imieniu, fabryka np. młotków nie może świadczyć sama sobie czynności z zakresu medycyny pracy, zatem jeśli są one dla niej świadczone, to w imieniu zleceniobiorcy, nie w imieniu fabryki. Podobne rozumowanie prezentuje P. Dawidczyk .[291]

Ponadto podmiot świadczący usługę medycyny pracy wykonuje ja w sposób opisany w przepisach. Stanowisko, zgodnie z którym podmiot taki jest administratorem prezentuje[292], ku mojej zawodowej radości, PUODO.

Adwokat, radca prawny.

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa adwokacka nie jest czynnością na danych osobowych. Usługa taka to (upraszczając) doradztwo i reprezentowanie, nie są to czynności na danych osobowych. Zlecenie takiej usługi nie jest zleceniem czynności na danych osobowych w imieniu zleceniodawcy.
Ponadto adwokat wykonuje usługę w sposób opisany w przepisach.

Z uwagi na różne formy wykonywania zawodu radcy prawnego, należy zwrócić uwagę, że radca prawny, który jest zatrudniony jako pracownik administratora lub działa co prawda na zlecenie ale w ramach struktury organizacyjnej administratora, nie jest podmiotem przetwarzającym ani administratorem, ale po prostu osoba, która administrator powinien traktować jak pozostałych pracowników.[293]

---

twarzania danych osobowych osób, których dane przekazuje w celu wypłaty przyznanych tym osobom świadczeń, Warszawa 2019. Lex.

[291] P. Dawidczyk, *Umowy z jednostkami medycyny pracy.* ABIEXPERT nr 4(9) 2018. s. 24-25.

[292] *Ochrona danych osobowych w miejscu pracy Poradnik dla pracodawców. Poradnik RODO.* Październik 2018. s. 28-29.

[293] Por. *Poradnik dla radców prawnych i adwokatów. Ogólne rozporządzenie o ochronie danych (RODO),* X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka, s. 29.

Kancelaria prawna[294]

Odbiorca, administrator, nie podmiot przetwarzający.

Adwokat, radca prawny, doradca podatkowy są administratorami.

Wymienieni przetwarzają dane osobowe w swoim imieniu, w sposób wynikający z przepisów zawodowych.

Zlecenie usługi wymienionych podmiotów/osób nie jest zleceniem czynności na danych.

Należy tu odróżnić świadczenie usługi adwokackiej czy radcowskiej, od sytuacji kiedy człowiek, który jest adwokatem, radcą prawnym, doradcą podatkowym, wykonuje inną funkcję i jej wykonywanie odbywa się w warunkach powierzenia, choć trudno jest tu o przykład. Przykładem, który znam jest prowadzenie przedsiębiorstwa zajmującego się usługami księgowymi i kadrowymi przez doradcę podatkowego (przykład nieidealny, ale autentyczny i pasujący). Uważam, że sytuacja ta nie zachodzi kiedy adwokat, radca prawny, doradca podatkowy wykonuje czynności doradcze n. p. przy procedurze związanej z udzieleniem zamówienia publicznego. Uważam, że adwokat/radca/doradca podatkowy powinni być tu traktowani jak pracownicy, uważam, ze zjawisko przetwarzania danych osobowych w imieniu administratora w takiej sytuacji nie zachodzi, choć przyznam, że spotkałem się też[295] z poglądem przeciwnym, który jednak uważam za mylny, z przyczyn opisanych wyżej. Poglądu tego nie mogę udokumentować inaczej niż tylko wskazując w przypisie, że pogląd taki wygłosił przy okazji którejś z publicznych dyskusji, częściowo anonimowy internauta. Źródła tego typu zdecydowałem się umieścić w kilku miejscach publikacji a to z dwóch powodów, skoro nie są to moje poglądy, to nie widzę powodu by je sobie przypisywać, skoro są to poglądy spotykane, to warto je wskazać. Ponadto uważam, że korzystanie z nieuporządkowanych naukowo, ale jednak istniejących poglądów praktyków ma przymiot swoistych badań podstawowych.

Podczas zainicjowanej przeze mnie fejsbukowej dyskusji, ciekawy pogląd zaprezentował T. Izydorczyk, który stwierdził, że: *czynność doradcza może być wykonana bez danych osobowych.* Doradza-

[294] Pytanie internauty o nicku FB - Tomuś Thomas.

[295] Pogląd internauty o nicku FB - Tomuś Thomas.

jący zna personalia osoby, której doradza, nie zna jednak personaliów innych osób np. klientów osoby, której doradza. Tomasz Izydorczyk zwrócił przy tym uwagę na fakt, że jego uwaga nie dotyczy zawodów adwokata i radcy prawnego, którzy muszą badać zawsze konflikt interesów.[296]

Świadczenie usług doradztwa prawnego

Administrator, odbiorca, nie podmiot przetwarzający.

Pozycję tak zatytułowaną umieścił[297] w swojej książce L. Kępa, jako podmiot, z którym należy zawierać umowę powierzenia przetwarzania danych osobowych. By zrozumieć, że jest to błędem wystarczy uświadomić sobie czy świadczenie usług doradztwa prawnego jest czynnością na danych osobowych. Oczywiście nie jest. Zlecenie usługi doradztwa prawnego nie jest zatem zleceniem wykonania czynności na danych osobowych (w imieniu administratora-zleceniodawcy), zatem o powierzeniu nie może tu być mowy.

Doradca podatkowy[298]

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa doradztwa podatkowego nie jest czynnością na danych osobowych. Usługa doradztwa podatkowego to (upraszczając) doradztwo i reprezentowanie, nie są to czynności na danych osobowych. Zlecenie usługi doradztwa podatkowego nie jest zleceniem czynności na danych osobowych.

Ponadto doradca podatkowy wykonuje usługę w sposób opisany w przepisach.

Biegły rewident

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa świadczona przez biegłego rewidenta nie jest czynnością na danych osobowych. Zlecenie usługi świadczonej przez biegłego rewidenta nie jest zleceniem czynności na danych osobowych.

---

[296] Słowa od: *czynność doradcza* do: *konflikt interesów* to zredagowana przeze mnie wypowiedź T. Izydorczyka, z którym miałem przyjemność w okolicy r. 2019 dyskutować publicznie w grupie dyskusyjnej w ramach portalu Facebook.

[297] L. Kępa, *Ochrona danych osobowych w praktyce.* Warszawa 2014. s. 151.

[298] Problem: (doradca podatkowy jako ADO), (biuro rachunkowe jako?), (biegły rewident jako?) został postawiony przez internautę, B. Gibułę.

Ponadto biegły rewident wykonuje usługę w sposób opisany w przepisach.

Przedsiębiorstwo szkoleniowe („Firma" szkoleniowa[299])

Odbiorca, administrator, nie podmiot przetwarzający.

Jest administratorem, usługa szkoleniowa nie jest czynnością na danych osobowych.

Jest administratorem, odbiorcą, ponieważ zlecenie szkolenie nie jest zleceniem czynności na danych osobowych. Podczas szkolenia mają miejsce czynności na danych, np. wystawienie zaświadczeń, odnotowanie obecności słuchaczy, ale to są czynności, które zleceniobiorca wykonuje we własnym imieniu w celu wykonania umowy o realizację szkolenia.

Niezwykłe, rzeczy a ten temat pisze PUODO. Zrazu PUODO wdaje się w rozważania o dystrybuowaniu formularzy z ofertą szkoleń wśród pracowników. PUODO przedkłada, że jeżeli formularze owe, wypełniane następnie przez pracowników, dystrybuuje firma szkoleniowa, to firma ta jest administratorem,[300] dalej PUODO przedkłada: „jeżeli pracodawca zajmie się rozdysponowaniem ww. formularzy do pracowników i następnie uzupełnione formularze odbierze od nich (by je przekazać firmie szkoleniowej) wówczas firma szkoleniowa będzie musiała zawrzeć z tym pracodawcą umowę powierzenia przetwarzania danych osobowych pracowników." [301]. Z poglądami tymi się zgadzam, pracodawca zbiera tu informacje o potrzebach szkoleniowych pracowników w imieniu firmy szkoleniowej, zwracam jednak przy tym uwagę na fakt, że dystrybucja formularzy nie stanowi istoty usługi szkoleniowej. Dalej PUODO pisze: *Jeżeli firma szkoleniowa zewnętrzna będzie podmiotem, któremu pracodawca powierzy przetwarzanie danych osobowych, wówczas będzie musiała spełnić obowiązki spoczywające na takim podmiocie oraz zawarte w umowie powierzenia*[302] – i tu rodzi się problem, PUODO nijak nie wyjaśnia skąd, dlaczego, po co, na jakiej podstawie – pojawia się tu mowa o umowie powierzenia. Z PUODO się nie zgadzam, z uwagi na brak argumen-

[299] Problem postawiła internautka B. Matczyńska w grupie fejsbukowej.

[300] *Ochrona danych osobowych w miejscu pracy Poradnik dla pracodawców. Poradnik RODO,* Październik 2018. s. 30.

[301] *Loc. cit.*

[302] *Loc. cit*.

tów po stronie PUODO, nie widzę możliwości polemiki, swój pogląd w przedmiotowej kwestii wyraziłem wyżej.

Mogę tylko powtórzyć tezy, podsumowując poniżej.

- Usługa szkoleniowa nie jest usługą na danych osobowych.
- Usługa szkoleniowa nie jest usługa na danych osobowych w imieniu administratora.
- Przedsiębiorstwo szkoleniowe przetwarza zwykle dane osobowe osób szkolonych, na przykład w celu wystawienia tzw. certyfikatów uczestnictwa w szkoleniu, jednak:
-- zleceniodawca, który zleca szkolenie, nie zleca wystawienia certyfikatów, czy zleca przetwarzania danych osobowych w swoim (zleceniodawcy) imieniu, wystawienie certyfikatów to czynność związana ze szkoleniem, której jednak zleceniodawca nie zleca.
-- Czynność taka jak wystawienie certyfikatów mieści w sobie element przetwarzania danych osobowych, jednak podkreślenia wymaga, że nie jest to przetwarzanie w imieniu zleceniodawcy, ale że jest to przetwarzanie danych osobowych w imieniu zleceniobiorcy.

Tytułem uzupełnienia dodam, że można próbować wywodzić, że umowie szkoleniowej (bez umowy powierzenia przetwarzania danych osobowych) towarzyszy czasem umowa powierzenia przetwarzania danych osobowych związana właśnie np. z weryfikacją obecności pracowników. Uważam, że jest to niepotrzebne komplikowanie relacji, uważam, że dopuszczalne jest by uznać, że sprawdzenie obecności jest elementem usługi szkoleniowej, nie zaś osobną, zlecaną firmie szkoleniowej czynnością na danych osobowych w imieniu administratora - zleceniodawcy.

Przedsiębiorstwo szkolące z zakresu BHP [303]

Uważam, że jest tu analogicznie jak z przedsiębiorstwem szkolącym z jakiegokolwiek innego zakresu.

Jest administratorem, usługa szkoleniowa BHP nie jest usługą na danych.

Jest administratorem ponieważ zlecenie usługi szkoleniowej BHP nie jest zleceniem czynności na danych osobowych.

[303] Problem postawiła internautka B. Matczyńska w grupie fejsbukowej.

W związku ze świadczeniem usługi szkoleniowej BHP mają miejsce czynności na danych, np. wystawienie zaświadczeń, sporządzenie listy obecności, przeprowadzenie egzaminów. Uważam, że są czynności, które zleceniobiorca wykonuje we własnym imieniu w celu wykonania umowy szkoleniowe BHP.

Można próbować wywodzić, że umowie szkoleniowej BHP (bez umowy powierzenia) towarzyszy czasem umowa powierzenia związana właśnie np. z weryfikacją obecności pracowników. Nie jestem w stanie podać źródła, ale jest to pogląd zasłyszany. Uważam, że jest to niepotrzebne komplikowanie relacji, uważam, że dopuszczalne jest by uznać, że sprawdzenie obecności jest elementem usługi szkoleniowej BHP.

Nie sposób zgodzić się tu z poglądem wyrażonym przez Ministerstwo Cyfryzacji w poradniku „RODO dla administracji". Poradnik ten ma postać pytań i odpowiedzi. Pytanie brzmi: „Czy z firmą prowadzącą szkolenia BHP należy zawrzeć umowę powierzenia?". Cytuję dalej słowa, są bowiem dowodem na brak zrozumienia zjawiska powierzenia przetwarzania danych przez anonimowych niestety autorów poradnika.[304] „W sytuacji, gdy zadania służby BHP powierzono specjalistom spoza zakładu pracy np. firmie zewnętrznej, administrator zobligowany jest do zawarcia umowy powierzenia danych osobowych. Umowa taka nakłada na podmiot, któremu dane powierzono do przetwarzania, obowiązek odpowiedniego zabezpieczenia danych, zgodnie z wytycznymi, zawartymi w RODO.". Prawdą jest, że specjalista BHP powinien chronić dane zgodnie z RODO, to jest oczywiste, jednak czynności specjalisty BHP nie są czynnościami na danych osobowych. Pracodawca powierza czynności z zakresu BHP zewnętrznemu wobec pracodawcy podmiotowi. Podmiot wykonuje te czynności na pewno dla pracodawcy, na pewno na zlecenie pracodawcy, być może nawet w imieniu pracodawcy, ale nie są to czynności na danych. Są to głownie czynności szkoleniowe, którym czynności na danych jedynie towarzyszą.

[304] *RODO dla administracji*. Ministerstwo Cyfryzacji Styczeń 2019. Projekt: Wydział Komunikacji, Ministerstwo Cyfryzacji. Ministrem w czasie wydania poradnika był M. Zagórski. Poradnik dostępny ze strony: https://www.gov.pl/web/finanse/poradnik-rodo-dla-administracji. (dostęp: 11.09.2019 godz. 1.19)

Usługi hotelarskie[305]

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa hotelowa (wynajem pokoi umeblowanych) nie jest czynnością na danych w imieniu administratora (zleceniodawcy). Więcej - usługa hotelowa w ogóle nie jest czynnością na danych. Dane osobowe występują w kontekście wykonywania usługi hotelowej (dane gościa hotelowego), jednak są to dane konieczne do realizacji usługi, jeżeli ktoś – pracodawca zleca wykonanie usługi hotelowej wobec swoich pracowników, to zleca wykonanie usługi hotelowej właśnie, a nie zleca przetwarzania danych osobowych w swoim (zleceniodawcy) imieniu przez hotel.

Urząd pracy przy pracach interwencyjnych lub stażu[306]

Urząd pracy jest administratorem danych tych osób jako osób kierowanych do pracy lub na staż.

Pracodawca również jest administratorem danych.

Urząd pracy udostępnia pracodawcy dane pracownika lub stażysty.

Powierzenie nie zachodzi również dlatego, że prace interwencyjne lub staż nie są czynnościami na danych wykonywanymi w imieniu administratora.

Pracodawca wobec danych studenta na praktykach zawodowych[307]

Odbiorca, administrator, nie podmiot przetwarzający[308].

Uważam, że pracodawca jest administratorem, z tej prostej przyczyny, że praktyki zawodowe nie są czynnością na danych. Niezależnie od istoty relacji miedzy uczelnią a pracodawcą (odpłatna, bezpłatna, umowa, porozumienie), to w relacji tej nie zachodzi powierzenie, ponieważ przedmiotem umowy nie jest czynność na danych.

---

[305] Problem postawiony przez internautę o nicku FB - Tomuś Thomas.

[306] Problem postawiony przez internautkę E. Dąbrowicz w grupie fejsbukowej.

[307] Problem postawiony przez internautkę E. Dąbrowicz w grupie fejsbukowej.

[308] Odmiennie uważa S. Kryczka, że jednak poglądu swego przekonująco nie uzasadnia, to nie widzę możliwości polemiki, fakt istnienia poglądu przeciwnego do mojego odnotowuję jedynie w przypisie. S. Kryczka. *Praktyki studenckie - powierzenie czy udostępnienie danych.* OCHRONA DANYCH OSOBOWYCH. LIPIEC 2019 NR 65. s. 21.

Uważam, że nie ma tu znaczenia, czy uczelnia przysłała praktykanta czy ów sam znalazł pracodawcę.

Organizator wycieczki szkolnej - biuro podróży

Odbiorca, administrator, nie podmiot przetwarzający.

Zlecenie organizacji wycieczki nie jest zleceniem czynności na danych osobowych.

Organizacja wycieczki szkolnej nie jest czynnością na danych osobowych. Czynności na danych wykonywane przy okazji organizacji wycieczki to czynności wykonywane przez administratora danych, w swoim imieniu w celu realizacji umowy zlecenia wycieczki.

Linie lotnicze[309]

Odbiorca, administrator, nie podmiot przetwarzający.

Lot samolotem, transport ludzi lub ładunku nie jest czynnością na danych.

Na marginesie zwracam uwagę, że linie lotnicze są administratorem (odbiorcą) zarówno kiedy usługę zleca np. pracodawca dla pracownika w podróży służbowej, osoba fizyczna – po prostu podróżując, jak i w sytuacji kiedy usługę przelotu zleca biuro podróży. W sytuacji kiedy usługę przelotu zleca biuro podróży, to zarówno biuro podróży jak i linie lotnicze, są administratorami.

Przedsiębiorstwo taksówkowe dla danych klientów - zleceniodawców usługi przewozu, danych osób wożonych (nie zawsze ta sama osoba).[310]

Jest administratorem, usługa przewozu nie jest czynnością na danych osobowych w imieniu administratora ponieważ w ogóle nie jest czynnością na danych osobowych.

Jest administratorem ponieważ zlecenie usługi przewozu nie jest zleceniem czynności na danych osobowych.

W związku ze świadczeniem usługi przewozu mają miejsce czynności na danych, np. wystawienie faktury, odnotowanie adresu czy nazwiska klienta (pomijam czy do zbioru, by nie komplikować,

[309] Problem postawił internauta R. M. Walewski w grupie fejsbukowej.

[310] Problem postawił internauta R. M. Walewski w grupie fejsbukowej.

załóżmy, że tak), ale to są czynności, które zleceniobiorca wykonuje we własnym imieniu w celu wykonania umowy przewozu taksówką.

Podmiot medyczny
sprawujący opiekę nad pracownikiem w „pakiecie medycznym"

Jest administratorem.

Zlecenie opieki medycznej nad pracownikami nie jest zleceniem czynności na danych.

Poza tym podmiot leczniczy ma własne cele wynikające z aktów prawnych.

W sprawie wypowiedział się, w poprzednim stanie prawnym L. Kępa. Autor ten uniknął rozstrzygania kwestii: administrator/podmiot przetwarzający, stwierdził jednak, że dane o pracowniku podlegają przekazaniu. Wydaje się, że można to utożsamić z udostępnieniem, acz mam świadomość, że być może nadinterpretuję słowa L. Kępy, acz czynię to w kierunku aprobatywnym. Autor ten zwrócił uwagę na to, że GIODO w swoim sprawozdaniu za rok 2005 uznał, cytuję L. Kępę, że: *Sama umowa między pracodawca a podmiotem świadczącym usługi medyczne nie stanowi podstawy do przekazania danych o pracowniku* (tu przypis L. Kępy do sprawozdania GIODO) *musi on wyrazić na to zgodę*.[311]

Przedsiębiorstwo ubezpieczeniowe,
na przykład przy ubezpieczeniach grupowych pracowników ADO

Jest administratorem.

Ma własne cele wynikające z ustawy.

Umowa, na mocy której pracodawca ubezpiecza pracowników nie jest umową zlecenia czynności na danych.

Agent ubezpieczeniowy

Podmiot przetwarzający.

Po zakończeniu umowy, która łączy agenta ubezpieczeniowego z przedsiębiorstwem ubezpieczeniowym, agent powinien zwrócić wszystkie dane przedsiębiorstwu ubezpieczeniowemu.

Leszek Kępa dostrzega[312] problem w tym, że agent sprzedaje ubezpieczenia również swoim znajomym zatem na przykład danych

[311] L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 83.

[312] L. Kępa, *op. cit.* s. 106.

kontaktowych swoich prywatnych znajomych, nie zwróci przedsiębiorstwu ubezpieczeniowemu. Ja tu problemu nie dostrzegam. Agent zwróci dane przetwarzane w imieniu przedsiębiorstwa ubezpieczeniowego, a prywatnie przetwarzane dane kontaktowe – zachowa, wskazany autor zwraca uwagę na to, że agent przetwarza niezwrócone dane swoich znajomych, w celach osobistych, z czym się zgadzam, żadnej sensacji w zjawisku jednak nie dostrzegam, zjawisko to nie modyfikuje relacji powierzenia, jest wobec niej równoległe.

Widzę możliwość oparcia relacji ochrony danych miedzy agentem ubezpieczeniowym a przedsiębiorstwem ubezpieczeniowym, również w oparciu o model upoważnienia nie powierzenia. Nieco wbrew sobie, bo wbrew definicji podmiotu przetwarzającego, uważam, że duże znaczenie mają tu kwestie logistyki bezpieczeństwa. Jeżeli agent ubezpieczeniowy działa w oparciu o „własne bezpieczeństwo", to przedsiębiorstwo ubezpieczeniowe powinno z nim podpisać umowę powierzenia przetwarzania, jeżeli jednak agent ubezpieczeniowy działa w oparciu o bezpieczeństwo przedsiębiorstwa ubezpieczeniowego (służbowy laptop, telefon, może lokal), to umowa powierzenia przetwarzania nie ma sensu, bo o kwestiach bezpieczeństwa i tak decyduje tylko jedna ze stron.

Broker ubezpieczeniowy[313]

Odbiorca, administrator, nie podmiot przetwarzający.

Dochodzimy do tego w sposób dalej opisany, otóż agent ubezpieczeniowy działa na rzecz zakładu ubezpieczeń. Broker ubezpieczeniowy działa na rzecz i w imieniu klienta, czyli osoby chcącej zawrzeć ubezpieczenie.

Broker jest administratorem, nie podmiotem przetwarzającym. Celem brokera jest pośrednictwo ubezpieczeniowe, czyli (nieco upraszczając) zawarcie umowy ubezpieczenia, ale w imieniu klienta, podmiotu ubezpieczanego. Odróżnia go to od agenta, którego celem jest zawarcie umowy w imieniu zakładu ubezpieczeń.

[313] Problem postawił internauta Tomuś Thomas w grupie fejsbukowej.

Podmioty medyczne, do których inny podmiot kieruje z wykorzystaniem skierowania (też laboratoria itp.) [314]

Podmioty te mają własne cele wynikające z przepisów.

Umowa miedzy podmiotem medycznym (wykonującym działalność leczniczą) a innym takim podmiotem nie jest umową zlecenia czynności na danych.

Można przyjąć, że każdy podmiot wykonujący działalność leczniczą jest osobnym administratorem. Tak samo relacja ze skierowaniem z podmiotu do podmiotu jest relacją administrator-administrator.

Nieco inaczej jest w badaniach klinicznych, tam bowiem nakładają się role. Piszę o tym w uwadze *3.13. Art. 4 pkt 8. Uwaga 13. Badania kliniczne. Role podmiotów na gruncie RODO*.

Związek zawodowy.

Odbiorca, administrator, nie podmiot przetwarzający.

Posiada własne cele wynikające z przepisów.

Główny Urząd Statystyczny, ZUS, SANEPID, Urząd Skarbowy

Odbiorca, administrator, nie podmiot przetwarzający.

Posiada własne cele wynikające z przepisów.

Przedsiębiorstwo kurierskie[315]

Odbiorca, administrator, nie podmiot przetwarzający.

„Firma kurierska" co do zasady jest administratorem.

Usługa kurierska nie jest czynnością na danych w imieniu administratora-zleceniodawcy.

Niewiele daje tu poszukiwanie odpowiedzi na drodze takiej, że administrator jest administratorem jeśli ma własny cel. Tu cel jest celem zleceniodawcy czyli administratora danych - dostarczenie towaru, ale dostarczenie towaru nie jest czynnością na danych, więc nie ma mowy o powierzeniu.

Możliwe jest też stanowisko, że cel jest celem zleceniobiorcy, ponieważ celem tym jest dostarczenie towaru – przesyłki, niezależnie od tego czyja ta przesyła jest, z poglądem tym raczej się nie zgadzam,

[314] Problem postawił internauta R. M. Walewski w grupie fejsbukowej.

[315] Problem postawił internauta M. Zach w grupie fejsbukowej.

w każdym razie pogląd ten nie zmienia mojego stanowiska w kwestii roli przedsiębiorstwa kurierskiego na gruncie RODO.

Czasem z usługą kurierską połączone są inne usługi np. odebranie oświadczenia na piśmie. Wtedy, ewentualnie można próbować wykazać, że jest to czynność na danych w imieniu administratora, więc zachodzi wtedy powierzenie przetwarzania, jednak ja tak nie uważam, są to bowiem dodatkowe elementy usługi kurierskiej.

Poczta Polska odnośnie danych adresatów[316]

Poczta jest administratorem wykonuje czynności wskazane w przepisach, które nawet jeśli są czynnościami na danych to nikt inny niż poczta ich wykonać nie może.

Są sytuacje, w których dodatkowo w przesyłce znajdują się inne dane osobowe niż dane adresatów i nadawców (np. listy płac, dokumentacja medyczna). Wobec takich danych poczta polska jest osobą trzecią poza sytuacjami kiedy musi przesyłkę otworzyć ponieważ np. poszukuje adresu, ponieważ np. przesyłka jest uszkodzona i trzeba ją zabezpieczyć, otworzyć bo przesyłka cieknie itp. Wtedy, jak uważam, poczta też jest administratorem.

Przedsiębiorstwo sprzątające[317]

Jest administratorem - tu nie ma powierzenia, nawet jeśli pracownicy przedsiębiorstwa sprzątającego zapoznają z danymi np. na drzwiach, to nie jest to przetwarzanie w imieniu ADO. (Można się zastanowić nad tym, czy przeczytanie danych na drzwiach przez pracownika sprzątającego mieści się w RODO, ale to zostawiam na boku by nie zaciemniać wywodu.)

Pracownik wypożyczony

Z art. 174^1 kodeksu pracy[318] wynika możliwość wypożyczenia pracownika. Wypożyczenie owo polega na tym, że za zgoda pracownika wyrażoną na piśmie, pracodawca udziela pracownikowi „urlopu bezpłatnego w celu wykonywania pracy u innego pracodawcy przez

[316] Problem postawił internauta M. Zach w grupie fejsbukowej.

[317] Problem postawił internauta o nicku Marek Be w grupie fejsbukowej.

[318] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy. Dz.U. 1974 nr 24 poz. 141 ze zm. t. j. dz. U. 2020 poz. 1320.

okres ustalony w zawartym w tej sprawie porozumieniu miedzy pracodawcami". Pracodawca, który wypożycza pracownika po to, żeby ten u niego pracował, jest po prostu nowym pracodawcą pracownika, tyle, że u starego pracodawcy pracownik przebywa na urlopie bezpłatnym, okres tego urlopu wlicza się wlicza się do okresu pracy u dotychczasowego pracodawcy.

Uważam, że nowy pracodawca jest administratorem danych osobowych pracownika.

Z uwagi na fakt, że okres pracy u nowego pracodawcy wlicza się do okresu pracy, od którego zależą uprawnienia pracownicze u starego pracodawcy, można by próbować wywodzić, że informacje dotyczące okresu pracy, nowy pracodawca przetwarza w imieniu dotychczasowego pracodawcy, jest zatem w tym zakresie, podmiotem przetwarzającym. Możliwość takiego poglądu sygnalizuję głównie po to, by zaznaczyć, że się z nim nie zgadzam. Nowy pracodawca jest administratorem danych pracownika wypożyczonego i jedynie informuje pracodawcę dotychczasowego o okresie pracy u siebie, tak by ten mógł doliczyć okres pracy u nowego pracodawcy do okresu pracy u pracodawcy dotychczasowego czyli u siebie. Teoretycznie informowanie to mogłoby nie zajść, ponieważ okres ten wynika z umowy między pracodawcami.[319]

Leszek Kępa zwraca uwagę, że pracownik wypożyczany jest po prostu pracownikiem, z tym, że zatrudnianym na czas określony.[320]

Anna Kosut zwraca uwagę na fakt, że nowy pracodawca ma te same obowiązki *(...) jakie zwykle ciążą na nim w związku z zatrudnieniem pracowników*,[321] co uważam za argument przemawiający za tym, że nowy przedsiębiorca jest administratorem danych.

[319] Szerzej: J. Iwulski w: K*omentarz do Kodeksu Pracy*. J. Iwulski, W. Sanetra, Warszawa 2009, s. 898.

[320] Podobnie: L. Kępa, *Ochrona danych osobowych w praktyce,* Warszawa 2014, s. 151.

[321] A. Kosut w: K. W. Baran. B.M. Ćwiertniak, S. Driczinski, Z. Góral, A. Kosut, D. Książek, M. Kuba, W. Perdeus, J. Piątkowski, P. Prusinowski, K. Stefański, M. Tomaszewska, M. Włodarczyk, T. Wyka. red. N. K. W. Baran, *Kodeks Pracy. Komentarz,* Warszawa 2018, s. 1111.

Pośrednik handlowy

Administrator danych.

Jeżeli przedsiębiorstwo A zleca przedsiębiorstwu B. sprzedaż towarów, to przedsiębiorstwo B ma własne obowiązki związane na przykład z wystawieniem faktur kupującym. W takim wypadku zleceniobiorca, czyli pośrednik, czyli przedsiębiorstwo B jest administratorem danych.

Leszek Kępa posłużył się pojęciem: „pośrednictwo w sprzedaży" i dodał, że „umowę powierzenia należy zawierać". Nie za bardzo mogę prowadzić polemikę, nie rozumiem bowiem intencji cytowanego autora. Może chodziło mu o zleceniobiorcę, który wiezie towar do kupującego, dostaje adres kupującego od zleceniodawcy, negocjuje w imieniu zleceniodawcy. Nie wiem, lecz jeśli o to chodziło L. Kępie, to rzeczywiście w takiej sytuacji należy zawrzeć umowę powierzenia przetwarzania i zleceniobiorca (pośrednik handlowy, pośrednik w sprzedaży) jest wtedy podmiotem przetwarzającym.

3.12. Art. 4 pkt 8. Uwaga 12.
Przykładowe podmioty przetwarzające.

Dla zilustrowania prowadzonych powyżej wywodów zamieszczam poniżej przykładowe podmioty, które są podmiotami przetwarzającymi.

Biuro rachunkowe

Podmiot przetwarzający.

Trafny jest pogląd, zgodnie z którym, biuro rachunkowe powinno podpisywać ze swoimi klientami umowy powierzenia przetwarzania danych osobowych.[322]

Ciekawą myśl wywiódł podczas dyskusji jeden z internautów[323], który stwierdził, że: *Istotą prowadzenia księgowości jest przetwarzanie danych finansowych, a nie osobowych*. Pogląd ten jest ciekawy, jednak nie powinien prowadzić do pochopnych wniosków. Biuro rachunkowe przetwarza dane z faktur wystawionych przez swoich klientów, są to zatem dane klientów ich klientów, dane podmiotów i osób, które zakupiły coś od klientów biura podatkowego.

[322] Podobnie, choć nie w sposób dosłowny: L. Kępa, *op. cit*. s. 108.

[323] Problem został postawiony przez internautę B. Gibułę.

Część tych danych to dane osobowe. Jeżeli na przykład osoba fizyczna zakupi coś od klienta biura podatkowego, to biuro podatkowe przetwarza następnie dane osobowe tej osoby fizycznej.

Przedsiębiorstwo świadczące usługę call center

Podmiot przetwarzający - jeżeli administrator przekazuje takiemu przedsiębiorstwu dane osobowe (numery telefonów, inne dane osobowe), aby przedsiębiorstwo to dzwonił do osób fizycznych w imieniu administratora.

Do grupy podmiotów przetwarzających zaliczył takie przedsiębiorstwo L. Kępa,[324] nie zwracając jednak jak się wydaje uwagi na fakt, że usługa call center **może być też** świadczona w taki sposób, że przedsiębiorstwo, które ją świadczy jest **administratorem danych**. Dzieje się tak wtedy kiedy zleceniodawca zleca wykonanie czynności call center wobec grupy osób, na przykład z jakiegoś terenu lub w jakimś wieku, przedsiębiorca podaje określone parametry osób należących do grupy docelowej, jednak dane osób należących do tej grupy posiada przedsiębiorca call center, który jest w takim wypadku administratorem tych danych.

Przedsiębiorstwo windykacyjne

Zasadą jest, że przedsiębiorstwo windykacyjne działa w imieniu wierzyciela. Jest wtedy podmiotem przetwarzającym.

Może się zdarzyć, że wierzyciel dokonuje cesji wierzytelności na rzecz przedsiębiorstwa windykacyjnego „sprzedaje dług". W takiej sytuacji przedsiębiorstwo windykacyjne przetwarza dane w swoim imieniu jest zatem administratorem danych. Podkreślam, że przedsiębiorstwo windykacyjne nie decyduje o tym czy jest administratorem czy podmiotem przetwarzającym, nie wybiera tego, decyduje o tym istota relacji między takim przedsiębiorstwem a wierzycielem.

Przedsiębiorstwo, na serwerze którego administrator prowadzi stronę internetową

Podmiot przetwarzający.

Leszek Kępa widzi rozróżnienie między outsourcingiem witryny www a hostingiem witryny www. Autor ten uważa, że w przy-

[324] L. Kępa, *op. cit*. s. 151.

padku outsourcingu zachodzi powierzenie a w przypadku hostingu powierzenie nie zachodzi.[325] Ja uważam, że powierzenie zachodzi w obu przypadkach – oczywiście o ile witryna zbiera lub udostępnia dane osobowe.

Przedsiębiorstwo prowadzące rejestrację pacjentów w warunkach outsourcingu, jako zleceniobiorca

Podmiot przetwarzający.

Cel przetwarzania jest celem szpitala, przychodni - zlecających rejestrację.

Przedsiębiorstwo zajmujące się niszczeniem dokumentacji

Podmiot przetwarzający.[326]

Dokumentacja, wszelka dokumentacja – dokumentacja medyczna, akta spraw, dokumentacja księgowa, nawet (zwykle) projekty architektoniczne – zawiera dane osobowe. Niszczenie dokumentacji jest zatem niszczeniem danych osobowych na zlecenie administratora danych.[327]

Przedsiębiorstwo zajmujące się przechowywaniem dokumentacji.

Podmiot przetwarzający.

Przechowywanie danych osobowych jest czynnością na danych. Przechowywanie rozumiane jako cel przetwarzania leży po stronie zleceniodawcy, jeżeli więc zleca on przechowywanie danych, to zleca czynność na danych.

Leszek Kępa użył pojęcia: *przechowywanie w archiwum dokumentów firmowych*[328]. Jeżeli realia są takie, że przedsiębiorstwo zleca komuś – archiwum państwowemu lub prywatnemu przechowawcy – przechowywanie dokumentów, to takie archiwum lub taki przechowawca są podmiotami przetwarzającymi, jeżeli jednak archiwum przechowuje dokumenty z uwagi na swoje obowiązki wynikające z Ustawy o Na-

[325] L. Kępa, *op. cit.* s. 120.

[326] Tak samo: L. Kępa, *op. cit.* s. 151.

[327] Podobnie: L. Kępa, *op. cit.* s. 115.

[328] L. Kępa, *op. cit.* s. 151.

rodowym zasobie archiwalnym i archiwach,[329] to archiwum takie jest administratorem, czego L. Kępa zdaje się nie zauważać.

Przedsiebiorstwo zajmujące się kopertowaniem i wysyłką korespondencji.

Podmiot przetwarzający.

Jest to przykład wskazany trafnie przez L. Kępę[330], zwracam jednak uwagę na to, że przykład ten jest trafny z uwagi na to, że częścią usługi jest „kopertowanie", czyli zapewne wkładanie korespondencji do zaadresowanych kopert lub wkładanie korespondencji i adresowanie kopert. W obu tych sytuacjach, zleceniobiorca musi dokonać analizy danych adresowych, czyli danych osobowych (chyba, że kopertowana jest korespondencja nie do osób fizycznych).

Jeśli chodzi o czynność wysyłania, to zależy co przez nią rozumiemy, ale jeżeli rozumiemy przez nią np. wypełnianie książek nadawczych, formularzy pocztowych itd., które to czynności związane są z wpisywaniem w różne miejsca danych osobowych (zwykle) adresatów, to takie wysyłanie powoduje, że wysyłający jest podmiotem przetwarzającym.

Pracownik tymczasowy.

Pracownik tymczasowy pojawia się na gruncie Ustawy o zatrudnianiu pracowników tymczasowych[331]. Relacja zachodzi tu między trzema podmiotami, agencją zatrudnienia, która zatrudnia pracownika, pracodawcą – użytkownikiem, u którego pracownik pracuje, ponieważ agencja pracodawcy – użytkownikowi wypożycza pracownika i oczywiście pracownik.

Agencja zatrudnienia jest administratorem danych pracownika, ona bowiem pracownika zatrudnia.

Pracodawca – użytkownik jest podmiotem przetwarzającym.[332]

---

[329] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Dz.U. 1983 nr 38 poz. 173. ze zm. t. j. Dz.U. 2020 poz. 164.

[330] L. Kępa, *loc. cit.*

[331] Ustawa z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych. Dz. U. 2003 nr 166 poz. 1608. ze zm. t.j. Dz. U. 2019 poz. 1563.

[332] Podobnie: L. Kępa, *op. cit*. s. 77.

3.12.a. Art. 4 pkt 8. Uwaga 12.a.
Przykładowe podmioty będące stronami trzecimi lub administratorami.

Możliwa jest sytuacja, w której podmiot, ze względów logistycznych, ma styczność z danymi osobowymi, które na przykład znajdują się w zamkniętym pokoju, do którego podmiot ten ma klucz, lub które znajdują się w zamkniętej paczce, która podmiot ten transportuje. Wtedy, wobec takich danych – danych w paczce, danych za ścianą – podmiot taki jest stroną trzecią.

Firma transportowa, lub kurierska, przewożąca dane w zamkniętych opakowaniach.

Administrator – wobec danych adresowych znajdujących się ewentualnie na opakowaniach.

Strona trzecia – wobec danych znajdujących się w opakowaniach.

Leszek Kępa pisze o transporcie *danych osobowych w zapieczętowanych przesyłkach przez firmę kurierską*[333] i zwraca uwagę na fakt, że „Firma ta nie przetwarza danych osobowych, bo nie wykonuje operacji bezpośrednio na danych, które transportuje”[334].

Przedsiębiorstwo sprzątające, które dostarcza również korespondencję. [335]

Odbywa się tu coś na kształt usługi gońca - np. sprzątaczka w bloku roznosi listy od zarządu wspólnoty. Uważam że w tym zakresie przedsiębiorstwo sprzątające jest podmiotem przetwarzającym.

Wobec danych osobowych, które znajdują się w zamkniętych opakowaniach, przedsiębiorstwo takie jest stroną trzecią.[336]

[333] L. Kępa, *op cit.* s. 146.

[334] L. Kępa, *loc cit.*

[335] Problem postawił internauta Marek Be w grupie FB.

[336] L. Kępa, *loc. cit.*

Przedsiębiorstwo ochroniarskie,
które dba o to by
osoby niepowołane nie dostały się do pomieszczeń

Jeżeli przedsiębiorstwo ochroniarskie, które dba o to by osoby niepowołane nie odstały się do pomieszczeń, po prostu tych pomieszczeń pilnuje, w pomieszczeniach tych są dane, jednak pracownicy przedsiębiorstwa ochroniarskiego do pomieszczeń nie wchodzą a nawet jeśli wejdą, to nie wolno im danych przetwarzać, to przedsiębiorstwo takie jest stroną trzecią.[337]

3.13. Art. 4 pkt 8. Uwaga 13.
Badania kliniczne. Role podmiotów na gruncie RODO

Podczas prowadzenie badań klinicznych występuje kilka podmiotów. Z punktu widzenia RODO pełnią one pewne role. Niżej wymieniam te podmioty, charakteryzuję je i wskazuję rolę pełnioną na gruncie RODO.[338]

Sponsor badania – jest administratorem (danych osobowych), bowiem ustala cele i sposoby przetwarzania danych osobowych. Cele i sposoby opisane są w protokole badania i w rozmaitych dokumentach stanowiących zwykle załączniki do tego protokołu lub dokumenty mu towarzyszące.

Pojawia się tu czasem krajowy przedstawiciel sponsora, np.: spółka córka - „Spółka X Polska" wobec spółki matki - „Spółka X z siedzibą np., w USA". Z punktu widzenia badania klinicznego pojawienie się takiego podmiotu nie jest kluczowe, badanie organizowane jest zwykle z ramienia spółki matki. Stosunki miedzy spółką matką a spółką córką to zwykle stosunki między dwoma administratorami, możliwe jest tu zjawisko współadministrowania, może się tu jednak zdarzyć również powierzenie przetwarzania, wszystko to

[337] L. Kępa, *loc .cit.*

[338] P. Więckowski wymienia więcej podmiotów, biorących udział w badaniu, czyni to trafnie, piszę tu o podmiotach takich jak: „Przedstawiciel Sponsora", „Podmioty powiązane ze sponsorem", „Zespół badawczy", „Uczestnik badania", „Opiekun prawny". (P. Więckowski. *Wpływ RODO na badania kliniczne.* ABI Expert 4(9). s. 33-35. Podmioty wskazane pomijam, nie są one bowiem istotne dla zagadnień tu poruszanych.

dotyczy już raczej nie badań klinicznych a przetwarzania danych osobowych w grupach kapitałowych.

Przedsiębiorstwo CRA / CRO. Poprawnie nazywając, przedsiębiorstwo monitorujące badanie to przedsiębiorstwo CRO czyli „contract research organization", zaś pracownik takiego przedsiębiorstwa to CRA czyli „clinical research associate". W swej pracy spotykałem się zwykle z określeniem „firma CRA", w znaczeniu przedsiębiorstwa zajmującego się monitorowaniem badań klinicznych. Przedsiębiorstwo takie jest podmiotem przetwarzającym dla którego sponsor badania jest administratorem danych. Oczywiście przedsiębiorstwo takie jest podmiotem przetwarzającym wobec danych pacjentów, którzy biorą udział w badaniu klinicznym, ale już na przykład wobec danych swoich pracowników, przedsiębiorstwo takie jest administratorem.
Badacz – kieruje „ośrodkiem badawczym", bywa określany głównym badaczem „main investigator". Z punktu widzenia danego badania klinicznego jest podmiotem przetwarzającym, wobec administratora, jakim jest sponsor badania, ale jednocześnie badacz pacjenta leczy, więc jest też administratorem.
Ośrodek badawczy, czyli miejsce, na terenie którego odbywa się badanie, może być to przychodnia, szpital, praktyka lekarska – podmiot wykonujący działalność leczniczą. Z punktu widzenia danego badania klinicznego jest podmiotem przetwarzającym, wobec administratora, jakim jest sponsor badania, ale jednocześnie wobec danych leczonego pacjenta jest też administratorem danych.

Jak widać zachodzi tu zjawisko nakładania się ról. Zjawisko nakładania się ról polega na tym, że jeden podmiot jest jednocześnie administratorem i podmiotem przetwarzającym. Jest to jeden z rodzajów wystąpienia zjawiska nakładania się ról. Drugi zachodzi wtedy, kiedy odbiorca jest jednocześnie administratorem.

Na marginesie trzeba zauważyć, że wyniki badań są przekazywane z ośrodka do sponsora w wersji spseudonimizowanej, ale są to dane osobowe. Są to dane osobowe, ponieważ dane spseudonimizowane to nadal dane osobowe. Ponadto sponsor ma dostęp do oryginałów dokumentacji badania, do dokumentacji źródłowej itd., ponieważ prowadzi nadzór nad badaniem, sprawdza kryteria włączenia do badania, kryteria wyłączenia z badania, zużycie leków etc. Sponsor

czyni to przez własnych pracowników lub przez przedsiębiorstwo „firmę" CRA/CRO, ale przedsiębiorstwo CRA/CRO jest podmiotem przetwarzającym dla sponsora, więc kiedy CRA monitoruje badanie to jest tak jakby sponsor monitorował.

Zadziwia stanowisko O. Zielińskiej, która pisze: *W praktyce sponsor badania lub podmioty prowadzące badania kliniczne na jego zlecenie (CRO) nie przetwarzają danych osobowych uczestników badania klinicznego*[339] – przyznam, że przeczytawszy ten fragment zdziwiłem się nieco, przy czym pierwszą myślą, była myśl dotycząca tego jak autorka uzasadni taki pogląd. Dalej wskazana autorka pisze: *Dane te są poddane pseudonimizacji, przez nadanie uczestnikom badania numerów lub liter*"[340] – przyznam, że tu zdziwiłem się jeszcze bardziej, z uwagi na fakt, że artykuł, który cytuję został wydrukowany w 2017 roku. Dalej jeszcze autorka pisze: *Zachodzi tutaj pewien dysonans, ponieważ pomimo obowiązku nałożonego na sponsora badania prawidłowości nadzorowanego przez siebie badania klinicznego nie ma on wglądu w dane osobowe uczestnika*[341] – tu widać, że autorka przyjęła błędne założenie, że *(...) sponsor badania lub podmioty prowadzące badania kliniczne na jego zlecenie (CRO) nie przetwarzają danych osobowych uczestników badania klinicznego*, po czym sama zaczęła się dziwić jak sponsor ma działać. Dalej autorka wykazuje się znajomością przepisów, siatki pojęciowej, chyba też praktyki. Następnie autorka pisze: *Zgodnie z "§ 10 ust. 1 Rozporządzenia w sprawie Dobrej Praktyki Klinicznej sponsor zapewnia monitorowanie badania klinicznego we wszystkich ośrodkach badawczych, w trakcie i po zakończeniu badania klinicznego. W ramach tego obowiązku monitorzy (z ramienia sponsora) i pracownicy podmiotu prowadzącego badania kliniczne na zlecenie (CRO) dokonują przeglądu dokumentacji badania klinicznego prowadzonej przez badacza i członków zespołu badawczego w danym ośrodku*[342] – w tym miejscu zdziwiłem się i zastanowiłem, czy autorka nie wie, że częścią dokumentacji badania klinicznego w ośrodku badawczym jest tzw. dokumentacja źródłowa, czyli (zwykle) kopie dokumentów medycznych

[339] O. Zielińska. Dane osobowe w badaniach klinicznych produktów leczniczych. ABI Expert 3(4) s. 53-56.

[340] O. Zielińska, *op. cit.*

[341] O. Zielińska, *op. cit.*

[342] O. Zielińska, *op. cit.*

dostarczonych przez pacjenta. Dokumenty te nie są spseudonimizowane, a ponieważ są (zwykle) fizycznie połączone z dokumentacją badania klinicznego, z dokumentacją poszczególnych pacjentów, to oczywiste jest, że jeżeli dokument źródłowy zawiera dane osobowe i włączony jest do dokumentacji pacjenta, to jest to ten sam pacjent, którego dotyczy dokument źródłowy. Na następnej stronie artykułu okazuje się jednak, że jego autorka jest świadoma istnienia dokumentów źródłowych , pisze ona bowiem: *Dokumentacja badania klinicznego zawiera dokumenty źródłowe, w tym formularze zgody na przetwarzanie danych osobowych uczestników badania. Osoby monitorujące badanie kliniczne uzyskują tym samym dostęp do danych osobowych uczestników* [343] – w tym momencie walczę z chęcią ponownego przeczytania wcześniejszych opowieści autorki, nijak bowiem stwierdzenie to ma się do wcześniejszego, że: *W praktyce sponsor badania lub podmioty prowadzące badania kliniczne na jego zlecenie (CRO) nie przetwarzają danych osobowych uczestników badania klinicznego*[344]. Od razu bowiem należy sobie postawić pytanie jak autorka widzi możliwość dostępu przy braku przetwarzania.

Cytowana autorka prawdopodobnie zauważyła niespójność swoich opowieści i zrobiła radykalny manewr pisząc: *Co istotne, monitorowanie badania klinicznego nie wymaga jednak utrwalania danych w żadnej formie, ani też tworzenia bazy danych. Należy zatem uznać, że przetwarzanie danych przez monitorów czy pracowników CRO w tym przypadku jest czynnością jedynie techniczną, wobec czego nie wymaga rejestracji zbioru przez GIODO*"[345].

Poświęciłem tyle miejsca artykułowi O. Zielińskiej, bowiem pisze ona w nim rzeczy przedziwne. Zdziwieniu swemu daje wyraz wyżej – cytując i omawiając tezy autorki. Odnoszę się poniżej do tez O. Zielińskiej przekształcając je w tezy prawdziwe, jednak z uwagi na owe przekształcenia nie zaznaczam tez tych cudzysłowami.

Po pierwsze, sponsor badania klinicznego lub podmioty prowadzące badanie kliniczne na jego zlecenie (CRO) przetwarzają dane osobowe uczestników badania klinicznego. Oczywiście od takiej tezy nie po-

[343] O. Zielińska, *op. cit.*

[344] O. Zielińska, *op. cit.*

[345] O. Zielińska, *op. cit.*

winno się zaczynać rozumowanie, taką powinno się ono kończyć, odnoszę jednak wrażenie, że O. Zielińska przyjęła swoją tezę (że *(...) sponsor badania lub podmioty prowadzące badania kliniczne na jego zlecenie (CRO) nie przetwarzają danych osobowych uczestników badania klinicznego*[346]) i dopasowała resztę rozważań do tej tezy. Błąd aprioryzmu popełnili tacy giganci jak św. Anzelm z Canterbury czy św. Tomasz z Akwinu, także O. Zielińska jest tu w bardzo dobrym, średniowiecznym, towarzystwie.

Po drugie, *Dane te są poddane pseudonimizacji, przez nadanie uczestnikom badania numerów lub liter*[347] – jak najbardziej, moja wieloletnia praca w tej dziedzinie potwierdza to twierdzenie, zwracam jednak uwagę, że dane spseudonimizowane są danymi osobowymi. Gdyby więc sponsor lub CRO nie mieli dostępu do danych niespseudonimizowanych, to przetwarzając dane spseudonimizowane, i tak przetwarzaliby oni dane osobowe.

Po trzecie, nie zachodzi dysonans, o którym autorka pisze tu: *Zachodzi tutaj pewien dysonans, ponieważ pomimo obowiązku nałożonego na sponsora badania prawidłowości nadzorowanego przez siebie badania klinicznego nie ma on wglądu w dane osobowe uczestnika*.[348] Nie zachodzi dysonans, ponieważ sponsor, który ma obowiązek badania prawidłowości nadzorowanego przez siebie badania klinicznego ma wgląd w dane osobowe uczestnika.

Po czwarte, monitorzy i pracownicy CRO *dokonują przeglądu dokumentacji badania klinicznego prowadzonej przez badacza i członków zespołu badawczego w danym ośrodku*[349], zapoznają się z nią, odnotowują swoje ustalenia, przekazują je sponsorowi – przetwarzają zatem dane osobowe pacjentów.

Po piąte, zgadzam się, że *Dokumentacja badania klinicznego zawiera dokumenty źródłowe, w tym formularze zgody na przetwarzanie danych osobowych uczestników badania. Osoby monitorujące badanie kliniczne uzyskują tym samym dostęp do danych osobowych uczestników*[350] – tu O. Zielińska ma rację, jednak to jest zdanie, które po-

[346] O. Zielińska, *op. cit.*

[347] O. Zielińska, *op. cit.*

[348] O. Zielińska, *op. cit.*

[349] O. Zielińska, *op. cit.*

[350] O. Zielińska, *op. cit.*

winno być podstawą jej wywodu, nie zaś założenie, zgodnie z którym *W praktyce sponsor badania lub podmioty prowadzące badania kliniczne na jego zlecenie (CRO) nie przetwarzają danych osobowych uczestników badania klinicznego*.

Po szóste, nic dla wywodu nie daje manewr wykonany przez O. Zielińską, manewr, którego celem było zapewne wskazanie, że sponsorzy i CRO przetwarzają dane poza materialnym zakresem stosowania RODO. Nic nie daje ponieważ:

- sponsorzy są administratorami danych osobowych w badaniu klinicznym,
- skoro sponsor jest administratorem danych, to przetwarzanie przez podmioty przetwarzające takie jak CRO i ośrodki badawcze jest w istocie przetwarzaniem danych przez sponsora,
- monitorzy utrwalają wyniki przeprowadzanych monitoringów, podobnie jak pracownicy CRO utrwalają wyniki swoich prac, co więcej czynią to zwykle z wykorzystaniem sprzętu komputerowego.

Zwracam szczególną uwagę na zadziwiające poglądy O. Zielińskiej. Jeżeli wymienione przez wskazaną autorkę podmioty przyjęłyby jej wizję przetwarzania danych w badaniach klinicznych, to nie tylko nie wiadomo kto miałby być administratorem tych danych, ale i narażałoby to sponsorów badań klinicznych i przedsiębiorstwa CRA/CRO na odpowiedzialność administracyjną i cywilną.

3.14. Art. 4 pkt 8. Uwaga 14.
Ustalanie podmiotu przetwarzającego, stanowisko ICO

Na stronie ICO zamieszczono trzy listy kontrolne. Nie omawiam ich tu, zwracam jedynie uwagę, na fakt, że poszczególne fragmenty list kontrolnych nie powinny być, w oderwaniu od pozostałych, uważane za przesądzające o roli podmiotu. Samo ICO pisze, że im więcej warunków z listy kontrolnej dany podmiot spełnia tym bardziej prawdopodobne jest, że należy do danej kategorii.[351] Istotnym brakiem w liście kontrolnej ICO jest pominięcie tego, że powierzenie przetwarzania należy utożsamiać ze zleceniem czynności na danych. Zagadnienie omawiam w uwadze *3.4. Art. 4 pkt 8. Uwaga 4. Powierzenie*

[351] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ dostęp: 2019.09.07, godz. 9.44. Tłum.: J. Rz.

przetwarzania jako zlecenie czynności na danych osobowych. Same listy kontrolne ICO omawiam niżej w uwadze *3.15. Art. 4 pkt 8. Uwaga 16. Listy kontrolne ICO, służące do ustalenia czy podmiot jest administratorem czy podmiotem przetwarzającym*.

3.14. Art. 4 pkt 8. Uwaga 15. Nakładanie się ról podmiotu przetwarzającego i administratora

W uwadze *3.13. Art. 4 pkt 8. Uwaga 13. Badania kliniczne. Role podmiotów na gruncie RODO* wspominam o zjawisku nakładania się ról. Należy na to zjawisko zwrócić baczną uwagę, nie jest bowiem, jak się zdaje, częste, jednak niewątpliwie zachodzi. Zjawisko to zachodzi kiedy podmiot przetwarzający jest wobec tych samych danych jednocześnie i podmiotem przetwarzającym i administratorem. Nie zauważyli tego zjawiska P. Litwiński, P. Barta i M. Kawecki, którzy napisali, że podmiot przetwarzający *(...) nie może więc – przetwarzając dane osobowe w imieniu administratora danych – realizować własnych celów przetwarzania danych*.[352]
Zachodzi ono w przypadku opisanym we wskazanej uwadze, kiedy to ośrodek badawczy (badacz) jest podmiotem przetwarzającym (ponieważ zawarł umowę ze sponsorem badania) i jest administratorem, ponieważ ma własne cele przetwarzania (leczenie, przechowywanie dokumentacji na podstawie przepisów prawa).

Analogiczny przykład zachodzi w przypadku wydatkowania środków europejskich. Instytucja zarządzająca jest administratorem a przedsiębiorca będący beneficjentem jest podmiotem przetwarzającym wobec danych beneficjentów ostatecznych np. swoich pracowników (ponieważ zawarł umowę z instytucją zarządzającą, z instytucją pośredniczącą) i jest administratorem danych osobowych tych samych swoich pracowników.

Sytuacji tej nie należy mylić z sytuacją, w której podmiot przetwarzający jest administratorem wobec jednych danych (na przykład danych swoich pracowników) i podmiotem przetwarzającym wobec innych danych (danych których powierzenie przetwarzania mu

[352] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 226.

powierzono). O tym właśnie drugim zjawisku pisze M. Sakowska-Baryła.[353]

3.15. Art. 4 pkt 8. Uwaga 16.
Listy kontrolne ICO, służące do ustalenia czy podmiot jest administratorem czy podmiotem przetwarzającym

Brytyjski organ ochrony danych, czyli Information Comissioner, znany zwykle pod skróconą nazwą: „ICO", publikuje na swojej stronie listy kontrolne, które mają pomóc w ustaleniu czy dany podmiot jest administratorem czy podmiotem przetwarzającym, czy współadministratorem (czy też raczej jednym ze współadministratorów). Listę kontrolną odnoszącą się do współadministratora zostawiam na boku, w niniejszym rozdziale zastanawiam się bowiem nad tym czy podmiot jest administratorem czy podmiotem przetwarzającym. Cytuję niżej listę kontrolną zaproponowana przez ICO, uważam bowiem, że jej analiza, analiza kolejnych kroków na tej liście, może pomóc w konkretnych sytuacjach, w odróżnieniu administratora od podmiotu przetwarzającego.

Nie jestem zwolennikiem przepisywania oficjalnych dokumentów, skądkolwiek by one pochodziły, ze względu na ich powszechną dostępność, uważam, jednak, że lista zaproponowana przez ICO, a właściwie listy, pewną wartość ma. Listy te poddaję niżej krytycznej analizie, podejście ICO jest bowiem niestety miejscami nieco życzeniowo-postulatywne. ICO ma tego zapewne świadomość, nad listami czytamy bowiem: *The following checklists set out indicators as to whether you are a controller, a processor or a joint controller. The more boxes you tick, the more likely you are to fall within the relevant category*, czyli: *Następujące listy kontrolne odnoszą się do wskaźników czy jesteś administratorem, podmiotem przetwarzającym, czy współadministratorem. Im więcej pól zaznaczysz, tym bardziej prawdopodobnie wpadasz do odpowiedniej kategorii*. Pomijając swobodę języka, należy zauważyć, że ICO nie daje w swoich listach, twardych wskazówek, listy te mają raczej charakter sugestii. Ze względu na fakt, że listy zapisane są w języku angielskim, poniżej cytuję orygi-

[353] M. Sakowska-Baryła w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych, Komentarz.* Warszawa 2018, s. 108.

nały angielskie tłumaczę je i odnoszę się do nich. Oryginały angielskie i tłumaczenia własne, oznaczam kursywą.[354]

Are we a controller?
Czy jesteśmy administratorem?

Odpowiedź na pytania zawarte w tej liście ma pomóc w ustaleniu czy odpowiadający jest administratorem.

Z uwagi na treść i formę pytań, odpowiedź twierdząca wskazuje, że analizowany podmiot jest raczej administratorem, odpowiedź przecząca wskazuje, że analizowany podmiot jest raczej podmiotem przetwarzającym. Piszę, że „raczej" bowiem sam ICO wskazuje na niekonkluzywny charakter pytań.

- We decided to collect or process the personal data.
- Zdecydowaliśmy by zbierać lub przetwarzać dane osobowe.

Tłumaczenie, które oddaje lepiej tłumaczoną treść, choć odchodzące od wierności językowej to: ***Zdecydowaliśmy o zbieraniu lub przetwarzaniu danych osobowych***. Parametr wydaje się trafny, rzeczywiście z art. 4 pkt 7 RODO wynika, że administrator decyduje o celu przetwarzania. Konieczne tu są jednak dwie uwagi.

Pierwsza ważniejsza – są podmioty, które nie decydują o celu przetwarzania danych ani o samym fakcie przetwarzania danych, a mimo tego są administratorami, są to podmioty, o celu przetwarzania danych osobowych, przez które, decyduje prawo.

Druga uwaga jest taka, że w angielskiej wersji definicji administratora czytamy: *(...) determines the purposes and means of the processing of personal data (...)*, podczas gdy na stronie ICO czytamy: ***decided to collect or process the personal data***. Jak widać w języku prawnym użyto formy czasownika „to determine", w języku prawniczym (na stronie www) użyto formy czasownika „to decide". Nie jest to wielki problem jest to jednak pewna niedoskonałość, która jednak, jak sądzę, nie wpływa na rozumowanie.

Poza tym w przepisie mowa jest o decydowaniu o celach, ICO odnosi się do decydowania o zbieraniu lub przetwarzaniu.

[354] Cała lista pochodzi ze strony https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ (dostęp" 2020.05.27. godz. 02.00.). Tłumaczenia oryginałów angielskich: J. Rzymowski.

- We decided what the purpose or outcome of the processing was to be.
- Zdecydowaliśmy jaki ma być cel lub wynik przetwarzania.

Parametr, podobnie jak poprzedzający, wydaje się trafny, jednak należy zwrócić uwagę, że zdarzają się sytuacje kiedy to nie administrator a prawo decyduje o celu przetwarzania a mimo tego administrator jest administratorem.

- We decided what personal data should be collected.
- Zdecydowaliśmy jakie dane osobowe powinny być zbierane.

Parametr, podobnie jak dwa poprzedzające, wydaje się trafny, jednak i tu należy zwrócić uwagę, że zdarzają się sytuacje kiedy to nie administrator a prawo decyduje o celu przetwarzania a mimo tego administrator jest administratorem. Jako przykład można podać tu podmioty medyczne, które w dokumentacji medycznej zbierają dane w zakresie wskazanym w stosownych przepisach. Podmioty te niewątpliwie są administratorami, choć nie decydują o zakresie zbieranych danych osobowych.

- We decided which individuals to collect personal data about.
- Zdecydowaliśmy o tym dane których osób fizycznych mają być zbierane.

Parametr, podobnie jak trzy poprzedzające, wydaje się trafny, jednak i tu należy zwrócić uwagę, że zdarzają się sytuacje kiedy to nie administrator a prawo decyduje o tym, że administrator ma obowiązek zbierać dane osobowe pewnych osób fizycznych. Lekarz zbiera dane osobowe pacjentów, urząd zbiera dane osobowe interesantów.

- We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.
- Uzyskujemy finansową korzyść lub inny zysk z przetwarzania z wyjątkiem jakiejkolwiek płatności od innego administratora.

Wydaje się, że ten parametr jest na tyle przemyślany, że nie sposób wskazać tu sytuacji granicznych, w których jego realizacja nie zachodzi a administrator i tak jest administratorem.

- We are processing the personal data as a result of a contract between us and the data subject.

- Przetwarzamy dane osobowe jako wynik umowy między nami a podmiotem danych.

Co do zasady, wydaje się, ze jeżeli podmiot zawiera umowę z osobą fizyczną, to jest administratorem jej danych, mam tu jednak pewien drobny niepokój, jestem bowiem w stanie wyobrazić sobie sytuację, w której podmiot zawiera umowę w imieniu innego podmiotu, wtedy wydaje się, że podmiot, który zlecił zawarcie umowy jest administratorem, wydaje się, że podmiot, który zawiera umowę na zlecenie, także jest administratorem, ale spraw wymaga zastanowienia.

- The data subjects are our employees.

- Podmioty danych są naszymi pracownikami.

W tym przypadku rzeczywiście niewątpliwie podmiot jest administratorem.

- We make decisions about the individuals concerned as part of or as a result of the processing.

- Podejmujemy decyzje o osobach zainteresowanych jako część lub jako wynik przetwarzania.

Nie jest to dobry parametr. Byłby dobry, gdyby pewne było, że podmiot, który podejmuje decyzje, nie podejmuje ich w imieniu administratora, a tego elementu w parametrze brak. Należy pamiętać, że decyzje może podejmować podmiot przetwarzający, jeżeli decyzje takie są konieczne dla wykonania czynności na danych zleconej przez administratora. Innymi słowy, parametr ten jest zbyt mało ostry.

- We exercise professional judgement in the processing of the personal data.

- Wykonujemy czynności profesjonalne przy przetwarzaniu danych osobowych.

Parametr ten wydaje się dobrze określony. Odpowiada on krokowi drugiemu w krokowej metodzie ustalenia czy podmiot jest administratorem danych (odbiorcą) czy podmiotem przetwarzającym *3.9. Art. 4 pkt 8. Uwaga 9. Krokowa metoda ustalenia czy podmiot jest administratorem danych (odbiorcą) czy podmiotem przetwa-*

rzającym. Krok 2. Czy podmiot lub osoba wykonuje zawód lub działalność uregulowaną prawem w taki sposób, że działa w sposób, który nie dopuszcza przyjmowania wskazówek od zleceniodawcy?. Wykonywanie czynności profesjonalnych jest zwykle uregulowane przepisami, mowa tu zapewne o czynnościach na danych, wykonywanych przez lekarzy, prawników itp.

- We have a direct relationship with the data subjects.
- Mamy bezpośrednią relację z podmiotami danych.

Parametr wydaje się być dobrze określony, zapewne mowa tu o sytuacji, w której administratora i podmiot danych wiąże umowa. Bezpośredniości nie należy tu jednak rozumieć dosłownie. Jeżeli administrator zawiera umowę za pośrednictwem podmiotu przetwarzającego, to nadal jest administratorem, mimo, że jego relacja z podmiotem danych – osobą, której dane dotyczą nie jest bezpośrednia w sensie dosłownym.

- We have complete autonomy as to how the personal data is processed.
- Mamy całkowitą samodzielność jeśli chodzi o to jak dane osobowe są przetwarzane.

Przez samodzielność, autonomię, można zapewne rozumieć to, że podmiot sam decyduje o celach i środkach, czyli, że podmiot taki jest administraotrem. Parametr jest dobrze dobrany.

- We have appointed the processors to process the personal data on our behalf.
- Wyznaczyliśmy podmioty przetwarzające do przetwarzania w naszym imieniu.

Parametr jest dobrze dobrany. Przylega znaczeniowo do definicji podmiotu przetwarzającego, zawartej w art. 4 pkt 8 RODO. Parametr ten odpowiada krokowi 6 w krokowej metodzie ustalenia czy podmiot jest administratorem danych (odbiorcą) czy podmiotem przetwarzającym *3.9. Art. 4 pkt 8. Uwaga 9. Krokowa metoda ustalenia czy podmiot jest administratorem danych (odbiorcą) czy podmiotem przetwarzającym. Krok 6. Czy administrator zleca wykonanie czynności na danych w swoim czyli zleceniodawcy czyli administratora imieniu?*

Are we a processor?
Czy jesteśmy podmiotem przetwarzającym?

Odpowiedź na pytania zawarte w tej liście ma pomóc w ustaleniu czy odpowiadający jest podmiotem przetwarzającym.

Z uwagi na treść i formę pytań, odpowiedź twierdząca wskazuje, że analizowany podmiot jest raczej podmiotem przetwarzającym, odpowiedź przecząca wskazuje, ze analizowany podmiot jest raczej administratorem. Piszę, że „raczej" bowiem sam ICO wskazuje na niekonkluzywny charakter pytań.

- ***We are following instructions from someone else regarding the processing of personal data.***
- ***Postępujemy według poleceń od kogoś innego, które to polecenia odnoszą się do przetwarzania danych osobowych***.

  Skoro podmiot postępuje według poleceń innego podmiotu, w zakresie przetwarzania danych osobowych, to podmiot ten nie ustala sposobów przetwarzania danych osobowych. Ustalanie sposobów przetwarzania jest elementem definicji administratora, zawartej w art. 4 pkt 7 RODO. Parametr wydaje się być dobrze określony.

- ***We were given the personal data by a customer or similar third party, or told what data to collect***.
- ***Dane zostały nam dane przez klienta lub podobną trzecią stronę lub powiedziano nam jakie dane zbierać.***

  Skoro „powiedziano nam jakie dane zbierać", to podmiot nie decyduje o celach przetwarzania. Drugi element: „Dane zostały nam dane przez klienta lub podobną trzecią stronę" wydaje się niezrozumiały. Samo zdanie, sam przekaz jest zrozumiały, jednak jak jego treść miałaby wpływać na decyzję o tym czy podmiot jest podmiotem przetwarzającym – nie wiem. Parametr wydaje się być dobrze określony w połowie.

- ***We do not decide to collect personal data from individuals***.
- ***Nie decydujemy o tym by zbierać dane osobowe od osób fizycznych***.

  Skoro podmiot nie decyduje o samym zbieraniu, to zapewne nie decyduje też o celach i sposobach tegoż, zatem nie jest administratorem. Parametr wydaje się być dobrze określony.

- ***We do not decide what personal data should be collected from individuals***.
- ***Nie decydujemy jakie dane osobowe powinny być zbierane od osób fizycznych***.

  Skoro podmiot nie decyduje o tym jakie dane osobowe zbiera, to zapewne nie decyduje również o celu zbierania tychże, zatem nie jest administratorem. Parametr wydaje się być dobrze określony.

- ***We do not decide the lawful basis for the use of that data***.
- ***Nie decydujemy o podstawach prawnych użycia danych*** (tych danych, danych osobowych).

  Skoro podmiot nie decyduje o użyciu danych, to wydaje się to tożsame z tym, ze podmiot nie decyduje o celu przetwarzania, zatem nie jest administratorem. Parametr wydaje się być dobrze określony.

- ***We do not decide what purpose or purposes the data will be used for***.
- ***Nie decydujemy o celu lub celach w jakich dane będą używane***.

  Idealna zgodność a właściwie niezgodność z definicją administratora (danych) z art. 4 pkt 7 RODO. Parametr wydaje się być dobrze określony.

- ***We do not decide whether to disclose the data, or to whom***.
- ***Nie decydujemy czy ujawniać dane lub komu je ujawniać***.

  Skoro podmiot nie decyduje o ujawnieniu danych, to wydaje się to tożsame z tym, że podmiot nie decyduje o celu przetwarzania, zatem nie jest administratorem. Parametr wydaje się być dobrze określony.

- ***We do not decide how long to retain the data***.
- ***Nie decydujemy o tym jak długo przechowywać dane.***

  Parametr wydaje się być dobrze dobrany. Skoro podmiot nie decyduje o okresie przechowywania, to o owym decydować musi kto inny. Problemem jest sytuacja, kiedy tym kimś innym jest prawodawca. W takiej sytuacji podmiot, który nie decyduje o okresie przetwarzania danych i tak jest administratorem. Parametr pozornie dobrze dobrany ale może dać fałszywy wynik.

- ***We may make some decisions on how data is processed, but implement these decisions under a contract with someone else***.
- ***Możemy podejmować niektóre decyzje dotyczące tego jak dane są przetwarzane ale wdrażamy te decyzje zgodnie z umową z kim innym.***

  Wdrażanie decyzji dotyczących przetwarzania danych osobowych, zgodnie z umową z innym podmiotem wskazuje na fakt, że ten inny podmiot jest administratorem. Parametr wydaje się być dobrze określony.

- ***We are not interested in the end result of the processing***.
- ***Nie jesteśmy zainteresowanie końcowym wynikiem przetwarzania***.

  Parametr mało prawniczy, rzekłbym. Wydaje się być dobrze dobrany, ale dobrany jest raczej w oparciu o rozsądek niż o analizę przepisów. Nie czyni go to złym ale może być trudno, w oparciu o ten parametr, na przykład uzasadnić pogląd w piśmie procesowym. Pozwolę sobie tu na uwagę, że źle czynią ci co odrzucają logikę, na rzecz rozsądku.

4. Art. 4 pkt 8. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 8 RODO definiuje **podmiot przetwarzający**, zatem zgodnie z dyrektywą języka prawnego[355], każdy kto interpretuje RODO powinien rozumieć pojęcie „**podmiot przetwarzający**" tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „**podmiot przetwarzający**" tak jest ono zdefiniowane w art. 4 pkt. 8 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „**podmiot przetwarzający**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

[355] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

5. Art. 4 pkt 8. Konkretyzacja zasady

Art. 4 ust. 8 sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Podmiot przetwarzający przetwarza dane w oparciu o podstawę prawną, w oparciu o którą dane przetwarza administrator danych, który powierzył mu przetwarzanie i w oparciu o umowę przetwarzania.

Realizacji **zasady rzetelności**. Realizując obowiązki wynikające z art. 13 RODO, z art. 14 RODO i z art. 15 RODO, administrator (danych) ma obowiązek informować o odbiorcach. Nie jest do końca jasne, czy podmiot przetwarzający jest odbiorcą. Ja uważam, że nie jest. Odsyłam tu do komentarza i uwag do art. 4 pkt 9 RODO. Jeżeli jednak administrator danych uważa że podmiot przetwarzający jest odbiorcą, to wtedy informując o odbiorcach, informuje również między innymi o podmiotach przetwarzających co sprzyja realizacji zasady rzetelności.

Realizacji **zasady przejrzystości** poprzez informowanie o podmiotach przetwarzających, przy okazji informowania o odbiorcach. i tu odsyłam do komentarza i uwag do art. 4 pkt 9 RODO. Jeżeli administrator danych uważa że podmiot przetwarzający jest odbiorcą, to wtedy informując o odbiorcach, informuje również między innymi o podmiotach przetwarzających co sprzyja również realizacji zasady przejrzystości.

Realizacji **zasady ograniczenia celu**, poprzez dbanie przez administratora danych o to by podmiot przetwarzający przetwarzał tylko w celu wskazanym w umowie przetwarzania lub innej analogicznej umowie. Oczywiste jest, że cel ten musi być zgodny z celem, w którym dane osobowe przetwarza administrator danych, przy czym czy przetwarza sam, czy wyłącznie za pośrednictwem podmiotu przetwarzającego – nie jest to istotne.

Realizacji **zasady minimalizacji** poprzez dbanie przez administratora danych o to by podmiot przetwarzający przetwarzał tylko te dane, których przetwarzanie jest niezbędne do osiągniecia celu przetwarzania, celu o którym decyduje administrator danych. Zasadę minimalizacji rozumiemy tu restrykcyjnie *3.2. Art. 5 ust. 1 lit. c. Uwaga 2. Treść zasady, podejście restrykcyjne*.

Realizacji **zasady minimalizacji** poprzez dbanie przez administratora danych o to by podmiot przetwarzający przetwarzał tylko te dane, których przetwarzanie nie jest co prawda niezbędne do osiągniecia celu przetwarzania, jednak dane te są adekwatne i stosowne do osiągnięcia celów do których są przetwarzane. Zasadę minimalizacji

rozumiemy tu łagodnie *3.3. Art. 5 ust. 1 lit. c. Uwaga 3. Treść zasady, podejście łagodne*.

Administrator ma obowiązek przyjmować żądania usunięcia danych, wysuwane na podstawie art. 17 RODO, przez osoby, których dane dotyczą i na te żądania stosownie reagować.

Administrator ma obowiązek przyjmować żądania ograniczenia przetwarzania, wysuwane na podstawie art. 18 RODO, przez osoby, których dane dotyczą i na te żądania stosownie reagować. Żądanie ograniczenia przetwarzania może skutkować poprawieniem przetwarzanych danych osobowych.

Administrator ma obowiązek przyjmować sprzeciw wobec przetwarzania danych, wysuwany na podstawie art. 21 RODO, przez osoby, których dane dotyczą i na ten sprzeciw stosownie reagować.

Może się zdarzyć, że żądanie wynikające z art. 17 RODO lub z art. 18 RODO lub z art. 21 RODO zostanie skierowane do podmiotu przetwarzającego a nie do administratora danych. Żądania takiego nie wolno zlekceważyć. Podmiot przetwarzający powinien żądanie takie przekazać administratorowi danych by ten mógł podjąć decyzję o sposobie realizacji żądania. Nieistotne jest tu, czy dane przetwarza administrator czy podmiot przetwarzający. Decyzja należy do administratora danych. Oczywiście przyjmowanie żądań lub/i podejmowanie decyzji o sposobie ich realizacji administrator danych może zlecić podmiotowi przetwarzającemu. Na marginesie zwracam uwagę, że podejmowanie decyzji i kontaktowanie się z osobą, której dane dotyczą, nie są czynnościami na danych, więc tu nie należy tworzyć umowy powierzenia przetwarzania. Usuwanie danych i poprawianie danych są czynnościami na danych, więc tu należy tworzyć umowy powierzenia przetwarzania.

Rozważania tu prowadzone aktualne są również w odniesieniu do art. 19 RODO, z którego wynika spoczywający na administratorze danych obowiązek informowania odbiorcy o tym, że administrator usunął dane lub ograniczył przetwarzanie.

Realizacja **zasady prawidłowości**. Administrator ma obowiązek przyjmować żądania sprostowanie danych, wysuwane na podstawie art. 16 RODO, przez osoby, których dane dotyczą i na te żądania stosownie reagować. Może się zdarzyć, że żądanie zostanie skierowane do podmiotu przetwarzającego a nie do administratora danych. Żądania takiego nie wolno zlekceważyć. Podmiot przetwarzający powinien żądanie takie przekazać administratorowi (danych) by ten mógł

podjąć decyzję o sposobie realizacji żądania. Nieistotne jest tu, czy dane przetwarza administrator czy podmiot przetwarzający. Decyzja należy do administratora danych. Oczywiście przyjmowanie żądań sprostowania danych lub/i podejmowanie decyzji o sposobie realizacji żądania administrator (danych) może zlecić podmiotowi przetwarzającemu. Na marginesie zwracam uwagę, że podejmowanie decyzji i kontaktowanie się z osobą, której dane dotyczą, nie są czynnościami na danych, więc tu nie należy tworzyć umowy powierzenia przetwarzania. Usuwanie danych i poprawianie danych są czynnościami na danych, więc tu należy tworzyć umowy powierzenia przetwarzania.

Rozważania tu prowadzone aktualne są również w odniesieniu do art. 19 RODO, z którego wynika spoczywający na administratorze (danych) obowiązek informowania odbiorcy o tym, że administrator sprostował dane.

Realizacja **zasady ograniczenia przechowywania danych**.

Administrator ma obowiązek przyjmować żądania usunięcia danych, wysuwane na podstawie art. 17 RODO, przez osoby, których dane dotyczą i na te żądania stosownie reagować.

Administrator ma obowiązek przyjmować żądania ograniczenia przetwarzania, wysuwane na podstawie art. 18 RODO, przez osoby, których dane dotyczą i na te żądania stosownie reagować. Żądanie ograniczenia przetwarzania może skutkować poprawieniem przetwarzanych danych.

Administrator ma obowiązek przyjmować sprzeciw wobec przetwarzania danych, wysuwany na podstawie art. 21 RODO, przez osoby, których dane dotyczą i na ten sprzeciw stosownie reagować.

Może się zdarzyć, że żądanie wynikające z art. 17 RODO lub z art. 18 RODO lub z art. 21 RODO zostanie skierowane do podmiotu przetwarzającego a nie do administratora danych. Żądania takiego nie wolno zlekceważyć. Podmiot przetwarzający powinien żądanie takie przekazać administratorowi danych by ten mógł podjąć decyzję o sposobie realizacji żądania. Nieistotne jest tu, czy dane przetwarza administrator czy podmiot przetwarzający. Decyzja należy do administratora danych. Oczywiście przyjmowanie żądań lub/i podejmowanie decyzji o sposobie ich realizacji administrator danych może zlecić podmiotowi przetwarzającemu. Na marginesie zwracam uwagę, że podejmowanie decyzji i kontaktowanie się z osobą, której dane dotyczą, nie są czynnościami na danych, więc tu nie należy tworzyć umowy powierzenia przetwarzania. Usuwanie danych i poprawianie

danych są czynnościami na danych, więc tu należy tworzyć umowy powierzenia przetwarzania.

Rozważania tu prowadzone aktualne są również w odniesieniu do art. 19 RODO, z którego wynika spoczywający na administratorze danych obowiązek informowania odbiorcy o tym, że administrator usunął dane lub ograniczył przetwarzanie.

Realizacja **zasady integralności**. Zasada integralności, w skrócie oznacza, że na administratorze danych spoczywa obowiązek dbałości o to by dane były modyfikowane, w tym niszczone lub uszkadzane, jedynie przez osoby, które czynią to w sposób autoryzowany przez ADO. Autoryzację osiąga się dzięki systemowi wynikającemu z art. 29 RODO i art. 32 ust. 4 RODO, piszę tu o obowiązku wydawania upoważnień i nadawania poleceń, oczywiście rozmaicie rozumianych. Upoważnienia nadaje administrator lub podmiot przetwarzający, dlatego też definicja podmiotu przetwarzającego, w odległy sposób, ale jednak, sprzyja realizacji zasady integralności.

Realizacja **zasady poufności**. Z art. 29 RODO i z art. 32 ust. 4 RODO wynika m.in., że podmiot przetwarzający powinien dbać o to by dane, których przetwarzanie mu powierzono, były przetwarzane przez osoby działające z jego upoważnienia. Pomijam tu sprawę natury tego upoważnienia, odsyłam do komentarzy do odpowiednich przepisów, zwracam jedynie uwagę, że osoby upoważnione niekoniecznie trzeba rozumieć jako osoby, którym podmiot przetwarzający nadał upoważnienie. Ze wskazanych przepisów pośrednio wynika zatem obowiązek upoważnienia do przetwarzania osób, które dane przetwarzać będą. Obowiązek ten spoczywa na administratorze i na podmiocie przetwarzającym, wydaje się, że precyzyjniej byłoby wskazać, że obowiązek ten spoczywa odpowiednio na administratorze lub na podmiocie przetwarzającym. Realizacja tego obowiązku sprzyja realizacji zasady poufności.

6. Art. 4 pkt 8. Postulaty de lege ferenda

6.1 Art. 4 pkt 8. Postulat 1. Uporządkowanie kwestii dalszego powierzenia

Wyżej, w uwadze *3.1. Art. 4 pkt 8. Uwaga 1. Co odróżnia administratora danych od podmiotu przetwarzającego* podnoszę, że z komentowanego przepisu nie wynika w sposób jednoznaczny czy podmiot, któremu administrator danych powierzy przetwarzanie da-

nych i który podpowierzył przetwarzanie tych danych i który sam nie przetwarza danych osobowych, których przetwarzanie podpowierzył, jest podmiotem przetwarzającym. Źródłem problemu interpretacyjnego są słowa definicji podmiotu przetwarzającego, które stanowią, że: *który przetwarza dane osobowe w imieniu administratora*. Czyli, że jeżeli podmiot nie przetwarza danych (osobowych), oczywiście w imieniu administratora, to nie jest podmiotem przetwarzającym.

Zapewne intencją prawodawcy było wskazanie, że dla istnienia zjawiska podmiotu przetwarzającego a tym samym dla istnienia zjawiska powierzenia nie jest ważne istnienie umowy, zaś ważne jest czy zachodzi przetwarzanie. Przetwarzanie przez podmiot, nazwany tu podmiotem przetwarzającym, przetwarzanie przez ten podmiot w imieniu administratora danych. Zgadzam, się, że ważna jest relacja, stan faktyczny, umowa jest dodatkiem, obowiązkowym dodatkiem ale dodatkiem, o czym piszę w uwadze *3.7. Art. 4 pkt 8. Uwaga 7. Bezumowne powierzenie przetwarzania danych osobowych a prowadzenie cudzych spraw bez zlecenia*. Może się jednak zdarzyć, że jest umowa powierzenia, umowa powierzenia skutkuje podpowierzeniem, jednak podmiot, któremu powierzono przetwarzanie i który je podpowierzył, sam nie przetwarza danych. Trudno powiedzieć, że nie ma tu relacji miedzy administratorem danych a tym podmiotem.

Można, co wyjaśniam w uwadze *3.3. Art. 4 pkt 8. Uwaga 3. Konieczność odróżnienia administratora danych od podmiotu przetwarzającego*, przyjąć, że nie jest to relacja administratora i podmiotu przetwarzającego, ale że jest to relacja mocodawcy i pełnomocnika. Można, tyle, że relacja administratora i podmiotu przetwarzającego i tak zawsze jest relacją mocodawcy i pełnomocnika a przynajmniej jest analogiczna do takiej relacji. Relacja mocodawcy i pełnomocnika jest zatem relacją o szerszym zakresie znaczeniowym aniżeli relacja administratora i podmiotu przetwarzającego. Znaczenie pojęcia relacji administratora i podmiotu przetwarzającego mieści się w znaczeniu pojęcia relacji mocodawcy i pełnomocnika. Podmiot, któremu powierzono przetwarzanie i który je podpowierzył i który sam nie przetwarza danych jest zatem pełnomocnikiem mocodawcy – administratora danych. Ciągle jednak nie daje to odpowiedzi na pytanie czy podmiot ten jest podmiotem przetwarzającym. Jeśli nie jest to jest stroną trzecią, co ogromnie mi się nie podoba. Problem, znika, jeżeli podmiot, któremu powierzono przetwarzanie i który je podpowierzył i który sam nie przetwarza danych, mieści się w definicji podmiotu przetwa-

rzającego. Jeśli jest on podmiotem przetwarzającym, to po drugie, nie jest on stroną trzecią a po pierwsze, wiadomo w końcu, kim on jest. W tym celu trzeba znowelizować art. 4 pkt 8 RODO.

Postuluję nowelizację art. 4 pkt 8 RODO przez dodanie na końcu przepisu słów: „lub który powierza przetwarzanie danych kolejnemu podmiotowi przetwarzającemu". Artykuł 4 pkt 8 RODO, po proponowanej nowelizacji miałby postać: „„podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora **lub który powierza przetwarzanie danych kolejnemu podmiotowi przetwarzającemu**". (Czcionką wytłuszczoną zaznaczam słowa dodane.)

7. Art. 4 pkt 8. Rozważania historyczne.

7.1. Art. 4 pkt 8. Rozważanie 1.
Historyczne nazwy podmiotu przetwarzającego

Definicja podmiotu przetwarzającego obecna jest w Dyrektywie 95/46/WE. w wersji polskojęzycznej czytamy: *"przetwarzający" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych*. Pozornie definicja ta różni się (sic!) od definicji znajdującej się w art. 4 pkt 8 RODO: *„podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora*.

Piszę, że definicja z Dyrektywy 95/46/WE różni się od definicji z RODO jedynie pozornie, ponieważ jeżeli porównamy wersje anglojęzyczne definicji, to okazuje się, że różnice są znikome. Definicja podmiotu przetwarzającego w Dyrektywie 95/46/WE, w wersji anglojęzycznej: *'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*. Definicja znajdująca się w art. 4 pkt 8 RODO w wersji anglojęzycznej: *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*.

Wnioski z porównania definicji w wersji z Dyrektywy 95/46/WE i z RODO są dość oczywiste. Definicja umieszczona w RODO nie różni się od definicji umieszczonej w Dyrektywie 95/46/WE. Różnice między: „shall mean" a „means" i między „any other body" a „other body" mogą zostać pominięte. Tajemnicą pozostanie dlaczego tłu-

macz na język polski dokonał zmian. Nie widzę sensu analizowania niezgrabnego tłumaczenia treści definicji, jednak uważam za konieczne zajecie stanowiska w kwestii podmiotu definiowanego.
- Wersja z Dyrektywy 95/46/WE w języku angielskim: „processor".
- Wersja z Dyrektywy 95/46/WE w języku polskim: „processor".
- Wersja z RODO w języku angielskim: „processor".
- Wersja z RODO w języku polskim: „podmiot przetwarzający".

To proste zestawienie każe zadać pytanie o to skąd w wersji polskiej w definicji znalazło się słowo „podmiot". Jeżeli dla potrzeb Dyrektywy 95/46/WE słowo to było niepotrzebne i samo „przetwarzający" wystarczało, to dlaczego dokonano zmiany?
Na pytanie to można odpowiedzieć rozmaicie, ja jednak wolę pozostawić je bez odpowiedzi.

Artykuł 4 ust. 1 pkt 9 RODO

„odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

1. Art. 4 pkt 9. Komentarz

Komentarz do art. 4 ust. 1 pkt 9 RODO składa się z dwóch części. Pierwsza część komentarza to ogólne wyjaśnienie zakresu definicji, druga część to „Ostateczna lista odbiorców", czyli lista podmiotów, które są odbiorcami. Lista ta nazwana została „ostateczną" Ponieważ jest ostatecznym efektem kolejnych analiz. Na drodze tych analiz powstały inne, nieostateczne, robocze, wcześniejsze, listy odbiorców, które zamieszczone są poniżej.

Najpierw powstała lista odbiorców, która znajduje się w pozycji: *2. Art. 4 pkt 9. Analiza*. Lista ta przeplata się z rozważaniami, które uzasadniają zawartość tej listy.

Następnie w pozycji: *3.1. Art. 4 pkt 9. Uwaga 1. Teoretyczna lista odbiorców* znajduje się robocza lista odbiorców, która stanowi wstępny wniosek, wyciągnięty z analiz przeprowadzonych w związku z pierwszą listą.

Następnie w pozycji *3.2. Art. 4 pkt 9. Uwaga 2. Teoretyczna lista odbiorców z komentarzami* Znajduje się lista odbiorców nazwana uprzednio „teoretyczną listą odbiorców", opatrzona komentarzami dotyczącymi poszczególnych podmiotów. Wynikiem analiz poprowadzonych w związku z tą listą jest: *Ostateczna lista odbiorców*, która jest, co dziwić nie powinno, ostatecznym wnioskiem z rozumowań prowadzonych w kontekście wcześniej przedstawianych list.

1. Art. 4 pkt 9. Komentarz I

Odbiorcą może być każdy z podmiotów wymienionych w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków. Wymienione w przepisie podmioty to: osoba fizyczna, osoba prawna, organ publiczny, jednostka, podmiot inny niż wymienione podmioty. Podstawowy z warunków zawartych w przepisie jest taki, że odbiorcy ujawniane są dane osobowe. Drugi z warunków zawartych w przepisie jest taki, że odbiorca może być stroną trzecią albo może nie być stroną trzecią.

Jeśli chodzi o organy państwa, którym ujawniane są dane osobowe, to są one odbiorcami jeżeli dane t ujawniane są poza konkretnym postępowaniem. Jeżeli dane ujawniane są organowi państwa w ramach konkretnego postępowania, to organ taki nie jest odbiorcą. Wydaje się więc ze organy są odbiorcami, kiedy administratorzy (danych) przekazują im dane osobowe w ramach swoich obowiązków sprawozdawczych.

1. Art. 4 pkt 9. Komentarz II
Ostateczna lista odbiorców

Zaproponowaną niżej ostateczną listę odbiorców można wykorzystywać jak narzędzie do sprawdzenia czy dana osoba, lub podmiot, może być odbiorcą czy nie może, jak również czy jest odbiorcą czy nie jest. Nie należy korzystać z niej jak z narzędzia umożliwiającego dokonanie decyzji czy dana osoba jest odbiorcą, czy należy z nią podpisywać umowę powierzenia przetwarzania.

Lista poniższa może znacznie pomóc w pracy nad RCPD, czy też w uzupełnianiu RCPD. Uważam, że jeśli przekazujemy dane odbiorcy i odbiorca ten nie należy do kategorii odbiorców, którzy już są w RCPD wymienieni i to w związku z daną czynnością, to przekazywanie to należy w RCPD odnotować. Lista jest efektem ustaleń prowadzonych poniżej w analizie.

- **osoba**[356] **fizyczna** (której udostępnia się dane osobowe) **inna niż osoba** (której udostępnia się dane osobowe)**, której dane dotyczą – może być odbiorcą,**

[356] Ortografia nakazywałaby zaczynanie niektórych punktów wyliczenia od wielkiej litery. Poświęcam tu reguły ortografii na rzez jasności. Nie chcę by niektóre

- **osoba fizyczna** (której udostępnia się dane osobowe) **inna niż administrator – może być odbiorcą,**
- **osoba fizyczna** (której udostępnia się dane osobowe) **inna niż podmiot przetwarzający – może być odbiorcą,**
- **osoba fizyczna** (której udostępnia się dane osobowe) **inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – może być odbiorcą,**
- **osoba fizyczna** (której udostępnia się dane osobowe) **- osoby upoważnione do przetwarzania danych osobowych,**
- **osoba prawna** (której udostępnia się dane osobowe) **- inna niż osoba, której dane dotyczą – może być odbiorcą,**
- **osoba prawna** (której udostępnia się dane osobowe) **- inna niż administrator – może być odbiorcą,**
- **osoba prawna** (której udostępnia się dane osobowe) **- inna niż podmiot przetwarzający – może być odbiorcą,**
- **osoba prawna** (której udostępnia się dane osobowe) **- inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający– może być odbiorcą**, z tym, że należy pamiętać, że osoby prawne nie są upoważniane z zasady, aczkolwiek, jeżeli administrator nie stosuje upoważnień, to dwuetapowe uprawnienie do danych może być skonstruowane inaczej niż za pomocą upoważnień i poleceń,
- **organ publiczny** (któremu udostępnia się dane osobowe) **otrzymujący dane nie w ramach konkretnego postępowania - inny niż osoba, której dane dotyczą – jest odbiorcą.** Tu w zasadzie należałoby odrzucić ten podmiot, bo organ to organ, nie osoba fizyczna, ale dla wywodu nie ma to większego znaczenia.
- **organ publiczny** (któremu udostępnia się dane osobowe) **otrzymujący dane nie w ramach konkretnego postępowania - inny niż administrator - jest odbiorcą,**
- **organ publiczny** (któremu udostępnia się dane osobowe) **otrzymujący dane nie w ramach konkretnego postępowania - inny niż podmiot przetwarzający – jest odbiorcą,**
- **organ publiczny** (któremu udostępnia się dane osobowe) **otrzymujący dane nie w ramach konkretnego postępowania - inny niż**

---

podmioty w wyliczeniu zapisane były małą, inne zaś wielką literą, mogłoby to bowiem skutkować wyciągnięciem z tej różnicy jakichś wniosków, który byłyby tu nieuprawnione i przypadkowe.

osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – jest odbiorcą. Tu w zasadzie należałoby odrzucić ten podmiot, bo organ to organ, nie osoba fizyczna, ale dla wywodu nie ma to większego znaczenia.

- **jednostka** (której udostępnia się dane osobowe) **- inna niż osoba, której dane dotyczą – jest odbiorcą,**
- **jednostka** (której udostępnia się dane osobowe) **- inna niż administrator – jest odbiorcą,**
- **jednostka** (której udostępnia się dane osobowe) **- inna niż podmiot przetwarzający – jest odbiorcą,**
- **jednostka** (której udostępnia się dane osobowe) **- inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – jest odbiorcą,**
- **podmiot** (któremu udostępnia się dane osobowe) **- inna niż osoba, której dane dotyczą – jest odbiorcą,**
- **podmiot** (któremu udostępnia się dane osobowe) **- inna niż administrator - jest odbiorcą,**
- **podmiot** (któremu udostępnia się dane osobowe) **- inna niż podmiot przetwarzający - jest odbiorcą,**
- **podmiot** (któremu udostępnia się dane osobowe) **- inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – jest odbiorcą.**

2. Art. 4 pkt 9. Analiza

Ze słów wytłuszczonych w przepisie: „**oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią**. (…)" należy wnioskować, że odbiorcą może być każdy z podmiotów wymienionych w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków.

Odbiorcą jest osoba fizyczna której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Odbiorcą jest osoba prawna której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Odbiorcą jest organ publiczny otrzymujący dane nie w ramach konkretnego postępowania, któremu jednak ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Odbiorcą jest jednostka której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
Odbiorcą jest inny podmiot któremu ujawnia się dane osobowe niezależnie od tego czy jest stroną trzecią.

Dla pełnego zrozumienia definicji odbiorcy należy zatem połączyć kolejne elementy definicji odbiorcy, z odpowiadającymi im znaczeniowo elementami definicji strony trzeciej. Operacji tej dokonuję poniżej.
Należy zwrócić uwagę na jeszcze jedno zjawisko, otóż z definicji odbiorcy wynika, że odbiorcą jest każdy komu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią.
Podążając więc dalej, widzimy, że **odbiorcą jest każdy komu ujawnia się dane osobowe jeżeli jest stroną trzecią i jeżeli nie jest stroną trzecią**.
Prowadzi nas to do dwóch grup konstatacji:
- Z faktu, że odbiorcą jest każdy komu ujawnia się dane osobowe jeżeli jest stroną trzecią nie wynika nic niepokojącego. **Należy po prostu uznać, że wszystkie strony trzecie są odbiorcami, o ile ujawnia się im dane osobowe**.
- Z faktu, że odbiorcą jest każdy komu ujawnia się dane osobowe jeżeli nie jest stroną trzecią nie wynika nic niepokojącego. **Należy po prostu uznać, że wszystkie osoby i podmioty inne niż strony trzecie są odbiorcami, o ile ujawnia się im dane osobowe**.

Z faktu, że odbiorcą jest każdy komu ujawnia się dane osobowe jeżeli nie jest stroną trzecią może wyniknąć pewien błąd interpretacyjny. Najprościej byłoby uznać, że jeżeli ktoś nie jest stroną trzecią, to wynika z tego, że jest odbiorcą o ile ujawnia mu się dane osobowe.
Prowadziłoby to do wniosku, że odbiorcą jest osoba fizyczna, której ujawnia się dane osobowe, o ile tylko nie jest stroną trzecią. Odbiorcami, przy takiej interpretacji, byłyby zatem, pod warunkiem ujawniania im danych osobowych: osoby których dane dotyczą, administrator, podmiot przetwarzający, wszelkie osoby fizyczne nie posiadające upoważnienia do przetwarzania danych osobowych. Nawet pobieżny pogląd na tak wysnuty wniosek powoduje, że widać, że wniosek ten jest co najmniej dziwaczny. Dziwaczność tę analizuję poniżej, pod zestawieniami pojęć pochodzących z definicji odbiorcy i z definicji osoby trzeciej, drobiazgowo, w odniesieniu do każdej kategorii danych osobowych, tu sygnalizuję tylko sposób rozumowania.

Czy osoba, której dane dotyczą jest odbiorcą danych? Nie, nie jest, jest bowiem osobą, której dane dotyczą. Za uznaniem, że osoba, której dane dotyczą nie jest odbiorcą przemawia zakaz wykładni synonimicznej.

Czy administrator (danych osobowych), któremu ujawnia się dane osobowe jest odbiorcą? Gdyby uznać, że jest, to prowadziłoby to do wniosku, że możliwe jest by administrator (danych) ujawnił dane osobowe sam sobie. Ujawnienie czegokolwiek samemu sobie jest nie tylko dziwaczne ale i absurdalne. Za uznaniem, że administrator (danych) nie jest odbiorcą przemawia zakaz wykładni synonimicznej[357] i zasada argumentum ad absurdum. [358] Oczywiście piszę tu o administratorze, który udostępnia, ujawnia dane osobowe.

Należy zwrócić uwagę, że zarówno w definicji odbiorcy, jak i w definicji osoby trzeciej występują następujące podmioty: osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe. Ustalenie zakresu pojęcia: „odbiorca" możliwe jest zatem dzięki zestawieniu odpowiednich cech wymienionych podmiotów, przy czym cechy te pochodzić powinny z obydwu przepisów.

Odbiorcą jest osoba fizyczna której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
Stroną trzecią może być osoba fizyczna.
inna niż osoba, której dane dotyczą,
inna niż administrator,
inna niż podmiot przetwarzający,
inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca jest stroną trzecią uzyskujemy następujące podmioty:
osoba fizyczna inna niż osoba, której dane dotyczą,

[357] M. Zirk-Sadowski w: *System Prawa Administracyjnego* Red: R Hauser, Z Niewiadomski, A Wróbel, *Tom IV. Wykładnia w prawie administracyjnym.* L. Leszczyński, B. Wojciechowski, M. Zirk-Sadowski, Warszawa 2012, s. 200.

[358] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 150.

osoba fizyczna inna niż administrator,
osoba fizyczna inna niż podmiot przetwarzający,
osoba fizyczna inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca nie jest stroną trzecią uzyskujemy następujące podmioty:
osoba fizyczna - której dane dotyczą,
osoba fizyczna – administrator,
osoba fizyczna - podmiot przetwarzający,
osoba fizyczna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Jak widać niektóre zestawienia kłócą się z rozsądkiem, nad czym deliberuję dalej.

Odbiorcą jest osoba prawna której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
Stroną trzecią może być osoba prawna.
inna niż osoba, której dane dotyczą,
inna niż administrator,
inna niż podmiot przetwarzający,
inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca jest stroną trzecią uzyskujemy następujące podmioty:
osoba prawna - inna niż osoba, której dane dotyczą,
osoba prawna - inna niż administrator,
osoba prawna - inna niż podmiot przetwarzający,
osoba prawna - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca nie jest stroną trzecią uzyskujemy następujące podmioty:
osoba prawna - której dane dotyczą,
osoba prawna – administrator,
osoba prawna - podmiot przetwarzający,

osoba prawna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Odbiorcą jest organ publiczny otrzymujący dane nie w ramach konkretnego postępowania, któremu jednak ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
Stroną trzecią może być organ publiczny.
inny niż osoba, której dane dotyczą,
inny niż administrator,
inny niż podmiot przetwarzający,
inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca jest stroną trzecią uzyskujemy następujące podmioty:
Odbiorcą jest organ publiczny otrzymujący dane nie w ramach konkretnego postępowania, któremu jednak ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią,
organ publiczny - inny niż osoba, której dane dotyczą,
organ publiczny - inny niż administrator,
organ publiczny - inny niż podmiot przetwarzający,
organ publiczny - inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca nie jest stroną trzecią uzyskujemy następujące podmioty:
organ publiczny - osoba, której dane dotyczą,
organ publiczny – administrator,
organ publiczny - podmiot przetwarzający,
organ publiczny - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Odbiorcą jest jednostka której ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
Stroną trzecią może być jednostka.
inna niż osoba, której dane dotyczą
inna niż administrator
inna niż podmiot przetwarzający

inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca jest stroną trzecią uzyskujemy następujące podmioty:
jednostka - inna niż osoba, której dane dotyczą,
jednostka - inna niż administrator,
jednostka - inna niż podmiot przetwarzający,
jednostka - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca nie jest stroną trzecią uzyskujemy następujące podmioty:
jednostka - osoba, której dane dotyczą,
jednostka – administrator,
jednostka - podmiot przetwarzający,
jednostka - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Odbiorcą jest inny podmiot któremu ujawnia się dane osobowe niezależnie od tego czy jest stroną trzecią.
Stroną trzecią może być podmiot
inny niż osoba, której dane dotyczą,
inny niż administrator,
inny niż podmiot przetwarzający,
inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca jest stroną trzecią uzyskujemy następujące podmioty:
podmiot - inna niż osoba, której dane dotyczą,
podmiot - inna niż administrator,
podmiot - inna niż podmiot przetwarzający,
podmiot - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Przyjmując, że odbiorca nie jest stroną trzecią uzyskujemy następujące podmioty:
podmiot - osoba, której dane dotyczą,
podmiot - administrator,
podmiot - podmiot przetwarzający,
podmiot - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

W wyniku zestawiania pojęć otrzymujemy 40 podmiotów, które teoretycznie mieszczą się w pojęciu odbiorcy. Najpierw, poniżej, pojęcia te zestawiam, w zestawieniu: „Teoretyczna lista odbiorców" – w ten sposób uzyskuję roboczą listę odbiorców, która dalej podlega obróbce. Niżej jeszcze, w kolejnym zestawieniu: „Teoretyczna lista odbiorców z komentarzami", komentuję poszczególne podmioty i eliminuję niektóre, a niżej jeszcze proponuję „Ostateczną listę odbiorców", którą umieszczam też na początku komentarza do przepisu jako Komentarz. w nazwach podmiotów, dla jasności, w tym graficznej, wywodu, pomijam słowa: „któremu ujawnia się dane osobowe"

3. Art. 4 pkt 9. Uwagi
3.1. Art. 4 pkt 9. Uwaga 1. Teoretyczna lista odbiorców

- osoba fizyczna inna niż osoba, której dane dotyczą
- osoba fizyczna inna niż administrator
- osoba fizyczna inna niż podmiot przetwarzający
- osoba fizyczna inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- osoba fizyczna - której dane dotyczą
- osoba fizyczna - administrator
- osoba fizyczna - podmiot przetwarzający
- osoba fizyczna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający
- osoba prawna - inna niż osoba, której dane dotyczą
- osoba prawna - inna niż administrator
- osoba prawna - inna niż podmiot przetwarzający
- osoba prawna - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- osoba prawna - której dane dotyczą

- osoba prawna - administrator
- osoba prawna - podmiot przetwarzający
- osoba prawna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż osoba, której dane dotyczą
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż administrator
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż podmiot przetwarzający
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - osoba, której dane dotyczą
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - administrator
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - podmiot przetwarzający
- organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- jednostka - inna niż osoba, której dane dotyczą
- jednostka - inna niż administrator
- jednostka - inna niż podmiot przetwarzający
- jednostka - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- jednostka - osoba, której dane dotyczą
- jednostka - administrator
- jednostka - podmiot przetwarzający
- jednostka - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- podmiot - inna niż osoba, której dane dotyczą
- podmiot - inna niż administrator
- podmiot - inna niż podmiot przetwarzający
- podmiot - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
- podmiot - osoba, której dane dotyczą
- podmiot - administrator

- podmiot - podmiot przetwarzający
- podmiot - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

3.2. Art. 4 pkt 9. Uwaga 2.
Teoretyczna lista odbiorców z komentarzami

- **osoba fizyczna inna niż osoba, której dane dotyczą – może być odbiorcą**
- **osoba fizyczna inna niż administrator – może być odbiorcą,**
- **osoba fizyczna inna niż podmiot przetwarzający – może być odbiorcą**
- **osoba fizyczna inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – może być odbiorcą**
- **osoba fizyczna - której dane dotyczą – nie może być odbiorcą.**

Pojęcie odbiorcy znajduje się w RODO w art. 4 pkt 9 – tam je zdefiniowano (a przynajmniej podjęto próbę sformułowania definicji).

Pojęcie odbiorcy znajduje się w art. 13 ust. 1 lit. e RODO – informowanie podczas zbierania danych od osoby, której dane dotyczą. W przepisie tym „odbiorca" znajduje się dwukrotnie, jako „ odbiorca" i jako „kategorie odbiorców". O odbiorcach i o ich kategoriach należy informować osoby, których dane dotyczą, podczas zbierania tych danych od tych osób. Są to podmioty, o których informuje się osobę, której dane dotyczą, więc absurdalne byłoby informowanie jej samej o niej samej.

Pojęcie odbiorcy znajduje się w art. 14 ust. 1 lit. e RODO – informowanie podczas zbierania danych nie od osoby, której dane dotyczą. W przepisie tym „odbiorca" znajduje się dwukrotnie, jako „odbiorca" i jako „kategorie odbiorców". O odbiorcach i o ich kategoriach należy informować osoby, których dane dotyczą, podczas zbierania tych danych nie od tych osób. W art. 14 ust. 1 lit. f RODO mowa jest o *odbiorcy w państwie trzecim lub organizacji międzynarodowej*. Są to podmioty, o których informuje się osobę, której dane dotyczą, więc absurdalne byłoby informowanie jej samej o niej samej.

Pojęcie odbiorcy znajduje się w art. 15 ust. 1 lit. c RODO – Informowanie w odpowiedzi napytanie osoby, której dane dotyczą. W przepisie tym „odbiorca" znajduje się dwukrotnie, jako „odbiorca" i jako „kategorie odbiorców" *którym dane osobowe zostały lub zostaną*

ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych. O odbiorcach i o ich kategoriach należy informować osoby, których dane dotyczą, na pytanie tych osób.

O odbiorcach jest również mowa w art. 19 RODO. Z przepisu tego wynika, że jeżeli administrator sprostuje dane osobowe, usunie dane osobowe, ograniczy przetwarzanie danych osobowych, to ma obowiązek poinformować o tym *każdego odbiorcę, któremu ujawniono dane osobowe*. Art. 19 RODO stanowi dalej, że: *Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda*. Wnioskujemy z tego, że osoba, której dane dotyczą nie jest odbiorcą, skoro administrator ma ją obowiązek informować o odbiorcach. Poza tym uważam, że osoba, której dane dotyczą nie jest odbiorcą, ponieważ z art. 13 ust. 1 lit. e RODO, z art. 14 ust. 1 lit. e RODO i z art. 15 ust. 1 lit. c RODO wynika, że osobę, której dane dotyczą należy informować (w różnych sytuacjach, w różny sposób) o odbiorcach, czyli o podmiotach, którym ujawnia się dane osobowe. Realizuje się w ten sposób zasadę przejrzystości, jednak przecież osoba, której dane dotyczą wie, jeżeli jej własne dane są jej przekazywane, czyli informowanie o niej samej jako o odbiorcy byłoby pozbawione sensu.

Z art. 58 ust. 2 lit. j RODO wynika m. in., że uprawnieniem organu nadzorczego jest *nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim*. Zakazanie przepływu danych do osoby, której dane dotyczą, w jakimkolwiek państwie, nie wydaje się celowe. Jeżeli osoba, której dane dotyczą pragnie swoje dane otrzymać, upublicznić itd., to nic nie stoi na przeszkodzie by to uczyniła.

Z art. 83 ust. 5 lit. c RODO wynika zagrożenie karą administracyjną za naruszenie przepisów dotyczących *przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej (...)* – nie wydaje się celowe by karać administratora za przekazywanie danych osobowych osobie, której dane dotyczą.

- **osoba fizyczna – administrator – nie może być odbiorcą**. Wewnątrz struktury ADO odbywają się czynności na danych, jednak wszystkie one odbywają się wewnątrz tej struktury. Przypominam, że odbiorca to podmiot (jaki dokładnie to ustalam właśnie), któremu ujawnia się dane osobowe. Koncepcja, że administrator ujawnia dane sam sobie jest absurdalna. Jeżeli administrator jakieś dane zna, to niemożebne jest by je sobie ujawnił.

- **osoba fizyczna - podmiot przetwarzający – Podmiot przetwarzający nie może być** odbiorcą, tu mam wątpliwości, jednak niewielkie. Podmiot przetwarzający *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora*, odbiorca *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe* co prawda dalej definicja odbiorcy stanowi: *niezależnie od tego, czy jest stroną trzecią*, ale nie przesądza to wcale o tym jakoby podmiot przetwarzający miał być odbiorcą. Otóż uważam, że słowa *niezależnie od tego, czy jest stroną trzecią* należy interpretować tak, że dla bycia odbiorcą nieważne jest to czy jest on stroną trzecią, bycie stroną trzecią nie wpływa na bycie odbiorcą. Pomijając zatem ten czynnik należy rozpatrzyć inne. Z cytowanych fragmentów definicji wynika, że podmiot przetwarzający *przetwarza dane osobowe w imieniu administratora* zaś odbiorca to podmiot któremu *ujawnia się dane osobowe*. Oczywiście można uparcie twierdzić, że odbiorcy najpierw ujawnia się dane, a potem on je w imieniu administratora przetwarza, jednak widniejące obok siebie przepisy opisują dwa różne podmioty. Podmioty te są inaczej zdefiniowane, więc utożsamianie ich ze sobą jest, moim zdaniem, interpretacją contra legem. Z teoretycznego punktu widzenia, podmiot przetwarzający i odbiorca są inaczej zdefiniowani, utożsamienie tych podmiotów złamałoby zakaz wykładni synonimicznej[359]. Zasada ta jest przejawem zasady niesprzeczności, czyli fundamentu rozważań naukowych, a na dobrą sprawę jakichkolwiek.
- **osoba fizyczna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – nie może być odbiorcą**. Osoby upoważnione do przetwarzania danych osobowych przez administratora są niejako częścią administratora, jeżeli administrator ujawnia im dane, to ujawnia je sobie sam, ciężko zatem byłoby mówić o ujawnianiu danych osobowych czy o ich otrzymywaniu, w odniesieniu do tych osób.
- **osoba prawna - inna niż osoba, której dane dotyczą – może być odbiorcą**
- **osoba prawna - innaniż administrator – może być odbiorcą**

[359] L. Morawski, *op. cit.* s. 103.

- **osoba prawna - inna niż podmiot przetwarzający – może być odbiorcą**
- **osoba prawna - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – może być odbiorcą**, z tym, że należy pamiętać, że osoby prawne nie są upoważniane z zasady
- **osoba prawna - której dane dotyczą – nie może być odbiorcą**. Jeżeli dane dotyczą osoby prawnej, to nie są to dane osobowe, więc nie można tu mówić o byciu odbiorcą. Podmiot poza zakresem RODO.
- **osoba prawna – administrator. – nie może być odbiorcą.** Koncepcja, że administrator ujawnia dane sam sobie jest absurdalna.
- **osoba prawna - podmiot przetwarzający – nie może być odbiorcą** – rozważania powyżej.
- **osoba prawna - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – nie może być odbiorcą** – osoby prawnej nie można upoważnić do przetwarzania danych osobowych, można jej powierzyć przetwarzanie, można udostępnić dane, ale upoważnić się nie da z uwagi na art. 32 ust. 4 RODO „(...) każda osoba fizyczna działająca z upoważnienia (...)"
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż osoba, której dane dotyczą – jest odbiorcą.** Tu w zasadzie należałoby odrzucić ten podmiot, bo organ to organ, nie osoba fizyczna, ale dla wywodu nie ma to większego znaczenia.
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż administrator - jest odbiorcą**
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż podmiot przetwarzający – jest odbiorcą**
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – jest odbiorcą.** Tu w zasadzie należałoby odrzucić ten podmiot, bo organ to organ, nie osoba fizyczna, ale dla wywodu nie ma to większego znaczenia.
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - osoba, której dane dotyczą – nie jest odbiorcą**, podmiot nieistniejący. Organ to nie osoba.

- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania – administrator – nie jest odbiorcą** – Koncepcja, że administrator ujawnia dane sam sobie jest absurdalna.
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - podmiot przetwarzający – nie jest odbiorcą** – rozważania powyżej.
- **organ publiczny otrzymujący dane nie w ramach konkretnego postępowania - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – nie jest odbiorcą**, podmiot nieistniejący. Organ to nie osoba.
- **jednostka - inna niż osoba, której dane dotyczą – jest odbiorcą**
- **jednostka - inna niż administrator – jest odbiorcą**
- **jednostka - inna niż podmiot przetwarzający – jest odbiorcą**
- **jednostka - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot - przetwarzający – jest odbiorcą.**
- **jednostka - osoba, której dane dotyczą – nie jest odbiorcą.** Rozważania wyżej.
- **jednostka – administrator – nie jest odbiorcą** – Koncepcja, że administrator ujawnia dane sam sobie jest absurdalna.
- **jednostka - podmiot przetwarzający – nie jest odbiorcą** – rozważania powyżej.
- **jednostka - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – nie jest odbiorcą** - jednostki, czymkolwiek jest, nie można upoważnić do przetwarzania danych osobowych, można jej powierzyć przetwarzanie, można udostępnić dane, ale upoważnić się nie da z uwagi na art. 32 ust. 4 RODO „(...) każda osoba fizyczna działająca z upoważnienia (...)".
- **podmiot - inna niż osoba, której dane dotyczą – jest odbiorcą**
- **podmiot - inna niż administrator - jest odbiorcą**
- **podmiot - inna niż podmiot przetwarzający - jest odbiorcą**
- **podmiot - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający – jest odbiorcą**
- **podmiot - osoba, której dane dotyczą – nie jest odbiorcą** – podmiot nieistniejący
- **podmiot - administrator – nie jest odbiorcą** – Koncepcja, że administrator ujawnia dane sam sobie jest absurdalna.

- **podmiot - podmiot przetwarzający – nie jest odbiorcą** – rozważania powyżej.
- **podmiot - osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający. – nie jest odbiorcą-** jednostki, czymkolwiek jest, nie można upoważnić do przetwarzania danych osobowych, można jej powierzyć przetwarzanie, można udostępnić dane, ale upoważnić się nie da z uwagi na art. 32 ust. 4 RODO „(...) każda osoba fizyczna działająca z upoważnienia (...)".

3.3. Art. 4 pkt 9. Uwaga 3. Ostateczna lista odbiorców

Ostateczną listę odbiorców umieściłem w komentarzu *1. Art. Art. 4 pkt 9. Komentarz*.

3.4. Art. 4 pkt 9. Uwaga 4. Tytuł prawny do ujawnienia danych osobowych odbiorcy

Nie zgadzam się z P. Litwińskim, P. Bartą i M. Kaweckim, którzy twierdzą[360] że nie ma znaczenia na drodze jakiego tytułu prawnego dane osobowe są ujawniane odbiorcy. Tytuł prawny na podstawie którego dane osobowe są ujawniane odbiorcy jest istotny ponieważ z punktu widzenia RODO to właśnie tytuł prawny statuuje kolejne podmioty i odróżnia je od siebie. Inny tytuł prawny do przetwarzania danych osobowych ma administrator (danych), inny tytuł prawny do przetwarzania danych osobowych ma podmiot przetwarzający, jeszcze inny tytuł prawny ma osoba upoważniona do przetwarzania.

3.5. Art. 4 pkt 9. Uwaga 5. Odbiorca a podmiot przetwarzający

Zupełnie nie zgadzam się z P. Litwińskim, P. Bartą i M. Kaweckim, którzy twierdzą że „podmiot przetwarzający powinien zostać uznany na gruncie komentowanego przepisu za odbiorcę danych"[361]. Należy zwrócić uwagę na fakt że przeciwko utożsamianiu odbiorcy

[360] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 226.

[361] P. Litwiński, P. Barta, M. Kawecki, *loc. cit.*

z podmiotem przetwarzającym przemawiają co najmniej **dwa argumenty**. **Pierwszy argument** jest taki że odbiorcę od podmiotu przetwarzającego odróżnia właśnie tytuł prawny legalizujący dostęp do danych. Odbiorca uzyskuje dostęp do danych z mocy prawa. Podmiot przetwarzający uzyskuje dostęp do danych z mocy umowy. Innymi słowy, w relacji: administrator danych a odbiorca, konieczna jest podstawa prawna która legalizuje przetwarzanie danych przez odbiorcę oceniana wobec odbiorcy z punktu widzenia pierwotnego administratora danych. Podmiot przetwarzający uzyskuje dostęp do danych z mocy umowy między administratorem danych a podmiotem przetwarzającym właśnie. Innymi słowy w relacji administrator danych a podmiot przetwarzający, podstawą prawną która legalizuje przetwarzanie danych przez podmiot przetwarzający jest umowa między administratorem danych a podmiotem przetwarzającym Przesłanki legalizujące przetwarzanie danych w przypadku przetwarzania ich przez podmiot przetwarzający nie są oceniane dla podmiotu przetwarzającego podmiot przetwarzający przetwarza dane osobowe zgodnie z prawem ponieważ łączy go z administratorem danych umowa powierzenia przetwarzania a przesłanki legalizujące oceniane są wobec administratora (danych).

Ostrożne stanowisko w tej kwestii prezentuje M. Sakowska-Baryła, która relacjonuje stanowiska doktryny dotyczące kwestii czy podmiot przetwarzający jest odbiorcą. Są te stanowiska dwa, część doktryny uważa, że podmiot przetwarzający odbiorcą jest, część, że wręcz przeciwnie. Niezwykle cenna jest uwaga M. Sakowskiej-Baryły, która wskazuje, że w art. 46 ust. 3 lit. a RODO podmiot przetwarzający występuje obok odbiorcy.[362] W kontekście tego właśnie spostrzeżenia, niepojęte dla mnie jest zdanie jego autorki, która odnosząc się do własnego spostrzeżenia twierdzi: *Nie oznacza to jednak, że brzmienie przytoczonego przepisu niweczy koncepcję, według której odbiorca to także podmiot przetwarzający*[363]. Otóż uważam, że jak najbardziej oznacza. Prawodawca jest racjonalny. Prawodawca wie co pisze i to co pisze, pisze w sposób celowy, celowy i racjonalny. Skoro prawodawca wymienia podmiot przetwarzający obok odbiorcy, to czyni to racjonalnie i celowo. Uważam, że można a wręcz należy tu

[362] M. Sakowska-Baryła w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018. s. 111.

[363] M. Sakowska-Baryła, *loc. cit.*

strawestować słowa M. Sakowskiej-Baryły następująco: fakt, że w art. 46 ust. 3 lit. a RODO, podmiot przetwarzający występuje obok odbiorcy danych osobowych oznacza, że niweczy to koncepcję, według której odbiorca to także podmiot przetwarzający. To właśnie jest, moim zdaniem **przejawem drugiego argumentu**, który przemawia za tym, że odbiorca i podmiot przetwarzający to inne podmioty. Skoro racjonalny prawodawca[364] wymienia dwa podmioty obok siebie i to w tym samym przepisie, o którym piszę wyżej, przy omawianiu słów M. Sakowskiej-Baryły, to są to na pewno inne podmioty.

Widzę tu również trzeci argument przemawiający za tym, że podmiot przetwarzający i odbiorca to inne podmioty. Argument ten bliski jest argumentowi drugiemu i wynika on z zakazu wykładni synonimicznej[365]. Skoro racjonalny prawodawca używa dwóch nazw, to czyni to zapewne dla nazwania dwóch różnych kategorii podmiotów i skoro tak, to nie wolno na drodze interpretacji tych kategorii podmiotów utożsamiać ze sobą.

4. Art. 4 pkt 9. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 9 RODO definiuje **odbiorcę**, zatem zgodnie z dyrektywą języka prawnego[366], każdy kto interpretuje RODO powinien rozumieć pojęcie „***odbiorca***" tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie ***odbiorca*** tak jest ono zdefiniowane w art. 4 pkt. 8 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia ***odbiorca*** zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

---

[364] L. Morawski, *op. cit.* s. 159-162.

[365] L. Morawski, *op. cit.* s. 103.

[366] L. Morawski, *op. cit.* s. 93-99, zwłaszcza 95.

5. Art. 4 pkt 9. Konkretyzacja zasad

Art. 4 pkt 9 sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Odbiorca przetwarza dane w oparciu o własną podstawę prawną. Udostępnianie danych jest przetwarzaniem, o czym należy pamiętać. Jeżeli administrator danych udostępnia odbiorcy dane osobowe, to musi dbać on o to by udostępnienie odbyło się w oparciu o konkretną podstawę prawną. Należy przy tym pamiętać, że jeżeli potencjalny, przyszły odbiorca posiada podstawę prawną do przetwarzania danych osobowych, które posiada pierwotny administrator, to nie oznacza to wcale, że pierwotny administrator powinien odbiorcy udostępnić dane osobowe. Konieczny jest jeszcze element pośredni, łączący, czyli podstawa prawna do udostepnienia danych osobowych przez danego administratora (danych) danemu odbiorcy.

Realizacji **zasady rzetelności**. Realizując obowiązki wynikające z art. 13 RODO, z art. 14 RODO i z art. 15 RODO, administrator (danych) ma obowiązek informować o odbiorcach. Informowanie o odbiorcach sprzyja realizacji zasady rzetelności.

Realizacji **zasady przejrzystości** poprzez informowanie o odbiorcach. Informowanie o odbiorcach sprzyja realizacji zasady przejrzystości.

Realizacji **zasady ograniczenia celu**, poprzez dbanie przez administratora danych o to by udostępnienie danych odbyło się tylko w oparciu o ważną podstawę prawną, o której piszę wyżej przy omawianiu konkretyzacji zasady zgodności z prawem. Administrator (danych) nie ma możliwości skontrolowania w jakim celu odbiorca używał będzie udostępnionych mu danych osobowych. Możliwość kontroli kończy się na etapie udostępnienia lub oczywiście nieudostępnienia danych. Właśnie dlatego, że władztwo administratora danych nad danymi kończy się w momencie ich udostępnienia, powinien on pieczołowicie dbać o podstawę prawna do udostępnienia. Jeżeli administrator danych posiada podstawę prawną do udostępnienia danych, to istnieje choć cień nadziei, ę odbiorca będzie przetwarzał dane w zgodzie z prawem, ale i w celu wynikającym z kolei z jego podstawy prawnej do przetwarzania danych osobowych.

Realizacja **zasady minimalizacji a**nalogiczna jest do realizacji zasady ograniczenia celu. Administrator (danych) dba o to by udostępnić tylko dane osobowe tylko wtedy jeżeli posiada do tego stosowną podstawę prawną.

Drugi, ważniejszy chyba nawet element związku pojęcia odbiorcy z realizacją zasady minimalizacji jest taki, że administrator (danych) powinien dbać o to by udostępniać dane w sposób zgodny z tą zasadą, czyli żeby udostępniać tylko dane w zakresie niezbędnym. Uważam, że udostępnianie danych, wyjmowanie ich niejako spod władztwa pierwotnego administratora danych, jest czynnością na tyle ryzykowną (choć konieczną), że zasadę minimalizacji należy tu rozumieć restrykcyjnie. Restrykcyjnie, czyli udostępniać dane wyłącznie w zakresie niezbędnym, nie zaś również dane adekwatne lub stosowne. Szerzej dwa rozumienia zasady minimalizacji omawiam w uwadze *3.2. Art. 5 ust. 1 lit. c. Uwaga 2. Treść zasady, podejście restrykcyjne* i w uwadze *3.3. Art. 5 ust. 1 lit. c. Uwaga 3. Treść zasady, podejście łagodne*.

Realizacja **zasady prawidłowości**. Administrator ma, wynikający z art. 19 RODO obowiązek informowania odbiorcy m.in. o sprostowaniu danych osobowych. Realizacja tego obowiązku sprzyja realizacji zasady prawidłowości.

Realizacja **zasady ograniczenia przechowywania danych**. Administrator ma, wynikający z art. 19 RODO obowiązek informowania odbiorcy m.in. o usunięciu danych lub o ograniczeniu przetwarzania. Realizacja tego obowiązku sprzyja realizacji zasady ograniczenia przechowywania danych.

Związek **zasady integralności** z definicją odbiorcy jest daleki. Jedyny jaki dostrzegam to wynikający z zasady zgodności z prawem obowiązek dbałości o to by dane osobowe udostępniane były w oparciu o odpowiednią podstawę prawną. Jeżeli dane zostają uzupełnione w oparciu o stosowną podstawę prawną, to można mieć nadzieję, że odbiorca, który posiada stosowną podstawę do uzyskania danych, zadba również o to by dane nie były modyfikowane bez stosownej podstawy prawnej.

Związek **zasady poufności**. Z definicją odbiorcy pewien jest. Otóż administrator danych musi, jak wiadomo dbać o to by dane były przetwarzane zgodnie z zasadą poufności, czyli przez osoby do tego uprawnione. Administrator danych jest o to w stanie zadbać w swojej organizacji, do pewnego stopnia również w organizacji podmiotu przetwarzającego. Na przetwarzanie danych w organizacji odbiorcy, rozumianego jako nowy administrator danych, pierwotny administrator nie ma wpływu, z pewnymi jednak zastrzeżeniami. Przede wszystkim administrator powinien udostępniać dane odbiorcom jedynie wte-

dy kiedy istnieje podstawa prawna do udostępnienia danych. Jeżeli administrator danych udostępnia dane bez takiej podstawy to niewątpliwie oprócz złamania zasady zgodności z prawem, łamie również zasadę poufności.

Grozić złamaniem zasady poufności może też niedbałe wybieranie odbiorcy. Kiedy administrator danych wybiera odbiorcę, to powinien czynić to w sposób roztropny. Oczywiście myśl ta ma sens tylko wtedy gdy administrator danych wybiera odbiorcę.

6. Art. 4 pkt 9. Postulaty de lege ferenda

6.1 Art. 4 pkt 9. Postulat 1.
Zmiana przepisu
tak by było oczywiste,
że podmiot przetwarzający jest odbiorcą

Uważam, że nie jest jasne czy do odbiorców należy zaliczyć podmioty przetwarzające. Piszę o tym w uwadze *3.5. Art. 4 pkt 9. Uwaga 5. Odbiorca a podmiot przetwarzający*. Mój, wyrażony we wskazanej uwadze, pogląd jest taki, że podmiot przetwarzający nie jest odbiorcą. Nie jest przede wszystkim dlatego, podmioty te różni podstawa przetwarzania. U podmiotu przetwarzającego podstawę przetwarzania stanowi podstawa administratora i umowa powierzenia przetwarzania, u odbiorcy podstawę przetwarzania stanowi prawo. Sama definicja odbiorcy napisana jest na tyle niejasno, że na jej podstawie nie sposób rozstrzygnąć czy podmiot przetwarzający jest odbiorcą czy nie.

Gdyby uznać, że podmiot przetwarzający nie jest odbiorcą to należałoby postawic postulat nowelizacyjny, gdyby uznac, że podmiot przetwarzający jest odbiorcą, to również należałoby postwic postulat nowelizacyjny, tyle, że inny. Na dobrą sprawę nie jest to istotne dla zjawiska ochrony danych, czy podmiot przetwarzający jest odbiorcą czy nie. Istotne nie jest ale utrudnia funkcjonowanie administratorom danych. Skoro nie wiadomo czy podmioty przetwarzajće są odbiorcami to nie wiadomo jak dokąłdnei sporządzić dokumenty wynikające z art. 13 RODO, z art. 14 RODO i z art. 15 RODO oraz RCPD. By ten patologiczny stan niepewności przerwac, przepis należy znowelizować, tak by niepewnosć została zastąpiona przez pewność.

W niniejszym postulacie, niżej, postuluje taką zmianę przepisu, by nie było wątpliwości, że podmiot przetwarzający nie jest odbiorcą.

W kolejnym postulacie *6.2. Art. 4 pkt 9. Postulat 2. Zmiana przepisu tak by było wiadomo, że podmiot przetwarzający nie jest odbiorcą*, jeszcze niżej, postuluje taką zmianę przepisu, by nie było wątpliwości, że podmiot przetwarzający jest odbiorcą.

Postuluję dodanie słów: „podmiot przetwarzający" po słowie: *jednostkę* i przed słowem *inny podmiot*. Przepis powinien zatem mieć treść: „„**odbiorca**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę, **podmiot przetwarzający** lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;". (Wytłuszczeniem i podkreśleniem zaznaczam słowa dodane do przepisu.)

6.2. Art. 4 pkt 9. Postulat 2. Zmiana przepisu tak by było oczywiste, że podmiot przetwarzający nie jest odbiorcą

Nie chcąc powtarzać rozważań z postulatu *6.1 Art. 4 pkt 9. Postulat 1. Zmiana przepisu tak by było wiadomo, że podmiot przetwarzający jest odbiorcą*, odsyłam do nich. Dla porządku powtarzam tu tylko, że uważam, że stan niepewności – przepis niejasny, powinien zostać zastąpiony stanem pewności – przepisem jasnym i zrozumiałym. Postulat, który tu stawiam nie jest mi bliski, uważam bowiem, że podmiot przetwarzający nie jest odbiorcą, jednak jest czy nie jest, jaka decyzja zapadłaby, gdyby prawodawca czytał takie rozważania, jest drugorzędne, dobrze by zapadłą jakaś, by ktoś RODO uporządkował i przyzwoicie zredagował.

W niniejszym postulacie, postuluję taką zmianę przepisu, by nie było wątpliwości, że podmiot przetwarzający nie jest odbiorcą.

Postuluję dodanie słów: „również podmioty przetwarzające nie są uważane za odbiorców" na końcu przepisu, po słowach: *stosownie do celów przetwarzania*. Przepis powinien zatem mieć treść: „„**odbiorca**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie

od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania, **<u>również podmioty przetwarzające nie są uważane za odbiorców</u>**;"

Wytłuszczeniem i podkreśleniem zaznaczam słowa dodane do przepisu.

6.2. Art. 4 pkt 9. Postulat 3.
Usunięcie z przepisu zalecenia dla organów publicznych

Komentowany przepis stanowi m.in., że: *przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania*. Wymienione w przepisie „te dane" to dane osobowe, otrzymywane przez organy publiczne w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego. Wobec tych właśnie danych przepis statuuje obowiązek, że *przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania*. Czyli te dane mają być przetwarzane zgodnie z przepisami i to zgodnie *z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania*. Lektura angielskiej wersji przepisu upewnia, że to przepisy mają być stosowne do celów przetwarzania danych – *(...) with the applicable data protection rules according to the purposes of the processing*.

Kiedy już ustalimy treść przepisu, porównując wersję polską z angielską, to musi pojawić się pewne pytanie. Pytanie o to dlaczego akurat w komentowanym przepisie prawodawca zwraca uwagę na fakt, że (nieco skracając) przetwarzania danych przez organy publiczne ma być zgodne z prawem i to zwłaszcza z (jak mniemam) zasadą ograniczenia celowego. Nie ma tu sensu relacjonować całego RODO, przypomnę jedynie, że komentowany akt prawny w żaden sposób nie wyłącza organów publicznych ze swego zakresu. W związku z tym pojawia się zagadka, dlaczego w komentowanym przepisie zwrócono uwagę na konieczność przestrzegania prawa, w tym oczywiście RODO przez organy publiczne.

Należy się zapytać czy można postawić tezę, że skoro organy publiczne mają stosować prawo, a zwłaszcza zasadę ograniczenia celowego, to może organy publiczne są zwolnione ze stosowania pozostałych zasad. Może należy zapytać o to, że skoro organy publiczne mają stosować prawo a zwłaszcza zasadę celowości to inne podmioty mają nie stosować zasady celowości. Może należy zapytać o to, czy inne podmioty niż organy publiczne mogą nie stosować prawa. Pytania te, jak i wypływające z nich wnioski są absurdalne i jako takie muszą zostać odrzucone. [367] Stawiam je tu tylko jako swoistą prowokację, mającą na celu zobrazowanie faktu, że nie wiadomo po co w przepisie umieszczono słowa: „przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania". Słowa te nic nie wnoszą, a prowadzić mogą do absurdalnych wniosków.

Postuluję usunięcie z przepisu słów: *przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania*. Przepis powinien zatem mieć treść: „**odbiorca**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; ~~przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania~~;"

Czcionką przekreśloną zaznaczam słowa których usunięcie z przepisu postuluję.

[367] L. Morawski *op. cit.* s. 150.

Artykuł 4. pkt 10 RODO

„strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

1.1. Art. 5 pkt 10. Komentarz I

Strony trzecie, które jednocześnie mogą stać się odbiorcami wymieniam poniżej.

- osoba fizyczna, której ujawnia się dane osobowe, inna niż osoba, której dane dotyczą
- osoba fizyczna, której ujawnia się dane osobowe, inna niż podmiot przetwarzający
- osoba fizyczna, której ujawnia się dane osobowe, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający

-- **przykładem** jaki tu można podać są osoby, którym udostępnia się dane osobowe na podstawie upoważnienia do dostępu do dokumentacji medycznej lub do informowania ich o stanie zdrowia na podstawie upoważnienia pacjenta

- osoba prawna, której ujawnia się dane osobowe, inna niż podmiot przetwarzający
- osoba prawna, której ujawnia się dane osobowe, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

-- podobny **przykład** jak wyżej – firma ubezpieczeniowa upoważniona przez ubezpieczonego do dostępu do jego danych medycznych.

- organ publiczny otrzymujący dane poza postępowaniem, któremu ujawnia się dane osobowe, - inny niż administrator
- organ publiczny otrzymujący dane poza postępowaniem, któremu ujawnia się dane osobowe, - inny niż podmiot przetwarzający

- organ publiczny otrzymujący dane poza postępowaniem, któremu ujawnia się dane osobowe, - inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
-- **przykład**: Minister Zdrowia otrzymujący tzw. MZki, Inspektor Sanitarny, do którego zgłaszamy zachorowanie np. na grypę

- jednostka, której ujawnia się dane osobowe, - inna niż podmiot przetwarzający
- jednostka, której ujawnia się dane osobowe, - inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

- podmiot, któremu ujawnia się dane osobowe,- inna niż podmiot przetwarzający
- podmiot, któremu ujawnia się dane osobowe,- inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Strony trzecie, które nie są odbiorcami wymieniam poniżej.
- osoba fizyczna, której nie ujawnia się danych osobowych, inna niż osoba, której dane dotyczą
- osoba fizyczna, której nie ujawnia się danych osobowych, inna niż podmiot przetwarzający
- osoba fizyczna, której nie ujawnia się danych osobowych, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający
-- **przykładem** jaki tu jest możliwy, są osoby w żaden sposób nie przetwarzające danych, osoba przebywająca na terenie siedziby ADO, ale nie będąca którąś z wymienionych, np. ktoś towarzyszy interesantowi i nie słyszy danych – czeka na korytarzu, osoba, która weszła na teren ADO by skorzystać z toalety czy by coś ukraść, osoba, która idzie za oknem i nie wie nawet o istnieniu ADO (ale tu możemy być poza zakresem RODO – mam tu wątpliwość).

- osoba prawna, której nie ujawnia się danych osobowych, inna niż podmiot przetwarzający

- osoba prawna, której nie ujawnia się danych osobowych, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
-- **przykład** dość prosty – osoby prawne, którym nie ujawnia się danych osobowych.

- organ publiczny któremu nie ujawnia się danych osobowych, inny niż administrator
- organ publiczny któremu nie ujawnia się danych osobowych, inny niż podmiot przetwarzający
- organ publiczny któremu nie ujawnia się danych osobowych, inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
-- **przykład** - organy, którym nie ujawnia się danych z punktu widzenia danego ADO.

- jednostka, której nie ujawnia się danych osobowych, inna niż podmiot przetwarzający
- jednostka, której nie ujawnia się danych osobowych, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.
-- podmiot nie posiadający osobowości prawnej, któremu dany ADO nie ujawnia danych osobowych – dowolna spółka cywilna

- podmiot , któremu nie ujawnia się danych osobowych, inna niż podmiot przetwarzający
- podmiot , któremu nie ujawnia się danych osobowych, inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

1.2. Art. 5 pkt 10. Komentarz II

Stroną trzecią jest osoba, która nie może przetwarzać danych, ponieważ nie jest osobą, której dane dotyczą lub nie jest osobą upoważnioną do przetwarzania danych.

Jeżeli stronie trzeciej zostaje nadane upoważnienie, to przestaje być ona osobą trzecia i staje się osobą upoważnioną.

Jeżeli osoba prawna lub organ publiczny lub jednostka nie są administratorem ani podmiotem przetwarzającym to są stronami

trzecimi. Jeżeli osoba prawna lub organ publiczny lub jednostka, które są stronami trzecimi wchodzą w posiadanie danych osobowych, to stają się administratorem lub podmiotem przetwarzającym i jednocześnie przestają być stronami trzecimi.

2.1. Art. 5 pkt 10. Analiza

Ze słów wytłuszczonych w przepisie: „**oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą**, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe" należy wnioskować, że stroną trzecią może być każdy z podmiotów wymienionych w przepisie, pod warunkiem spełnienia pozostałych wymienionych w przepisie warunków.
Stroną trzecią może być osoba fizyczna.
Stroną trzecią może być osoba prawna.
Stroną trzecią może być organ publiczny.
Stroną trzecią może być jednostka.
Stroną trzecią może być podmiot
inny niż osoba, której dane dotyczą
inny niż administrator
inny niż podmiot przetwarzający
inny niż osoby upoważnione przez administratora lub podmiot przetwarzający.

Uważam, że ze względu na konstrukcję i na treść przepisu, należy go rozumieć w sposób wskazany poniżej.

Stroną trzecią może być osoba fizyczna.
inna niż osoba, której dane dotyczą
inna niż administrator
inna niż podmiot przetwarzający
inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Stroną trzecią może być osoba prawna.
inna niż osoba, której dane dotyczą
inna niż administrator
inna niż podmiot przetwarzający

inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Stroną trzecią może być organ publiczny.
inny niż osoba, której dane dotyczą
inny niż administrator
inny niż podmiot przetwarzający
inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Stroną trzecią może być jednostka.
inna niż osoba, której dane dotyczą
inna niż administrator
inna niż podmiot przetwarzający
inna niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

Stroną trzecią może być podmiot
inny niż osoba, której dane dotyczą
inny niż administrator
inny niż podmiot przetwarzający
inny niż osoby upoważnione do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający.

2.2. Art. 5 pkt 10. Analiza II

Z uwagi na niejasność komentowanej definicji, analizuję ją poniżej dodatkowo metodą odmienną niż etapowa analiza semantyczna.

Analizowana definicja brzmi: „„**strona trzecia**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;”.

Analiza definicji pozwala ustalić zależności zachodzące między poszczególnymi jej elementami. Rozpisując definicję uzyskujemy efekt jak poniżej.
„strona trzecia” to
osoba fizyczna inna niż osoba, której dane dotyczą
lub

osoba fizyczna inna niż osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe
lub
osoba prawna inna niż administrator lub inna niż podmiot przetwarzający,
lub
organ publiczny inny niż administrator lub inny niż podmiot przetwarzający
lub
jednostka inna niż administrator lub inna niż podmiot przetwarzający
lub
podmiot inny niż administrator, lub inny niż podmiot przetwarzający.

Ustalenie, że strona trzecia to m.in.
osoba fizyczna inna niż osoba, której dane dotyczą
lub
osoba fizyczna inna niż osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe
prowadzi do wniosku, że strona trzecia to
osoba fizyczna inna niż osoby której dane dotyczą lub inna niż osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Zastanowienie się nad tym kto może przetwarzać dane osobowe prowadzi do wniosku, że dane osobowe może przetwarzać osoba, której dane dotyczą oraz że dane osobowe mogą przetwarzać osoby upoważnione przez administratora lub podmiot przetwarzający.

Stroną trzecią jest zatem osoba, która nie może przetwarzać danych, ponieważ nie jest osobą, której dane dotyczą lub nie jest osobą upoważnioną do przetwarzania danych. Osobą, której dane dotyczą się jest albo nie. Osobą upoważnioną można się stać w momencie nadania upoważnienia. Jeżeli osobie trzeciej zostaje nadane upoważnienie, to przestaje być ona osobą trzecia i staje się osobą upoważnioną.

Jednocześnie ustalenie, że strona trzecia to m.in.
osoba prawna inna niż administrator lub inna niż podmiot przetwarzający,
lub
organ publiczny inny niż administrator lub inny niż podmiot przetwarzający

lub
jednostka inna niż administrator lub inna niż podmiot przetwarzający
lub
podmiot inny niż administrator, lub inny niż podmiot przetwarzający.
prowadzi do wniosku, że strona trzecia to
osoba prawna lub organ publiczny lub jednostka lub podmiot inne niż administrator lub podmiot przetwarzający.

Osoba prawna lub organ publiczny lub jednostka mogą być administratorem lub podmiotem przetwarzającym lub mogą nie być ani administratorem ani podmiotem przetwarzającym.

Jeżeli osoba prawna lub organ publiczny lub jednostka nie są administratorem ani podmiotem przetwarzającym to są osobami trzecimi. Jeżeli osoba prawna lub organ publiczny lub jednostka, które są osobami trzecimi wchodzą w posiadanie danych osobowych, to stają się administratorem lub podmiotem przetwarzającym i jednocześnie przestają być stronami trzecimi.

3. Art. 4 pkt 10. Uwagi

3.1. Art. 4 pkt 10. Uwaga 1.
Brak uprawnień do przetwarzania danych osobowych jako cecha konstytutywna osoby trzeciej

W świetle rozważań prowadzonych w analizie (2.1. Art. 5 pkt 10. Analiza) i w analizie (2.2. Art. 5 pkt 10. Analiza II) należy zgodzić się ze zdaniem P. Litwińskiego, P. Barty i M. Kaweckiego, którzy twierdzą, że „Strona trzecia jest zbiorczą kategorią podmiotów, które nie mogą wywodzić swojego uprawnienia do dostępu do danych osobowych z faktu, że dane osobowe dotyczą tej właśnie osoby (osoba której dane dotyczą), z faktu decydowania o celach i sposobach przetwarzania danych osobowych (administrator danych), z faktu działania w imieniu lub z upoważnienia administratora danych (podmiot przetwarzający i osoba upoważniona).”[368]

[368] P. Litwiński, P. Barta, M. Kawecki. w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 227-228.

Z myśli cytowanych autorów wyprowadzić można myśl lapidarniejszą, że strona trzecia to podmiot lub osoba, który nie ma uprawnienia do dostępu do danych osobowych.

4. Art. 4 pkt 10. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 10 RODO definiuje **stronę trzecią**, zatem zgodnie z dyrektywą języka prawnego[369], każdy kto interpretuje RODO powinien rozumieć pojęcie „**strona trzecia**" tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „**strona trzecia**" tak jest ono zdefiniowane w art. 4 pkt. 8 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „**strona trzecia**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. Art. 4 pkt 10. Konkretyzacja zasady

Zasada zgodności z prawem. Strona trzecia to ktoś kto nie ma uprawnień do dostępu do danych osobowych, zatem i do przetwarzania danych osobowych. Ustalenie kto w danym stanie faktycznym jest stroną trzecią, współgra z realizacją zasady.

Zasada rzetelności. Związek strony trzeciej z zasadą rzetelności jest daleki. Jeżeli administrator danych przetwarza dane osobowe i realizuje obowiązek informacyjny to osoba której dane dotyczą wie, że dany podmiot jest administratorem jej danych więc zasada rzetelności jest zrealizowana. Jednocześnie należy zwrócić uwagę że wobec takiego administratora osoba ta nie jest stroną trzecią, choć trzeba tu dodać, że fakt czy dany administrator zrealizował obowiązek informacyjny z art. 13 ROD nie ma wpływu na to, że osoby, których dane przetwarza nie są stronami trzecimi.

[369] L. Morawski, *op. cit.* s. 93-99, zwłaszcza 95.

Zasada przejrzystości. Związek zasady przejrzystości z definicją strony trzeciej jest bardzo daleki. Administrator danych który realizuje obowiązek informacyjny wynikający z art. 13 RODO, w sytuacji kiedy przetwarzanie oparte jest o przesłankę wynikającą z artykułu 6 ust. 1 lit. f RODO czyli w oparciu o prawnie uzasadniony interes administratora lub strony trzciej, ma obowiązek o tym poinformować osobę, której dane dotyczą. Tym samym administrator taki musi poinformować osobę której dane dotyczą o jaką to chodzi osobę trzecią której uzasadniony interes jest realizowany.

Zasada ograniczenia celu. Jeżeli administrator (danych) przetwarza dane osobowe zgodnie z zasadą ograniczenia celu to w pewnym momencie ten administrator przestaje konkretne dane przetwarzać (chyba, że ma obowiązek, lub wolno mu, przetwarzać je wieczyście). Jeżeli administrator danych nie ma już danych osobowych pewnych osób, to osoby te przestają z jego punktu widzenia być osobami których dane dotyczą, bowiem on już tych danych nie ma, stają się natomiast stronami trzecimi.

Zasada prawidłowości. Związek zasady prawidłowości z definicją strony trzeciej jest bardzo daleki można go jednak wyprowadzić. Na podstawie art. 15 RODO na administratorze danych osobowych spoczywają pewne obowiązki wobec osób których dane dotyczą. Osoby takie mogą najpierw ustalić czy administrator ten przetwarza dotyczące ich dane osobowe, następnie zaś mogą pytać o kolejne wynikające z art. 15 RODO szczegóły dotyczące przetwarzania danych osobowych. Jeżeli jednak już na etapie pytania o to czy administrator przetwarza dane osobowe danej osoby okazuje się, że administrator nie przetwarza danych osobowych tej osoby, to pozostałe obowiązki wynikające z art. 15 RODO nie spoczywają w danej relacji z tą konkretną osobą, na tym konkretnym administratorze. Osoba ta nie jest osobą której dane dotyczą. z punktu widzenia tego administratora osoba ta jest stroną trzecią.

Zasada ograniczenia przechowywania. Związek zasady ograniczenia przechowywania z definicją strony trzeciej jest analogiczny do związku zasady ograniczenia celu z definicją strony trzeciej. Administrator danych przestaje w pewnym momencie przetwarzać dane osobowe osoby której dane dotyczą, szanuje bowiem zasadę ograniczenia przechowywania, tym samym z punktu widzenia tego administratora osoba taka staje się stroną trzecią. Osoba taka może być osobą upoważnioną przez danego administratora, wtedy nie jest stroną

trzecią, nie jest ona jednak stroną trzecia na podstawie innej relacji, a to relacji upoważnienia nie zaś na podstawie relacji wynikającej z faktu bycia osobą, której dane dotyczą.

Zasada integralności. Osoby lub podmioty mające charakter strony trzeciej nie powinny mieć dostępu do danych i oczywiście nie powinny mieć możliwości tych danych modyfikować, zmieniać, usuwać, co sprzyja realizacji zasady integralności

Zasada poufności. Zabezpieczenie danych osobowych przed dostępem osób lub podmiotów mających charakter strony trzeciej można do pewnego stopnia utożsamić z realizacją zasady poufności. Dane osobowe przetwarzane w sposób poufny to dane osobowe przetwarzane przez osoby lub podmioty inne niż strony trzecie.

Zasada odpowiedzialności administratora danych. Administrator danych osobowych jest odpowiedzialny za realizację zasad wynikających z artykułu 5 ust. 1 RODO. Zasady te mają charakter obowiązków zaś z obowiązków tych wynikają uprawnienia osób których dane dotyczą. Naruszenie tych uprawnień może skutkować odpowiedzialnością administracyjną lub cywilną, podkreślenia jednak wymaga że administrator danych osobowych może naruszyć uprawnienia osób, których dane dotyczą, zaś nie może naruszyć uprawnień stron trzecich, nawet jeżeli są osobami fizycznymi, bowiem ich danych osobowych administrator taki zwykle nie przetwarza. Jeżeli administrator przetwarza dane osobowe konkretnej osoby fizycznej, to osoba ta nie jest już z punktu widzenia tego administratora stroną trzecią, zaś jest osobą której dane dotyczą.

Zasada rozliczalności. Administrator danych osobowych ma obowiązek wykazać że realizuje zasady przetwarzania danych wynikające z artykułu 5 ust. 1 RODO, co jest jego obowiązkiem a tym samym uprawnieniem osób których dane dotyczą, nie jest zaś uprawnieniem stron trzecich.

6. Art. Art. 4 pkt 10. Postulaty de lege ferenda

6.1 Art. 4 pkt 10. Postulat 1.

Propozycja nowej treści przepisu

Nie mogę oprzeć się wrażeniu niejasności komentowanego przepisu. Fakt że komentowany przepis jest niejasny to dopiero jedna strona problemu. Drugą stronę problemu stanowi fakt że stronę trzecią zdefiniowaną w komentowanym przepisie, można zdefiniować w spo-

sób dużo prostszy. Wydaje się, że najlepiej byłoby znowelizować przepis w sposób wywodzący się z myśli P. Litwińskiego, P. Barty i M. Kaweckiego, do której odwołuję się w uwadze (3.1. Art. 4 pkt 10. Uwaga 1. Brak uprawnień do przetwarzania danych osobowych jako cecha konstytutywna osoby trzeciej.).

W związku z powyższym postuluję aby przepis znowelizowano w sposób : „„strona trzecia" oznacza **podmiot lub** osobę ~~fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby,~~ które ~~z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe~~ **nie mają uprawnienia do dostępu do danych osobowych**" (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Przepis po nowelizacji miałby postać:
„„strona trzecia" oznacza podmiot lub osobę, nie mają uprawnienia do dostępu do danych osobowych"

Artykuł 4. pkt 11 RODO

„zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

1. Art. 4. pkt 11. Komentarz

Przepis dotyczy zgody osoby, której dane dotyczą.
Zgoda, której dotyczy przepis jest wyrażana przez osobę, której dane dotyczą.
Przepis definiuje zgodę osoby, której dane dotyczą.
Zgoda oznacza okazanie woli spełniające cztery warunki wymienione w przepisie.
Pierwszym warunkiem jest dobrowolność zgody.
Drugim warunkiem jest konkretność zgody.
Trzecim warunkiem jest świadomość zgody (złożenie jest w warunkach świadomości osoby, której dane dotyczą).
Czwartym warunkiem jest jednoznaczność zgody.

Pierwszym warunkiem, który musi spełnić okazanie woli jest dobrowolność. Osoba, której dane dotyczą wyraża zgodę dobrowolnie jeżeli sama podejmuje decyzję o jej wyrażeniu.
Drugim warunkiem, który musi spełnić okazanie woli jest by okazanie woli było konkretne.
Konkretne okazanie woli to okazanie woli, którego nie można pomylić z niczym innym.
Trzecim warunkiem, który musi spełnić okazanie woli jest by okazanie woli było świadome. Świadomość, jako cecha oświadczenia woli jest analogiczna do dobrowolności oświadczenia woli.
Czwartym warunkiem, który musi spełnić okazanie woli jest by okazanie woli było jednoznaczne.

Dla ważności zgody konieczne jest by zaszło okazanie, przejawienie woli osoby, której dane dotyczą. Okazanie woli przyzwolenia na

przetwarzanie danych osobowych musi dla swej ważności mieć formę oświadczenia lub wyraźnego działania potwierdzającego.
Działania potwierdzającego - nie wystarczy zatem, że osoba, której dane dotyczą dostarczy administratorowi swoje dane osobowe. Jest to co prawda działanie ale nie działanie potwierdzające. Fakt, że osoba której dane dotyczą przyzwoliła działaniem na ich przetwarzanie powinien wynikać z jej czynności (działania) w sposób oczywisty.

2. Art. 4. pkt 11. Analiza

Ze słów oznaczonych w przepisie: „„**zgoda**" **osoby, której dane dotyczą** (…)" wynika, że przepis dotyczy zgody osoby, której dane dotyczą.

Ze słów oznaczonych w przepisie: „(…) **osoba, której dane dotyczą**, (…)" również wynika, że zgoda, której dotyczy przepis jest wyrażana przez osobę, której dane dotyczą. Możliwe jest, że zgodę wyraża kto inny niż osoba, której dane dotyczą. Wynika to z faktu, że zgoda jest oświadczeniem woli czyli czynnością prawną. Jeżeli osoba, której dane dotyczą nie dysponuję pełną zdolnością do czynności prawnych, to zgodę na przetwarzanie danych tej osoby powinien wyrazić kto inny. Piszę o tym w uwadze (3.1. **Art. 5 ust. 11.** Uwaga 1. Zgoda a zdolność do czynności prawnych.)

Ze słów oznaczonych w przepisie: „„**zgoda" osoby, której dane dotyczą oznacza** (…)" wynika, że przepis definiuje zgodę osoby, której dane dotyczą.

Ze słów oznaczonych w przepisie: „„**zgoda**" osoby, której dane dotyczą **oznacza** dobrowolne, konkretne, świadome i jednoznaczne **okazanie woli**, (…)" wynika, że zgoda oznacza okazanie woli spełniające warunki wymienione w przepisie

Ze słów oznaczonych w przepisie: „„**zgoda**" osoby, której dane dotyczą oznacza **dobrowolne**, konkretne, świadome i jednoznaczne **okazanie woli**, (…)" wynika, że pierwszym warunkiem, który musi spełnić okazanie woli jest dobrowolność tego okazania woli.

Dobrowolne okazanie woli należy rozumieć tak, że aby miało ono miejsce, osoba, która okazuje wolę musi okazywać ją w warunkach dobrowolności. Innymi słowy – zgoda jest ważna, kiedy osoba,

która ją wyraża, wyraża ją dobrowolnie. Tu właśnie dotykamy istoty zagadnienia, a mianowicie tego kiedy osoba, której dane dotyczą wyraża zgodę dobrowolnie. Wydaje się, że osoba, której dane dotyczą wyraża zgodę dobrowolnie jeżeli sama podejmuje decyzję o jej wyrażeniu. Możliwe są tu następujące sytuacje:

- osoba której dane dotyczą wyraża zgodę w sposób całkiem dobrowolny – nie ma tu wątpliwości w kwestii ważności zgody z punktu widzenia jej dobrowolności.
- osoba, której dane dotyczą wyraża zgodę ponieważ jest do tego zmuszona, na przykład przemocą – zgoda jest nieważna. Zwracam uwagę, że zgoda jest tu nieważna również dlatego, ze zgoda to oświadczenie woli w przedmiocie zgody,[370] zaś brak swobody to jedna z wad oświadczeń woli, skutkująca nieważnością oświadczenia obciążonego taką wadą.
- osoba, która wyraża zgodę wyraża ją na polecenie, na przykład przełożonego – zgoda w takiej sytuacji jest nieważna, ponieważ niedobrowolna
- osoba, której dane dotyczą wyraża zgodę przy dużej dysproporcji sił między tą osobą a ADO, np. ADO jest jej przełożonym, najważniejszym klientem itd. – nie ma miejsca polecenie wyrażenia zgody, ale nie ma równorzędności podmiotów – podmiot słabszy wyraża zgodę pod przymusem – wydaje się, że i tu zgoda jest nieważna bo niedobrowolna
- osoba, której dane dotyczą wyraża zgodę w zamian za jakąś opcję w umowie z ADO, na przykład za niższą cenę produktu oferowanego przez ADO, tu sytuacja jest dość skomplikowana, ale przede wszystkim uważam, że taka zgoda jest dobrowolna. Poza tym uważam, że jeżeli zgoda jest częścią umowy, to istnieje wątpliwość, czy taką zgodę można wycofać. Co prawda z art. 7 ust. 3 RODO wynika, że zgodę można wycofać, ale uważam, że tyczy się to sytuacji kiedy zgoda jest podstawą przetwarzania. Inaczej sytuacja wygląda kiedy ADO sprzedaje towar taniej, jednak obniżenie ceny uwarunkowane jest od zgody, wtedy nawet jeśli w treści umowy zawarto zgodę, to uważam, że podstawą przetwarzania danych jest umowa czyli art. 6 ust. 2 RODO, nie zaś zgoda. Pozostaje pytanie czy zgodę taką można wycofać. Najuczciwsza

[370] R. Szałowski, *Ochrona danych osobowych. Komentarz do ustawy z dnia 29 sierpnia 1997 r.,* Zielona Góra 2000, s. 76.

odpowiedź brzmi, że takiej zgody wycofać nie można, bo w istocie nie ma co wycofywać – podstawą nie jest zgoda tylko umowa. Obawiam się jednak, że takie stanowisko się nie ostoi. Przewiduję, że przeważy stanowisko, zgodnie z którym zgodę, która jest częścią umowy i która wpłynęła obniżająco na cenę, można wycofać. Uważam, że w przypadku jeżeli uznamy, że taką zgodę można wycofać to ADO należy się odszkodowanie od osoby która wycofuje zgodę, co najmniej równe różnicy między ceną produktu a ceną produktu obniżoną z uwagi na zgodę.

Ze słów oznaczonych w przepisie: „„**zgoda**" osoby, której dane dotyczą oznacza dobrowolne, **konkretne**, świadome i jednoznaczne **okazanie woli**, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;" wynika, że drugim warunkiem, który musi spełnić okazanie woli jest by okazanie woli było konkretne.

Konkretne okazanie woli to zapewne okazanie woli, którego nie można pomylić z niczym innym. Wolę można okazać słowem mówionym, słowem pisanym, wypełnieniem pozycji w formularzu, „zaptaszeniem" opcji w formularzu elektronicznym, gestem i różnymi innymi sposobami. Katalog sposobów okazania woli jest otwarty, niewątpliwe jest jednak, że jakimkolwiek sposobem by tej woli nie okazywano, to sposób ten musi być na tyle zrozumiały i właśnie konkretny, by mógł zostać właściwie zinterpretowany przez ADO. Konkretność okazania woli Może być oceniana z dwóch punktów widzenia. Pierwszy to spojrzenie na konkretność okazania woli jako zjawisko, które pojawia się w akcie komunikacji zachodzącym miedzy ADO a osobą, która wolę okazuje. Drugi punkt widzenia to spojrzenie na konkretność okazania woli jako zjawisko, które co prawda zachodzi między ADO a osobą, która wolę okazuje, jednak które jest oceniane z punktu widzenia obserwatora zewnętrznego wobec ocenianego aktu komunikacji. Przyjęcie pierwszego punktu widzenia wydaje się racjonalne, skoro komunikacja zachodzi Między ADO a osobą, która wolę okazuje, to nie ma powodu by patrzeć inaczej, by wprowadzać do analizowanej relacji, dodatkowe, czasem hipotetyczne osoby. Przyjęcie pierwszego punktu widzenia jest racjonalne jednak jedynie na pozór. Bardzo łatwo wyobrazić sobie ADO, który wyłudza zgody na przetwarzanie danych osobowych. ADO może przyjmować, że jakiś akt,

jakaś czynność osoby która (rzekomo) wolę okazuje, jest konkretnym okazaniem woli oznaczającym wyrażenie zgody. Osoba, która akt ten odbywa, czynność wykonuje, może w ogóle nie być świadoma, że ADO traktuje odbycie aktu, wykonanie czynności, jako konkretne okazanie woli skutkujące wyrażeniem zgody. Z komentowanej definicji wynika, że samo konkretne okazanie woli nie wystarczy dla wyrażenia zgody, konieczna jest kumulatywna realizacja pozostałych warunków, zwracam jednak uwagę, że umiejętny ale niegodziwy ADO może wyłudzać oświadczenia woli, symulując nie tylko ich konkretność ale i pozostałe cechy konieczne. Z opisanych przyczyn, lepiej chyba, dla oceny konkretności oświadczenia woli przyjmować drugi, proponowany przeze mnie punkt widzenia, czyli oceniać konkretność okazania woli z punktu widzenia obserwatora zewnętrznego wobec aktu komunikacji. Drugi punkt widzenia należy przyjmować zwłaszcza w sytuacjach konfliktowych, kiedy to ADO i osoba, której dane dotyczą wchodzą w relację, ADO przyjmuje, że zgodę wyrażono, zaś osoba której dane dotyczą uważa dokładnie odwrotnie. Zależnie od stanu faktycznego, oceny takiej dokonywać będzie ADO, PUODO, sąd. z punktu widzenia bezpieczeństwa prawnego ADO wydaje się, że najlepiej jest by ADO obstawał, że zgoda została wyrażona w sposób konkretny i że ewentualne protesty osoby, której dane dotyczą, jakoby zgoda nie została wyrażona w sposób konkretny są bezpodstawne oraz, że ADO traktuje je jak wycofanie zgody na przetwarzanie danych osobowych.

Kiedy zastanowimy się jak powinno sprawę oceniać PUODO i sąd to sytuacja nie jest tak oczywista. Podejście pierwsze – chroni oszustów, a jednak należałoby chronić ludzi uczciwych. Podejście drugie – jest nieco oderwane od realiów – jeżeli PUODO lub sąd oceni z własnego, zewnętrznego punktu widzenia, to niewątpliwie ochroni osobę, której dane dotyczą, jednak może przy tym jednak skrzywdzić ADO, który może być nie tyle umiejętnym niegodziwcem, ile podmiotem uczciwym acz niekompetentnym, który jest przekonany, że odebrał konkretną zgodę. Wydaje się, że najlepsze byłoby tu rozwiązanie nawiązujące do koncepcji H.L.A Harta – PUODO czy sąd powinni przy ocenie przyjąć nie optykę ADO, nie optykę własną, nawet nie optykę osoby, której dane dotyczą, ale optykę przyjmowaną powszechnie w takich sytuacjach. Podejście takie, w duchu Reguły Rozpoznania wydaje się najlepszym, z punktu widzenia poszanowania praw obydwu stron, zarówno ADO jak i osoby, której dane dotyczą.

Obawiam się, że nie będzie ono miało miejsca i podejście drugie, w którym PUODO czy sąd będą używać swojego rozeznania jako ostatecznej instancji, przeważy.

Ze słów oznaczonych w przepisie: „„**zgoda**" osoby, której dane dotyczą oznacza dobrowolne, konkretne, **świadome** i jednoznaczne (…)" wynika, że trzecim warunkiem, który musi spełnić okazanie woli jest by okazanie woli było świadome. Świadomość, jako cecha oświadczenia woli jest analogiczna do dobrowolności oświadczenia woli.

Świadome okazanie woli to zapewne okazanie woli, którego świadoma jest osoba, która wolę tę okazuje. Trudno wyobrazić sobie stan faktyczny, w którym osoba wyrażająca zgodę na przetwarzanie danych osobowych upoważniła pełnomocnika do wyrażenia takiej zgody i pełnomocnik ten wyraził tę zgodę nieświadomie. Pełnomocnik wyraził zgodę w imieniu mocodawcy, jednak zrobił to nieświadomie. w takim wypadku należałoby oceniać świadomość pełnomocnika.
Świadomość okazania woli to zjawisko, które pojawia się w akcie komunikacji zachodzącym miedzy ADO a osobą, która wolę okazuje, jednak jest to zjawisko z punktu widzenia osoby, której dane dotyczą, niejako wewnętrzne. Administrator (danych) może doprowadzić osobę, której dane dotyczą do wykonywania czynności, które administrator uzna za świadome okazanie woli, jednak osoba ta nie będzie tej świadomości internalizować. W takiej sytuacji należy brać pod uwagę świadomość osoby, której dane dotyczą, nie zaś towarzyszące czynnościom okoliczności wygenerowane przez administratora i również nie stanowisko administratora.

Samo świadome okazanie woli nie wystarczy dla wyrażenia zgody, konieczna jest kumulatywna realizacja pozostałych warunków z punktu widzenia bezpieczeństwa prawnego ADO wydaje się, że najlepiej jest by ADO obstawał, że zgoda została wyrażona w sposób świadomy i że ewentualne protesty osoby, której dane dotyczą, jakoby zgoda nie została wyrażona w sposób świadomy są bezpodstawne oraz, że ADO traktuje je jak wycofanie zgody na przetwarzanie danych osobowych.
Podejście w duchu koncepcji H.L.A Harta, w duchu Reguły Rozpoznania nie wydaje się w przypadku oceny świadomości zgody, rozwiązaniem. Świadomość ma charakter wewnętrzny i tak też, z punktu widzenia świadomej lub nieświadomej składania zgody osoby te zgodę składającej, należy tę świadomość oceniać.

Ze słów oznaczonych w przepisie: „„**zgoda**” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i **jednoznaczne** okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;” wynika, że **czwartym warunkiem**, który musi spełnić okazanie woli jest by okazanie woli było jednoznaczne.

Jak piszę wyżej, katalog sposobów okazania woli jest otwarty, sposób okazywania woli musi być na tyle jednoznaczny, by mógł zostać jako jednoznaczny, czyli właściwie zinterpretowany przez ADO. Jednoznaczność okazania woli (podobnie jak konkretność) może być oceniana z dwóch punktów widzenia. Pierwszy to spojrzenie na jednoznaczność okazania woli jako zjawisko, które pojawia się w akcie komunikacji zachodzącym miedzy ADO a osobą, która wolę okazuje. Drugi punkt widzenia to spojrzenie na jednoznaczność okazania woli jako zjawisko, które zachodzi między ADO a osobą, która wolę okazuje, jednak które jest oceniane z punktu widzenia obserwatora zewnętrznego wobec ocenianego aktu komunikacji. Wydaje się, że zasadne jest przyjęcie drugiego punktu widzenia, zwłaszcza z uwagi na możliwe funkcjonowanie administratorów danych wyłudzających zgody. z punktu widzenia bezpieczeństwa prawnego ADO i tu wydaje się, że najlepiej jest by ADO obstawał, że zgoda została wyrażona w sposób jednoznaczny i że ewentualne protesty osoby, której dane dotyczą, jakoby zgoda nie została wyrażona w sposób jednoznaczny są bezpodstawne oraz, że ADO traktuje je jak wycofanie zgody na przetwarzanie danych osobowych.
Podejście hartowskie, w duchu Reguły Rozpoznania wydaje się najlepszym, z punktu widzenia poszanowania praw ADO jak i osoby, której dane dotyczą.

Ze słów oznaczonych w przepisie: „„**zgoda**” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne **okazanie woli, którym osoba, której dane dotyczą**, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;” wynika, że dla ważności zgody konieczne jest by zaszło okazanie woli osoby, której dane dotyczą. Okazanie woli w przedmiocie zgody. Nie wystarczy by oso-

ba, która okazuje wolę, tę wolę miała w sobie. Dla ważności zgody osoba ta musi wolę tę przejawić.

Ze słów oznaczonych w przepisie: „„**zgoda**" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, **którym osoba, której dane dotyczą**, w formie oświadczenia lub wyraźnego działania potwierdzającego, **przyzwala na przetwarzanie dotyczących jej danych osobowych**;" wynika, że z oświadczenia woli w przedmiocie zgody, aby stanowiło zgodę musi wynikać, ze sobą wyrażająca zgodę przyzwala na przetwarzanie danych osobowych, które jej dotyczą. Przyzwala, czyli chce by jej dane były przetwarzane. Zdecydowanie konieczny jest tu akt przyzwolenia na przetwarzanie danych osobowych, nie wystarczy brak protestu przeciwko takiemu przetwarzaniu.

Ze słów oznaczonych w przepisie: (…) okazanie woli (…) w **formie oświadczenia** lub **wyraźnego działania potwierdzającego** (…)" wynika, że okazanie woli przyzwolenia na przetwarzanie danych osobowych musi dla swej ważności mieć formę oświadczenia lub wyraźnego działania potwierdzającego. Jeśli chodzi o formę oświadczenia to należy przez nią rozumieć oświadczenie w formie ustnej, lub w formie pisemnej, lub w formie dokumentowej, lub w formie aktu notarialnego, lub w formie dokumentu z podpisem notarialnie poświadczonym. Jeśli chodzi o formę wyraźnego działania potwierdzającego, to należy tu zwrócić uwagę na dwie sprawy. Po pierwsze, że okazanie woli przyzwalające na przetwarzanie danych osobowych może mieć formę działania. Niekonieczne jest oświadczenie, może być inna czynność, na przykład kiwnięcie głową, wypełnienie formularza, na którym jest napisane, że wypełnienie oznacza zgodę itp. Po drugie działanie przyzwalające na przetwarzanie danych osobowych musi dla swej ważności być wyraźne. Nie wystarczy zatem, że osoba, której dane dotyczą dostarczy administratorowi swoje dane osobowe. Jest to co prawda działanie ale nie działanie potwierdzające. Różnica miedzy działaniem a działaniem potwierdzającym może w konkretnych stanach faktycznych być trudna do uchwycenia i wskazania, jednak ustalanie tej różnicy i jej szanowanie jest konieczne. Konieczne też z uwagi na to, ze działanie o którym piszę, nie dość, że ma mieć charakter działania potwierdzającego a nie jakiejkolwiek czynności ale też „wyraźnego" działania potwierdzającego. Innymi słowy nic nie

można pozostawić domysłowi. Fakt, że osoba której dane dotyczą przyzwoliła działaniem na ich przetwarzanie powinien wynikać z jej czynności (działania) w sposób oczywisty.

3. Art. 4. pkt 11. Uwagi

3.1. Art. 4. pkt 11. Uwaga 1.
Zgoda – podstawa prawna

Przetwarzanie zgodne z prawem danych osobowych, w oparciu o zgodę, to przetwarzanie zgodnie z art. 6 ust. 1 lit a RODO w zw. z art. 7 RODO.

Przetwarzanie zgodne z prawem danych osobowych, w oparciu o zgodę, w przypadku usług społeczeństwa informacyjnego, przy świadczeniu tychże usług wobec dziecka to to przetwarzanie zgodnie z art. 6 ust. 1 lit a RODO w zw. z art. 7 RODO w zw. z art. 8 RODO.

Przetwarzanie zgodne z prawem szczególnych kategorii danych, o których mowa w art. 9 ust. 1 RODO, w oparciu o zgodę, to przetwarzanie zgodnie z art. 6 ust. 1 lit a RODO w zw. z art. 9 ust. 2 lit a RODO w zw. z art. 7 RODO.

Zgoda z art. 6 ust. 1 lit a RODO wydaje się różnić od zgody z art. 9 ust. 2 lit a RODO kategorią danych na jakich przetwarzanie jest wyrażana. Wydaje się, że wystarczy wyrazić ja raz, jednak podstawę prawną należy podawać całą, zarówno wskazując art. 6 ust. 1 lit a RODO jak i wskazując art. 9 ust. 2 lit a RODO.

3.2 Art. 4. pkt 11. Uwaga 2.
Zgoda a wady oświadczeń woli

Warto zwrócić uwagę na związek poszczególnych warunków zgody z wadami oświadczeń woli.

Zamknięty katalog wad oświadczeń woli jest następujący: brak świadomości lub swobody, pozorność, błąd, podstęp, groźba, wyzysk.

Poszczególne warunki zgody wydają się być związane z poszczególnymi wadami oświadczeń woli, a nawet sprawiają wrażenie ich odpowiedników.

Dobrowolność zgody. Zgoda niedobrowolna to w odniesieniu do wad oświadczeń woli zgoda złożona wskutek groźby skierowanej do osoby wyrażającej zgodę. Groźbę uregulowano w art. 87 kodeksu cywilnego. Zgoda niedobrowolna to również zgoda złożona pod wpływem podstępu. Podstęp może być wynikiem działania administratora

danych, podmiotu przetwarzającego lub strony trzeciej. Podstęp uregulowano w art. 86 kodeksu cywilnego.

Zwracam uwagę na fakt że z art. 86 § 2 kodeksu cywilnego wynika że jeżeli podstępnie zachowa się osoba trzecia to podstęp ten jest jednoznaczny z podstępem strony, w naszym wypadku z podstępem administratora danych osobowych, pod pewnymi jednak warunkami. Podstęp osoby trzeciej jest jednoznaczny z podstępem administratora jeżeli administrator o podstępie wiedział i nie zawiadomił o nim osoby której dane dotyczą. Osobę trzecią występującą w kodeksie cywilnym można utożsamić ze stroną trzecią występującą w RODO. Uważam że podmiotu przetwarzającego występującego w RODO nie można utożsamić z osobą trzecią występującą w art. 86 §2 KC. Podmiot przetwarzający przetwarza dane w imieniu administratora (danych), podstawa prawna przetwarzania danych przez podmiot przetwarzający składa się z odpowiedniej przesłanki przetwarzania danych ocenianej dla administratora (danych) oraz z umowy powierzenia przetwarzania danych. Podmiot przetwarzający jest po prostu zleceniobiorcą administratora w zakresie przetwarzania danych osobowych. Uważam że działanie podmiotu przetwarzającego powinno być w zakresie podstępu oceniane tak jak działanie administratora.

Z art. 86 § 2 kodeksu cywilnego wynika również że jeżeli osoba trzecia zachowa się podstępnie to jej podstęp jest jednoznaczny z podstępem strony, w naszym wypadku administratora danych osobowych, jeżeli czynność prawna, w naszym wypadku wyrażenie zgody, była nieodpłatna. Wyrażenie zgody co do zasady jest czynnością nieodpłatną, więc co do zasady podstęp strony trzeciej doprowadzający do wyrażenia zgody, należy oceniać jednoznacznie z podstępem administratora (danych osobowych). Gdyby zdarzyło się, że zgoda na przetwarzanie danych osobowych miałaby charakter odpłatny, to podstęp osoby trzeciej czyli strony trzeciej nie byłby jednoznaczny z podstępem administratora danych, czyli nie zachodziłaby wada oświadczenia woli określana jako podstęp, co oczywiście nie oznacza że taka zgoda na pewno byłaby ważna ponieważ należałoby i tak oceniać ją z punktu widzenia RODO.

Konkretność zgody. Konkretność zgody wydaje się mieć pewien związek z wadą oświadczenia woli znaną jako pozorność a uregulowaną w artykule 83 kodeksu cywilnego.

Świadomość zgody (złożenie jest w warunkach świadomości osoby, której dane dotyczą). Zgoda złożona bez świadomości osoby

której dane dotyczą o fakcie składania zgody może, choć nie musi być związana z błędem oświadczenia woli znanym jako brak świadomości lub swobody, uregulowanym w art. 82 kodeksu cywilnego.

Jednoznaczność zgody. Jednoznaczność zgody podobnie jak jej konkretność wydaje się mieć związek z pozornością uregulowaną w art. 83 kodeksu cywilnego

Związek poszczególnych warunków zgody z poszczególnymi wadami oświadczeń woli jest zjawiskiem ciekawym i wręcz dopraszającym się o osobną publikację. Wydaje się że nie każda wada oświadczenia woli ma swój odpowiednik wśród warunków zgody na przetwarzanie danych osobowych, nie należy jednak wyciągać z tego pochopnych wniosków. Jeżeli bowiem oświadczenie woli w przedmiocie zgody na przetwarzanie danych osobowych obciążone jest którąkolwiek z wad oświadczeń woli, to takie oświadczenie woli w przedmiocie zgody na przetwarzanie danych osobowych jest nieważne, czyli nieważna jest zgoda na przetwarzanie danych osobowych. To z kolei może doprowadzić do przetwarzania danych osobowych bez podstawy prawnej i tym samym prowadzić do przetwarzania danych osobowych z naruszeniem zasady zgodności z prawem.

3.3 Art. 4. pkt 11. Uwaga 3.
Obowiązek wykazania zgody

Motyw 42 Preambuły RODO stanowi m.in.: „Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania.”. Zachodzi tu ciekawe zjawisko, a mianowicie obowiązek wynikający z preambuły RODO. Obowiązek ten, prawie tymi samymi słowy powtórzony jest w art. 7 ust. 1 RODO. Odsyłam do komentarz do tego przepisu, tu jednak zwracam uwagę na pewien fakt. Obowiązek wykazania zgody nie oznacza obowiązku odbierania jej w formie pisemnej, ale nie należy tego obowiązku bagatelizować. Wykazanie faktu wyrażenia zgody może być czasem jedynym narzędziem wykazania realizacji zasady zgodności z prawem ustanowionej w art. 5 ust. 1 lit. a RODO.

3.4 Art. 4. pkt 11. Uwaga 4.
Zgoda warunkowa

Dominik Lubasz twierdzi[371], że zgoda może mieć charakter warunkowy. Mam wątpliwość, czy pogląd ten jest trafny. Nie jestem pewien jego nietrafności, mam jedynie poważną wątpliwość. Wyrażeniu zgody „pod warunkiem" nie przeszkadza treść art. 6 ust. 1 RODO, jednak mam wątpliwość, czy nie czyni tego treść definicji zgody, znajdującej się w art. 4 pkt 11 RODO. Zgoda – okazanie woli ma być: dobrowolne, konkretne, świadome i jednoznaczne. Mam wątpliwość, czy warunkowa zgoda realizuje posiada wszystkie te cechy, a zwłaszcza czy ma charakter konkretny i jednoznaczny, jeżeli ktoś wyraził zgodę pod warunkiem, to nie od rzeczy jest pytanie, czy zgodę tę wyraził, czy nie. Odpowiedź, która brzmiałaby mniej więcej tak, że owszem, że zgodę wyraził z tym, że pod warunkiem, to niestety żadna odpowiedź, bowiem udzielając jej popełniamy błąd samoodniesienia. Czyli wątpliwość pozostaje.

4. Art. 4. pkt 11. Podsumowanie
w duchu Konceptualizmu Prawniczego
– Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 9 RODO definiuje **zgodę**, zatem zgodnie z dyrektywą języka prawnego[372], każdy kto interpretuje RODO powinien rozumieć pojęcie ***zgoda*** tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie ***zgoda*** tak jest ono zdefiniowane w art. 4 pkt. 8 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie

[371] D. Lubasz, *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 355.

[372] L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 93-99, zwłaszcza 95.

rozumiał znaczenie pojęcia „**zgoda**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4. pkt 11. Konkretyzacja zasady

Artykuł 4 pkt 11 sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Zgoda stanowi jedną z przesłanek dopuszczalności przetwarzania danych. Odbiorca przetwarza dane w oparciu o własną podstawę prawną. Udostępnianie danych jest przetwarzaniem, o czym należy pamiętać. Jeżeli administrator danych udostępnia odbiorcy dane osobowe, to musi dbać on o to by udostępnienie odbyło się w oparciu o konkretną podstawę prawną. Należy przy tym pamiętać, że jeżeli potencjalny, przyszły odbiorca posiada podstawę prawną do przetwarzania danych osobowych, które posiada pierwotny administrator, to nie oznacza to wcale, że pierwotny administrator powinien odbiorcy udostępnić dane osobowe. Konieczny jest jeszcze element pośredni, łączący, czyli podstawa prawna do udostepnienia danych osobowych przez danego administratora danemu odbiorcy.

Realizacji **zasady rzetelności**. Realizując obowiązki wynikające z art. 13 RODO, z art. 14 RODO i z art. 15 RODO, administrator danych ma obowiązek informować o odbiorcach. Informowanie o odbiorcach sprzyja realizacji zasady rzetelności.

Realizacji **zasady przejrzystości** poprzez informowanie o odbiorcach (z art. 4 pkt 9 RODO). Informowanie o odbiorcach sprzyja realizacji zasady przejrzystości.

Realizacji **zasady ograniczenia celu**, poprzez dbanie przez administratora danych o to by udostępnienie danych odbyło się tylko w oparciu o ważną podstawę prawną, o której piszę wyżej przy omawianiu konkretyzacji zasady zgodności z prawem. Administrator danych nie ma możliwości skontrolowania w jakim celu odbiorca używał będzie udostępnionych mu danych osobowych. Możliwość kontroli kończy się na etapie udostępnienia lub oczywiście nieudostępnienia danych. Właśnie dlatego, ze władztwo administratora danych nad danymi kończy się w momencie ich udostępnienia, powinien on pieczołowicie dbać o podstawe prawna do udostępnienia. Jeżeli administrator danych posiada podstawę prawną do udostępnienia danych, to istnieje choć cień nadziei, ę odbiorca będzie przetwarzał dane

w zgodzie z prawem, ale i w celu wynikającym z kolei z jego podstawy prawnej do przetwarzania danych osobowych.

Realizacja **zasady minimalizacji** analogiczna jest do realizacji zasady ograniczenia celu. Administrator (danych) dba o to by udostępnić tylko dane osobowe tylko wtedy jeżeli posiada do tego stosowną podstawę prawną.

Drugi, ważniejszy chyba nawet element związku pojęcia odbiorcy z realizacją zasady minimalizacji jest taki, że administrator danych powinien dbać o to by udostępniać dane w sposób zgodny z tą zasadą, czyli żeby udostępniać tylko dane w zakresie niezbędnym. Uważam, że udostępnianie danych, wyjmowanie ich niejako spod władztwa pierwotnego administratora danych, jest czynnością na tyle ryzykowną (choć konieczną), że zasadę minimalizacji należy tu rozumieć restrykcyjnie. Restrykcyjnie, czyli udostępniać dane wyłącznie w zakresie niezbędnym, nie zaś również dane adekwatne lub stosowne. Szerzej dwa rozumienia zasady mimalizacji omawiam w uwadze *3.2. Art. 5 ust. 1 lit. c. Uwaga 2. Treść zasady, podejście restrykcyjne i w* uwadze *3.3. Art. 5 ust. 1 lit. c. Uwaga 3. Treść zasady, podejście łagodne*.

Realizacja **zasady prawidłowości**. Administrator ma, wynikający z art. 19 RODO obowiązek informowania odbiorcy m.in. o sprostowaniu danych osobowych. Realizacja tego obowiązku sprzyja realizacji zasady prawidłowości.

Realizacja **zasady ograniczenia przechowywania danych**. Administrator ma, wynikający z art. 19 RODO obowiązek informowania odbiorcy m.in. o usunięciu danych lub o ograniczeniu przetwarzania. Realizacja tego obowiązku sprzyja realizacji zasady ograniczenia przechowywania danych.

Związek **zasady integralności** z definicją odbiorcy jest daleki. Jedyny jaki dostrzegam to wynikający z zasady zgodności z prawem obowiązek dbałości o to by dane osobowe udostępniane były w oparciu o odpowiednią podstawę prawną. Jeżeli dane zostają uzupełnione w oparciu o stosowną podstawę prawną, to można mieć nadzieję, że odbiorca, który posiada stosowną podstawę do uzyskania danych, zadba również o to by dane nie były modyfikowane bez stosownej podstawy prawnej.

Związek **zasady poufności**. Z definicją odbiorcy pewien jest. Otóż administrator danych musi, jak wiadomo dbać o to by dane były przetwarzane zgodnie z zasadą poufności, czyli przez osoby do tego uprawnione. Administrator danych jest o to w stanie zadbać w swojej

organizacji, do pewnego stopnia również w organizacji podmiotu przetwarzającego. Na przetwarzanie danych w organizacji odbiorcy, rozumianego jako nowy administrator danych, pierwotny administrator nie ma wpływu, z pewnymi jednak zastrzeżeniami. Przede wszystkim administrator powinien udostępniać dane odbiorcom jedynie wtedy kiedy istnieje podstawa prawna do udostępnienia danych. Jeżeli administrator danych udostępnia dane bez takiej podstawy to niewątpliwie oprócz złamania zasady zgodności z prawem, łamie również zasadę poufności.

Grozić złamaniem zasady poufności może też niedbałe wybieranie odbiorcy. Kiedy administrator danych wybiera odbiorcę, to powinien czynić to w sposób roztropny. Oczywiście myśl ta ma sens tylko wtedy gdy administrator danych wybiera odbiorcę.

6. Art. 4 pkt 11. Postulaty de lege ferenda

6.1 Art. 4 pkt 11. Postulat 1. Doprecyzowanie pojęcia definiowanego

W art. 4 pkt 11 RODO zdefiniowano zgodę osoby, której dane dotyczą na przetwarzanie danych osobowych. Niestety sposób zapisania przepisu w akcie prawnym może sugerować, że zdefiniowano jedynie zgodę. Jest tak ponieważ na początku przepisu znajduje się ujęte w cudzysłów słowo „zgoda". Rozwiązanie takie jest mylące i nieporządne. W związku z tym postuluję dodanie do przepisu słów: „na przetwarzanie danych osobowych" oraz ujęcie w cudzysłów całego pojęcia definiowanego.

Przepis po nowelizacji miałby postać:

„zgoda osoby, której dane dotyczą na przetwarzanie danych osobowych" oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych."; (zmieniona część przepisu jest wytłuszczona).

Artykuł 4. pkt 12 RODO

„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

1. Art. 4. pkt 12. Komentarz

W przepisie definiowane jest naruszenie ochrony danych osobowych.

Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa, o cechach określonych dalej w przepisie. Jeżeli zastąpimy to pojęcie naruszenia bezpieczeństwa, pojęciem „zdarzenie”, to dla zrozumienia przepisu nic to nie zmienia.

Naruszeniem bezpieczeństwa jest zagrożenie wystąpieniem zdarzeń wymienionych dalej w przepisie lub wystąpienie zdarzeń wymienionych dalej w przepisie.

Naruszenie ochrony danych osobowych to zdarzenia skutkujące przypadkowym lub niezgodnym z prawem zniszczeniem danych i nieuprawnionym wyciekiem danych jak również zdarzenia zagrażające przypadkowym lub niezgodnym z prawem zniszczeniem danych i nieuprawnionym wyciekiem danych.

Przez naruszenie ochrony danych osobowych rozumieć należy naruszenie bezpieczeństwa o cechach opisanych w omawianym przepisie. Naruszenie bezpieczeństwa opisywane w przepisie, by zaszło, musi prowadzić do pewnych skutków. Dla uznania, że zaszło „naruszenie ochrony danych osobowych” nie jest konieczne by zaszły owe skutki. Wystarczy, że zdarzenie jedynie prowadzi do opisanych w przepisie skutków – z tego właśnie powodu, skutki te opisane są poniżej jako skutki możliwe.

- **Pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych, które są przesyłane. Raczej przesyłane przez administratora, nie do administratora, nie jest to jednak pewne, zwłaszcza .
  Zwracam uwagę, że przepis stanowi o danych osobowych, które są przesyłane, przepis nie stanowi, czy są one przesyłane do administratora czy od administratora, czy wręcz za pośrednictwem administratora. Naruszenie może mieć miejsce w każdej ze wskazanych sytuacji.
- **Drugim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych które są przechowywane, przez administratora.
- **Trzecim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych które są przetwarzane, w sposób inny niż przesyłanie lub przechowywanie, czyli, które są przetwarzane w jakikolwiek sposób.
- **Czwartym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe utracenie danych osobowych, które są przesyłane. Zwłaszcza przesyłane przez administratora, utracenie danych osobowych może jednak ujawnić się, nie jeszcze w strukturze ADO, ale dalej, jest to nawet bardzo prawdopodobne. Co więcej, jeżeli utracenie danych osobowych zachodzi w strukturze administratora, to trudno mówić o danych przesyłanych.
- **Piątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe utracenie danych osobowych, które są przechowywane przez administratora.
- **Szóstym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe utracenie danych osobowych, które są przetwarzane przez administratora w sposób inny niż przesyłanie lub przechowywanie.
- **Siódmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych, które są przesyłane przez administratora. Zagadnienie oceniamy z punktu widzenia administratora i widać od razu, że administratora może nie być świadom naruszenia.
- **Ósmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych, które są przechowywane przez administratora.

- **Dziewiątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych, które są przetwarzane przez administratora, w sposób inny niż przesyłanie lub przechowywanie.
- **Dziesiątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieuprawnione ujawnienie danych osobowych, które są przesyłane. Naruszenie może mieć miejsce w strukturze administratora – nadawcy, administratora – odbiorcy, administratora – dostawcy usługi przesyłu.
- **Jedenastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieuprawnione ujawnienie danych osobowych, które są przechowywane przez administratora.
- **Dwunastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieuprawnione ujawnienie danych osobowych, które są przetwarzane przez administratora, w sposób inny niż przesyłanie lub przechowywanie.
- **Trzynastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych, które są przesyłane przez administratora.

  Wydaje się, że z takim dostępem mamy do czynienia, kiedy przy świadczeniu usługi pocztowej, ktoś nieuprawniony zapozna się z treścią przesyłanej wiadomości, o ile ta zawiera dane osobowe. Problemem, o którym trzeba pamiętać jest to kto powinien zgłosić ewentualne naruszenie, czy administrator wysyłający, czy administrator świadczący usługę przesyłki, czy administrator, do którego przesyłka dociera. Administrator wysyłający może nie mieć świadomości naruszenia, nie można zatem od niego oczekiwać, że je zgłosi.
- **Czternastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych, które są przechowywane przez administratora lub przez podmiot przetwarzający.
- **Piętnastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych, które są przetwarzane w sposób inny niż przesyłanie lub przechowywanie, czyli które są w jakiś, jakikolwiek (z uwzględnieniem zawartego w przepisie wyłączenia) przetwarzane.
- **Szesnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych, które są prze-

syłane. Naruszenie może mieć miejsce zwłaszcza podczas samego transferu danych osobowych miedzy administratorem – nadawcą a adresatem.

- **Siedemnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych, które są przechowywane.
- **Osiemnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych, które są przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.
- **Dziewiętnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych, które są przesyłanych. Utracenie należy utożsamiać z zagubieniem, wydaje się, że z zagubieniem podczas transferu, transportu, przesyłania.
- **Dwudziestym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych, które są przechowywanych, czyli ich zagubienie przez administratora lub przez podmiot przetwarzający podczas ich przechowywania.
- **Dwudziestym pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych, które są przetwarzanych w sposób inny niż przesyłanie lub przechowywanie czyli ich zagubienie przez administratora lub przez podmiot przetwarzający podczas wykonywania czynności innych niż przesyłanie lub przechowywanie.
- **Dwudziestym drugim** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych, które są przesyłanych. Zmodyfikowanie danych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek
- **Dwudziestym trzecim** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych. Zmodyfikowanie bez upoważnienia lub polecenia, czyli ze złamaniem zasady integralności.
- **Dwudziestym czwartym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.
- **Dwudziestym piątym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych. Przesyłanych od administratora do pod-

miotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.

- **Dwudziestym szóstym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych. Jest to ujawnienie z naruszeniem zasady zgodności z prawem i zasady poufności, ujawnienie, nad którym nie sprawuje świadomej kontroli administratora.
- **Dwudziestym siódmym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.
- **Dwudziestym ósmym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przesyłanych od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.
- **Dwudziestym dziewiątym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
- **Trzydziestym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. Przetwarzanych przez administratora lub przez podmiot przetwarzający.
- **Trzydziestym pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych. Przepis niestety nie wskazuje z jakim przesyłaniem wiąże skutki, czy mowa tu o przesyłaniu w kierunku od administratora, czy mowa tu o przesyłaniu do administratora, czy mowa tu o przesyłaniu wewnątrz administratora.
- **Trzydziestym drugim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych. Przepis nie wskazuje z jakim przechowywaniem wiąże skutki, wydaje się jednak, że przede wszystkim mowa tu o przechowywaniu danych osobowych przez administratora, wewnątrz jego struktury. Należy uczciwie przyznać, że przepis nie zawiera słów „przechowywanych przez administratora", z czego wynika, że dotyczy on również naruszenia och-

rony danych osobowych, przechowywanych nie wewnątrz struktury administratora, ale wewnątrz struktury podmiotu przetwarzającego.

- **Trzydziestym trzecim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.
- **Trzydziestym czwartym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przesyłanych od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.
- **Trzydziestym piątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
- **Trzydziestym szóstym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.
- **Trzydziestym siódmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przesyłanych od administratora do podmiotu przetwarzającego lub od administratora lub podmiot przetwarzający do kogokolwiek. Przypadkowe – zmodyfikowanie danych wykryto i administrator dosłał właściwe dane, niezgodne z prawem – celowa modyfikacja przesyłanych danych, przypadkowe i niezgodne z prawem – nieświadoma modyfikacja przesyłanych danych.
- **Trzydziestym ósmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych prze administratora lub przez podmiot przetwarzający. Przypadkowe – zmodyfikowanie przechowywanych danych wykryto i usunięto, niezgodne z prawem – celowa modyfikacja przechowywanych przez administratora lub PP danych, przypadkowe i niezgodne z prawem – nieświadoma modyfikacja przechowywanych przez administratora lub przez podmiot przetwarzający danych.

- **Trzydziestym dziewiątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie, na przykład zmodyfikowanie danych osobowych przy okazji ich adaptowania do jakiegoś celu, jednak zmodyfikowanie poza instytucjonalną świadomością administratora, skutkujące naruszeniem zasady prawidłowości przetwarzania danych osobowych.
- **Czterdziestym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek, na przykład ujawnienie podczas przesyłania.
- **Czterdziestym pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
- **Czterdziestym drugim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie, czyli w jakikolwiek sposób.
- **Czterdziestym trzecim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przesyłanych.
- **Czterdziestym czwartym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przechowywanych.
- **Czterdziestym piątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

2. Art. 4. pkt 12. Analiza

Ze słów „**naruszenie ochrony danych osobowych**" (…)" wynika, że w przepisie omawianym definiowane jest właśnie naruszenie ochrony danych osobowych.

Ze słów wytłuszczonych w przepisie: „naruszenie ochrony danych osobowych" **oznacza naruszenie bezpieczeństwa** (…)" wynika, że naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa, o cechach określonych dalej w przepisie. Niestety prawodawca popełnił tu dwa błędy. Po pierwsze wprowadził pojęcie „naruszenie bezpieczeństwa", którego nigdzie w RODO nie zdefiniował, dopuścił się zatem błędu logicznego znanego pod nazwą „nieznane przez nieznane". Po drugie prawodawca niepotrzebnie wprowadził pojęcie „naruszenie bezpieczeństwa". Uważam, że prawodawca wprowadził to pojęcie niepotrzebnie, ponieważ jeżeli zastąpimy to pojęcie słowem „zdarzenie", to dla zrozumienia przepisu, dla dokonania jego wykładni, nic to nie zmienia.

Ze słów: „(…) **prowadzące do** (…)" wynika, że naruszenie bezpieczeństwa to zdarzenie, które prowadzi do zdarzeń wskazanych dalej w przepisie. Prowadzi do tych zdarzeń, jednak niekoniecznie do nich doprowadza. Naruszeniem bezpieczeństwa jest zatem **zagrożenie wystąpieniem** zdarzeń wymienionych dalej w przepisie lub **wystąpienie** zdarzeń wymienionych dalej w przepisie. Szerzej piszę o tym w uwadze *3.3. Art. 4. pkt 12.Uwaga 3. Konkretyzacja obowiązku zgłoszenia naruszenia.*

Ze słów: „(…) **do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;**" wynika, jakie zdarzenie mogą skutkować lub skutkują naruszeniem ochrony danych osobowych. Zdarzenia te to przypadkowe lub niezgodne z prawem zniszczenie danych i nieuprawnione udostepnienie lub dostęp do danych czyli tzw. wyciek danych. Zdarzenia te analizuję niżej, dochodząc do czterdziestu pięciu potencjalnych, przewidzianych w przepisie stanów faktycznych. Wersja superskrócona pozwala stwierdzić, że naruszenie ochrony danych osobowych to zdarzenia skutkujące przypadkowym lub niezgodnym z prawem zniszczeniem danych i nieuprawnionym wyciekiem danych jak również zdarzenia zagrażające przypadkowym lub niezgodnym z prawem zniszczeniem danych i nieuprawnionym wyciekiem danych.

Analizuję poniżej możliwe skutki naruszeń bezpieczeństwa. Skutki te ponumerowałem, jednak zwracam uwagę, że z takiej a nie innej ich kolejności nie należy wywodzić żadnych skutków. Skutki omówione są w tej samej kolejności w jakiej pojawiają się w przepisie, uważam jednak, że również z ich kolejności w przepisie, nie należy wywodzić żadnych skutków.

Ze słów: „(...) **przypadkowego lub niezgodnego z prawem** (...)" wynika, że zjawiska wymienione w przepisie mogą być jedynie przypadkowe bądź jedynie niezgodne z prawem bądź przypadkowe i niezgodne z prawem, co wynika z użycia słów: „przypadkowego **lub** niezgodnego" a w zasadzie z użycia funktora „lub". Należy przy tym zwrócić uwagę na fakt, że prawodawca odróżnia zdarzenia przypadkowe od zdarzeń niezgodnych z prawem. Zważywszy na fakt, że uprawnienie do przetwarzania danych tworzone jest dwuetapowo, przez upoważnienie i polecenie, to trudno sobie wyobrazić zdarzenie przypadkowe i zgodne z prawem.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zniszczenia** (...) **danych osobowych przesyłanych** (...)" wynika, że **pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych przesyłanych. Przepis niestety nie wskazuje z jakim przesyłaniem wiąże skutki. Czy mowa tu o przesyłaniu w kierunku od administratora, czy mowa tu o przesyłaniu do administratora, czy mowa tu o przesyłaniu wewnątrz administratora. Wydaje się, że raczej mowa tu o przesyłaniu od administratora, ponieważ to jest przesyłanie, na które administrator ma wpływ. Na przesyłanie wewnątrz administratora, administrator również ma wpływ. Administrator nie ma wpływu na przesyłanie w kierunku do administratora, choć mogą się tu pojawić wyjątki, na przykład przesyłanie, o którym decyduje administratora w kierunku od podmiotu przetwarzającego do administratora, jednak kwalifikowałbym to raczej jako przesyłanie wewnątrz administratora. Możliwe jest też, że administrator narzuca sposób przesyłania innemu administratorowi, wtedy należy się poważnie zastanowić, czy naruszenie bezpieczeństwa zostaje popełnione przez administratora czy przez nowego, innego administratora.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zniszczenia** (...) **danych osobowych** (...) **przechowywanych** (...)" wynika, że **drugim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych przechowywanych. Przepis nie wskazuje z jakim przechowywaniem wiąże skutki, wydaje się jednak, że przede wszystkim mowa tu o przechowywaniu danych osobowych przez administratora, wewnątrz jego struktury. Należy uczciwie przyznać, że przepis nie zawiera słów „przechowywanych przez administratora", z czego wynika, że dotyczy on również naruszenia ochrony danych osobowych, przechowywanych nie wewnątrz struktury administratora, ale wewnątrz struktury podmiotu przetwarzającego, nie zapominając przy tym, że przechowywanie przez podmiot przetwarzający można rozumieć też jako przechowywanie przez administratora.

W przypadku naruszeń, które miałyby skutkować zgłoszeniem do PUODO, należy zwracać baczną uwagę na to kto w konkretnych stanach faktycznych i prawnych ma konkretnie zrealizować obowiązek zgłoszenia.

Możliwa jest też sytuacja, w której administrator powierza przetwarzanie pewnych danych, podmiot przetwarzający je przetwarza w imieniu administratora i jednocześnie podmiot przetwarzający jest administratorem tych samych danych. Jeżeli podmiot przetwarzający przechowuje je w sposób skutkujący naruszeniem, to możliwe jest, że jedno naruszenie popełnia dwóch administratorów. Jeśli chodzi o administratora powierzającego, to dokładnie rzecz biorąc popełnia je podmiot przetwarzający, który przetwarza dane osobowe w jego imieniu. Ten właśnie podmiot przetwarzający jest jednocześnie administratorem i popełnia to samo naruszenie.

Wspólne popełnienie naruszenia ochrony danych osobowych możliwe jest też w sytuacji współadministrowania.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zniszczenia** (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **trzecim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zniszczenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. z przepisu wynika, że dotyczy on zniszczenia danych osobowych przetwarzanych w jakikolwiek sposób, o ile tylko przetwarzaniem tym nie jest przesyłanie ani przechowywanie.

W tym przypadku nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany. Ze wszystkich sposobów przetwarzania wydzielono przesyłanie i przechowywanie, potraktowano je tak samo jak pozostałe sposoby przechowywania, zaś przetwarzanie inne niż przesyłanie i przechowywanie potraktowano tak samo jak przesyłanie i przechowywanie. Po co to uczyniono?

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zniszczenia** (...) **danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**" wynika, że możliwym skutkiem naruszenia jest przypadkowe zniszczenie przetwarzanych danych osobowych. Dane osobowe przesyłane, przechowywane i przetwarzane w inny sposób niż przesyłanie i przetwarzane w inny sposób niż przechowywanie to po prostu dane osobowe przetwarzane.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **przypadkowego utracenia** (...) **danych osobowych przesyłanych** (...)" wynika, że **czwartym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe utracenie danych osobowych przesyłanych. Z przepisu nie wynika niestety kto miałby owe dane przypadkowo utracić. Nadawca? Odbiorca? Dostawca usługi przesyłu. Wydaje się, że dane przypadkowo utracić może każdy ze wskazanych podmiotów. Przepis skonstruowany jest tak, że za naruszenie ochrony danych osobowych można uznać sytuację, kiedy to nie administrator ową ochronę naruszył. Wystarczy wyobrazić sobie sytuację przesyłki, przesyłkę wysyła ktoś do administratora i po dotarciu przesyłki do administratora, okazuje się, że utracono przesyłane dane. Administrator nijak nie zawinił a dane utracono, co może pociągać za sobą skutki

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **przypadkowego utracenia** (...) **danych osobowych** (...) **przechowywanych** (...)" wynika, że **piątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe utracenie danych osobowych przechowywanych, zapewne przechowywanych przez administratora.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **utracenia** (...) **danych osobowych** (...) **lub** w **inny sposób przetwarzanych**;" wynika, że szóstym z możliwych skutków naru-

szenia bezpieczeństwa jest przypadkowe utracenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

W tym przypadku po raz drugi nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) **oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **utracenia** (...) **danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**" wynika, że możliwym skutkiem naruszenia jest przypadkowe utracenie przetwarzanych danych osobowych.

Ze słów zaznaczonych w przepisie: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowe**go (...) **zmodyfikowania**, (...) **danych osobowych przesyłanych (**...)" wynika, że siódmym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych przesyłanych.

Zapewne chodzi o przesyłanie przez administratora. Należy jednak zwrócić uwagę na fakt, że jeżeli administrator przesyła dane osobowe, to może to co prawda robić sam, na przykład za pomocą własnego gońca, ale jednak częściej przesyłanie danych osobowych, jak czegokolwiek, odbywa się za pośrednictwem wyspecjalizowanego podmiotu. i tu pojawia się problem. Podmiot taki jest wobec wysyłającego administratora odbiorcą, czyli z własnego punktu widzenia jest on również administratorem. Owszem, administratorem, ale administratorem czego, jakich danych osobowych? Niewątpliwie danych adresowych, zarówno administratora, jak i odbiorcy przesyłki, mam jednak poważną wątpliwość, czy podmiot ten jest również administratorem danych znajdujących się w przesyłce. Wydaje się, że jest to zależne od samej specyfiki usługi. Jeżeli elementem usługi jest przesłanie treści przesyłki, łączące się z zapoznaniem z tą treścią – coś na kształt telegramu (pomijam fakt, że jest to usługa coraz rzadsza, o ile w ogóle jeszcze świadczona).

Ze słów zaznaczonych w przepisie: „**(...) naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zmodyfikowania** (...) **danych osobowych** (...) **przechowywanych** (...)" wynika, że ósmym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych **przechowywanych** przez admini-

stratora. Ze względu na specyfikę czynności przechowywania, nie ma wątpliwości, że zmodyfikowanie to może odbyć się głównie w strukturze administratora. Głównie ale nie wyłącznie, ponieważ zmodyfikowane mogą zostać też dane przechowywane w imieniu administratora przez podmiot przetwarzający.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowe**go (...), **zmodyfikowania**, (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że dziewiątym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe zmodyfikowanie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

W tym przypadku, już po raz trzeci, nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **zmodyfikowania**, (...) **danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**" wynika, że możliwym skutkiem naruszenia jest przypadkowe zmodyfikowanie przetwarzanych danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **nieuprawnionego ujawnienia (...) do danych osobowych przesyłanych**, (...);" wynika, że **dziesiątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.

Tu również administrator może nie być świadom tego naruszenia. Podmiot świadczący usługę przesyłu może być świadom że skutek naruszenia bezpieczeństwa, jakim jest przypadkowe i nieuprawnione ujawnienie danych osobowych mógł mieć miejsce, podmiotem, który może mieć tę świadomość może być również adresat. Jeśli adresat znajduje się w zakresie podmiotowym RODO, to należy się poważnie zastanowić, czy nie powinien rozważyć zgłoszenia naruszenia.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych** (...), **przechowywanych** (...);" wynika, że **jedenastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieupraw-

nione ujawnienie danych osobowych **przechowywanych**. Z uwagi na specyfikę przechowywania, naruszenie to może być popełnione głównie przez administratora, też przez podmiot przetwarzający działający w imieniu administratora, skoro bowiem naruszenia ma dotyczyć danych przechowywanych, to może je popełnić właśnie tylko ten, kto owe dane przechowuje.

Ze słów : „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...), **nieuprawnionego ujawnienia** (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **dwunastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i nieuprawnione ujawnienie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie, czyli przetwarzanych w jakikolwiek sposób, o ile tylko sposobem tym nie jest przesyłanie danych osobowych ani przechowywanie danych osobowych. Należy zwrócić uwagę, że może tu wystąpić naruszenie związane z każdą czynnością przetwarzania danych osobowych, z wyjątkiem ich przechowywania i przesyłania.

Przykładem naruszenia może tu być przypadkowe ujawnienie danych osobowych przez osobę, która tych danych ujawniać nie powinna.

W tym przypadku (po raz czwarty) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „**naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) nieuprawnionego ujawnienia (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest przypadkowe i nieuprawnione ujawnienie przetwarzanych danych osobowych.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **nieuprawnionego dostępu do danych osobowych przesyłanych**, (...);" wynika, że **trzynastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych **przesyłanych**.

Przypadkowy nieuprawniony dostęp do przesyłanych danych osobowych może zostać dokonany przez administratora, kiedy dane mu przesłane do niego dotrą i zapozna się z nimi w sposób przypadkowy osoba nieuprawniona. Przypadkowy nieuprawniony dostęp do prze-

syłanych danych osobowych może zostać dokonany przez kogoś kto zapoznaje się z danymi podczas ich transferu od administratora – nadawcy do adresata.

Przykładem może być tu zapoznanie się z danymi przez osobę inną niż adresat przesyłki z danymi, przeczytanie cudzego listu, cudzego emaila.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **nieuprawnionego dostępu do danych osobowych** (...), **przechowywanych** (...)" wynika, że **czternastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych **przechowywanych**.

Dane osobowe są zwykle przechowywane przez administratora lub przez podmiot przetwarzający, w związku z tym, w strukturze tych podmiotów może zajść opisywane naruszenie.

Przypadkowy, nieuprawniony dostęp do przechowywanych danych osobowych może zostać dokonany zwłaszcza w strukturze administratora. Administrator nie dopilnowuje przechowywanych danych i ktoś nieuprawniony uzyskuje do tych danych dostęp.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...)**nieuprawnionego dostępu do danych osobowych** (...)**lub w inny sposób przetwarzanych**;" wynika, że **piętnastym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

Przykładem naruszenia może tu być przypadkowe uzyskanie dostępu do danych osobowych przez osobę, która tego dostępu uzyskać nie powinna – przez osobę trzecią. Wydaje się, że o ile dostęp uzyskuje osoba trzecia, o tyle przypadkowość działań dotyczy raczej działań ADO.

W tym przypadku, po raz piąty, również nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego** (...) **nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**"

wynika, że możliwym skutkiem naruszenia jest przypadkowy i nieuprawniony dostęp do przetwarzanych danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem zniszczenia** (...) **danych osobowych przesyłanych**, (...);" wynika, że **szesnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych przesyłanych.

O przesyłaniu danych osobowych można tu mówić, kiedy opuszczają one strukturę administratora. Dane, których jeszcze nie wysłano, to nie są dane przesyłane, ale są to dane przechowywane. Zniszczenie może zatem mieć miejsce podczas transferu. Czy wymienione w przepisie zniszczenie może mieć miejsce u adresata – trudno orzec, jednak raczej nie, ponieważ dane osobowe, które dotarły do adresata to już nie są dane osobowe przesyłane, to już są dane osobowe, które są przechowywane.

Przykładem może być zniszczenie danych w przesyłce przez operatora pocztowego, przez dostawcę usługi poczty elektronicznej. Bardzo poważnie należy się tu zastanowić nad niszczeniem zawirusowanych maili. Godzące w rozsądek by było, gdybym twierdził, że nie wolno usuwać wirusów a czasem i zawirusowanych wiadomości, jednak trudno orzec jak uzasadnić to na gruncie RODO – można tu próbować użyć zasady integralności danych osobowych lub zasady poufności danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem zniszczenia**, (...),**danych osobowych** (...) **przechowywanych** (...);" wynika, że **siedemnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych przechowywanych.

Niezgodne z prawem zniszczenie przechowywanych danych osobowych może zostać dokonane zwłaszcza w strukturze ADO.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** przypadkowego lub **niezgodnego z prawem zniszczenia**, (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **osiemnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zniszczenie danych osobowych przetwarzanych

w sposób inny niż przesyłanie lub przechowywanie, czyli poza tym dwiema czynnościami – przetwarzanych w jakikolwiek sposób.

W tym przypadku (po raz szósty) również nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem zniszczenia (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**" wynika, że możliwym skutkiem naruszenia jest niezgodne z prawem zniszczenie danych osobowych, które są przetwarzane w dowolny sposób.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **utracenia**(...) **danych osobowych przesyłanych** (...)" wynika, że **dziewiętnastym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych przesyłanych.

Utracenie danych osobowych należy odróżnić od ich zniszczenia, ponieważ prawodawca użył dwóch różnych słów. Problemem jest fakt, że trudno jest wskazać różnicę miedzy zniszczeniem danych osobowych a utraceniem danych osobowych. Wydaje się, że przez utracenie należy rozumieć coś na kształt utracenia kontroli nad danymi, coś na kształt zagubienia tych danych. Administrator wysyła dane, dostawca usługi pocztowej (też usługi poczty elektronicznej) je transportuje, dane nie docierają do adresata. Z danymi coś się stało. Postaje pytanie czy zostały one zniszczone czy utracone. Wydaje się, że jeżeli dane po prostu zaginęły, ale nie wiadomo co się z nimi stało, to raczej zostały one utracone niż zniszczone. Należy uznać, że dane zostały zniszczone jeżeli rzeczywiście zostały zniszczone, jeżeli nie wiadomo co się z nimi stało, to należy uznać, że zostały utracone.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...), **utracenia**, (...) **danych osobowych** (...), **przechowywanych** (...)" wynika, że **dwudziestym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych przechowywanych.

Skoro utracenie to inne zdarzenie niż zniszczenie, to przez utracenie przechowywanych danych należy rozumieć zagubienie danych przechowywanych przez administratora lub przez podmiot przetwarzający.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...), **utracenia**, (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **dwudziestym pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem utracenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. Przez utracenie danych osobowych, o którym mowa jest w przepisie należy zapewne rozumieć zagubienie danych przy wykonywaniu czynności przetwarzania danych, innych niż przesyłanie lub przechowywanie tych danych.
I w tym przypadku – po raz siódmy - nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) naruszenie bezpieczeństwa prowadzące do (...) niezgodnego z prawem (...) utracenia (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest niezgodne z prawem utracenie przetwarzanych danych osobowych.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **zmodyfikowania**, (...) **danych osobowych przesyłanych**, (...)" wynika, że **dwudziestym drugim** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych **przesyłanych**. Przez zmodyfikowanie przesyłanych danych osobowych należy rozumieć zmodyfikowanie tych danych w trakcie trwania przesyłania (pocztą, pocztą elektroniczną, kurierem), czyli zmodyfikowanie przez podmioty znajdujące się poza strukturą administratora. Możliwe jest też zmodyfikowanie danych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzają cego do kogokolwiek.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...), **zmodyfikowania**, (...)**danych osobowych** (...), **przechowywanych** (...);" wynika, że **dwudziestym trzecim** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych **przechowywanych**. W przepisie zapewne mowa jest o przechowywaniu danych przez administratora lub przez podmiot przetwarzający. Przez niezgodne z prawem zmodyfikowanie danych

osobowych przechowywanych należy rozumieć takie ich zmodyfikowanie, które zaszło bez upoważnienia i bez polecenia administratora, lub za upoważnieniem ale bez polecenia administratora. Przez niezgodne z prawem zmodyfikowanie danych osobowych należy rozumieć zmodyfikowanie danych z naruszeniem zasady integralności.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...)**niezgodnego z prawem** (...) **zmodyfikowania**, (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **dwudziestym czwartym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

W tym przypadku (po raz ósmy) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „**oznacza naruszenie bezpieczeństwa prowadzące do** (...) niezgodnego z prawem (...) zmodyfikowania (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest przypadkowe i nieuprawnione zmodyfikowanie przetwarzanych danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych przesyłanych**, przechowywanych lub w inny sposób przetwarzanych;" wynika, że dwudziestym piątym z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych **przesyłanych**. Naruszenie o którym mowa w przepisie to ujawnienie danych, które jest niezgodne z prawem i nieuprawnione i dotyczy danych osobowych, które są przesyłane.

Możliwe jest niezgodne z prawem i nieuprawnione ujawnienie danych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych** (...), **przecho-**

wywanych (...)" wynika, że dwudziestym szóstym z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych **przechowywanych**. Naruszenie o którym mowa w przepisie to ujawnienie danych, które jest niezgodne z prawem i nieuprawnione i dotyczy danych osobowych, które są przechowywane.

Możliwe jest niezgodne z prawem i nieuprawnione ujawnienie danych podczas ich przechowywania przez administratora lub przez podmiot przetwarzający. Niezgodne z prawem i nieuprawnione ujawnienie to ujawnienie z naruszeniem zasady zgodności z prawem i zasady poufności. Patrząc operacyjnie, jest to takie ujawnienie, nad którym nie sprawuje świadomej kontroli administrator.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **dwudziestym siódmym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. Naruszenie o którym mowa w przepisie to ujawnienie danych, które jest niezgodne z prawem i nieuprawnione i dotyczy danych osobowych, które są przetwarzane w sposób inny niż przesyłanie lub przechowywanie.

W tym przypadku (po raz dziewiąty) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „oznacza naruszenie bezpieczeństwa prowadzące do (...) niezgodnego z prawem (...) nieuprawnionego ujawnienia (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest niezgodne z prawem i nieuprawnione ujawnienie przetwarzanych danych osobowych.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...)**niezgodnego z prawem** (...) **nieuprawnionego dostępu do danych osobowych przesyłanych** (...)" wynika, że **dwudziestym ósmym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych **przesyłanych**.

Naruszenie o którym mowa w przepisie to nieuprawniony dostęp do danych osobowych, które są przesyłane. Możliwy jest nieuprawniony dostęp do danych osobowych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek. Nieuprawniony dostęp do danych osobowych, które są przesyłane to dostęp z naruszeniem zasady minimalizacji i zasady poufności. Jest to taki dostęp, nad którym nie sprawuje świadomej kontroli administrator, ani podmiot przetwarzający ani podmiot z którego usług do przesyłania administrator lub podmiot przetwarzający korzysta.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **nieuprawnionego dostępu do danych osobowych** (...), **przechowywanych** (...);" wynika, że **dwudziestym dziewiątym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych **przechowywanych**. Naruszenie o którym mowa w przepisie to nieuprawniony dostęp do danych osobowych, które są przechowywane.

Możliwy jest nieuprawniony dostęp do danych osobowych podczas ich przechowywania przez administratora lub przez podmiot przetwarzający. Nieuprawniony dostęp do danych osobowych, które są przechowywane to dostęp z naruszeniem zasady zgodności z prawem i zasady minimalizacji i zasady poufności. Jest to taki dostęp, nad którym nie sprawuje świadomej kontroli administrator, ani podmiot przetwarzający ani podmiot z którego usług do przesyłania administrator lub podmiot przetwarzający korzysta. Przez nieuprawniony dostęp do danych przechowywanych należy też rozumieć dostęp bez upoważnienia i bez polecenia administratora, lub za upoważnieniem ale bez polecenia administratora lub bez upoważnienia podmiotu przetwarzającego i bez polecenia administratora lub bez upoważnienia administratora lub bez polecenia podmiotu przetwarzającego.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do** (...) **niezgodnego z prawem** (...) **nieuprawnionego dostępu do danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **trzydziestym** z możliwych skutków naruszenia bezpieczeństwa jest niezgodny z prawem i nieu-

prawniony dostęp do danych osobowych danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

Naruszenie o którym mowa w przepisie to nieuprawniony dostęp do danych osobowych, które są przetwarzane w sposób inny niż przesyłanie i przechowywanie.

Możliwy jest nieuprawniony dostęp do danych osobowych podczas ich przetwarzania przez administratora lub przez podmiot przetwarzający. Nieuprawniony dostęp do danych osobowych, które są przetwarzane to dostęp z naruszeniem zasady zgodności z prawem i zasady minimalizacji i zasady poufności. Jest to taki dostęp, nad którym nie sprawuje świadomej kontroli administratora, ani podmiot przetwarzający ani podmiot z którego usług do przesyłania administratora lub podmiot przetwarzający korzysta. Przez nieuprawniony dostęp do danych przetwarzanych należy też rozumieć dostęp bez upoważnienia i bez polecenia administratora, lub za upoważnieniem ale bez polecenia administratora lub bez upoważnienia podmiotu przetwarzającego i bez polecenia administratora lub bez upoważnienia administratora lub bez polecenia podmiotu przetwarzającego.

W tym przypadku (po raz już dziesiąty) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) oznacza naruszenie bezpieczeństwa prowadzące do (...) niezgodnego z prawem (...) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest niezgodne z prawem i nieuprawnione ujawnienie przetwarzanych danych osobowych.

Ze słów: „ (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia**, (...) **danych osobowych przesyłanych** (...);" wynika, że **trzydziestym pierwszym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych. Przepis niestety nie wskazuje z jakim przesyłaniem wiąże skutki. Czy mowa tu o przesyłaniu w kierunku od administratora, czy mowa tu o przesyłaniu do administratora, czy mowa tu o przesyłaniu wewnątrz administratora.

Ze słów: „ (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia**, (...) **danych**

osobowych (...), **przechowywanych** (...);" wynika, że **trzydziestym drugim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych. Przepis nie wskazuje z jakim przechowywaniem wiąże skutki, wydaje się jednak, że przede wszystkim mowa tu o przechowywaniu danych osobowych przez administratora, wewnątrz jego struktury. Należy uczciwie przyznać, że przepis nie zawiera słów „przechowywanych przez administratora", z czego wynika, że dotyczy on również naruszenia ochrony danych osobowych, przechowywanych nie wewnątrz struktury administratora, ale wewnątrz struktury podmiotu przetwarzającego.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia** (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że **trzydziestym trzecim** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie..

W tym przypadku (już po raz jedenasty) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest przypadkowe lub niezgodne z prawem zniszczenie przetwarzanych danych osobowych.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...), **utracenia**, (...) **danych osobowych przesyłanych**, (...)" wynika, że **trzydziestym czwartym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przesyłanych.

Możliwe jest utracenie danych osobowych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek. Możliwe jest utracenie **przesyłanych** danych, które jest tylko przypadkowe – zagubienie przesyłanych danych jednak w sytuacji, w której nikt się z nimi nie zapoznaje – naruszona jest co najwyżej zasada ograniczenia czaso-

wego i zasada ograniczenia celu, choć nie wykluczam, ze immanentną cechą takiego utracenia jest też jego niezgodność z prawem.

Możliwe jest utracenie **przesyłanych** danych, które jest tylko niezgodne z prawem – możliwe ale mało prawdopodobne – administrator, lub inny podmiot doprowadza świadomie to utracenia danych – naruszona jest zasada zgodności z prawem ponieważ czynność tracenia, gubienia danych, ciężko jest osadzić w art. 6 RODO lub w art. 9 RODO.

Możliwe jest utracenie **przesyłanych** danych, które jest przypadkowe i niezgodne z prawem – nieświadome zagubienie danych, nieosadzalne w art. 6 RODO lub w art. 9 RODO.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...), **utracenia**, (...)**danych osobowych** (...), **przechowywanych** (...)" wynika, że **trzydziestym piątym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przechowywanych. Ze względu na konstrukcję przepisu należy odróżnić utracenie danych przypadkowe od utracenia danych niezgodnego z prawem, od utracenia danych przypadkowego i niezgodnego z prawem. O wszystkich tych typach utracenia danych tu mowa. O samym utraceniu danych piszę wyżej (dziewiętnasty ze skutków). Pokrótce, utracenie danych osobowych to ich zagubienie. Niezgodne z prawem utracenie danych to utracenie ze złamaniem zasady zgodności z prawem. Zagubienie - utracenie, z uwagi na swój niespodziewany charakter jest chyba zwykle niezgodne z zasadą zgodności z prawem. Zwykle, bo może się jednak okazać, że zagubiono dane, których administrator mieć nie powinien. Co prawda ich nie zniszczono, ale danych nie ma, czy też raczej administrator nie wie gdzie one są. Wtedy utracenie wydaje się być utraceniem przypadkowym ale niekoniecznie niezgodnym z prawem. Utracenie jednocześnie przypadkowe i niezgodne z prawem to zapewne przypadkowe, nieplanowane przez administratora utracenie danych, które to dane administratora powinien nadal mieć. Utracenie o jakim mowa w przepisie to utracenie przez administratora lub przez PP.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **utracenia**, (...) **danych osobowych** (...) **lub w inny**

sposób przetwarzanych;" wynika, że **trzydziestym szóstym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem utracenie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. Przez utracenie danych osobowych, o którym mowa jest w przepisie należy zapewne rozumieć utracenie - zagubienie danych przy wykonywaniu czynności przetwarzania danych, innych niż przesyłanie lub przechowywanie tych danych osobowych.

W tym przypadku po raz dwunasty nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" wynika, że możliwym skutkiem naruszenia jest przypadkowe i nieuprawnione ujawnienie przetwarzanych danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **zmodyfikowania**, (...) **danych osobowych przesyłanych** (...)" wynika, że **trzydziestym siódmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych **przesyłanych**. Możliwe jest zmodyfikowanie danych osobowych podczas ich przesyłania od administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.

Możliwe jest zmodyfikowanie **przesyłanych** danych, które jest tylko przypadkowe – zmodyfikowanie przesyłanych danych jednak w sytuacji, w której fakt zmodyfikowania danych zostaje wykryty, niezmodyfikowanie dane zostają dostarczone nieco później niż zmodyfikowane – naruszona jest co najwyżej zasada prawidłowości i zasada integralności, choć i tu nie wykluczam, że immanentną cechą takiego zmodyfikowania danych osobowych jest też jego niezgodność z prawem.

Możliwe jest zmodyfikowanie **przesyłanych** danych, które jest tylko niezgodne z prawem – możliwe ale mało prawdopodobne – administrator, lub inny podmiot doprowadza świadomie do zmody-

fikowania danych – naruszona jest zasada zgodności z prawem. Możliwe jest zmodyfikowanie **przesyłanych** danych, które jest przypadkowe i niezgodne z prawem – nieświadome zagubienie danych, nieosadzalne w art. 6 RODO lub w art. 9 RODO.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **zmodyfikowania**(...) **danych osobowych** (...) **przechowywanych**(...)" wynika, że **trzydziestym ósmym** z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych **przechowywanych**.

Możliwe jest zmodyfikowanie danych osobowych podczas ich przechowywania przez administratora (danych) lub przez podmiot przetwarzający.

Możliwe jest zmodyfikowanie **przechowywanych** danych, które jest tylko przypadkowe – zmodyfikowanie **przechowywanych** danych jednak w sytuacji, w której fakt zmodyfikowania danych zostaje wykryty, dane zostają przywrócone do właściwej treści np. z kopii bezpieczeństwa – naruszona jest co najwyżej zasada prawidłowości i zasada integralności. Jeżeli naruszeniu przeciwdziałano, to złamanie zasady zgodności z prawem jest mało prawdopodobne.

Możliwe jest zmodyfikowanie **przechowywanych** danych, które jest tylko niezgodne z prawem – administrator, lub podmiot przetwarzający doprowadza świadomie do zmodyfikowania danych – naruszona jest zasada zgodności z prawem, zachodzi tu świadome zmodyfikowanie danych, nieosadzalne w art. 6 RODO lub w art. 9 RODO, ponieważ popełnione przez administratora w celu manipulacji danymi, ich sfałszowania itd.

Możliwe jest zmodyfikowanie **przechowywanych** danych, które jest przypadkowe i niezgodne z prawem – administrator lub podmiot przetwarzający doprowadza nieświadomie do zmodyfikowania danych osobowych, które zmodyfikowane być nie powinny, zachodzą przypadkowe zmiany w posiadanych danych osobowych.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **zmodyfikowania**, (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że trzydziestym dziewiątym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem zmodyfiko-

wanie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie. Przez przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych, o którym mowa w tej części przepisu należy rozumieć zmodyfikowanie danych przechowywanych przez administratora lub przez PP, które dokonuje się w jakikolwiek sposób, z wyjątkiem przesyłania i z wyjątkiem przechowywania.

Możliwe jest zmodyfikowanie danych osobowych **przetwarzanych inaczej niż przez przesyłanie i przechowywanie**, które jest tylko przypadkowe – niedbałe zebranie danych, po którym jednak następuje ich poprawienie, tak, że nie są przechowywane błędne dane, pobrani przypadkowych danych, jednak bez pobrania danych, których administratorowi pobierać nie wolno. Możliwe jest zmodyfikowanie danych osobowych **przetwarzanych inaczej niż przez przesyłanie i przechowywanie**, które jest tylko niezgodne z prawem – zmiana treści danych przez (np. bez upoważnienia). Możliwe jest zmodyfikowanie danych osobowych **przetwarzanych inaczej niż przez przesyłanie i przechowywanie**, które jest przypadkowe i niezgodne z prawem na przykład zmodyfikowanie danych zapisywanych w ten sposób, że administrator nie we, że dane osobowe zostały zmodyfikowane, zatem po takim zdarzeniu przechowuje dane z naruszenie zasady prawidłowości.

W tym przypadku (po raz trzynasty) nasuwa się refleksja, czy przepis nie został niepotrzebnie skomplikowany.

Nie naruszając znaczenia przepisu można stwierdzić, że ze słów: „(...) naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem (...) zmodyfikowania (...) danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;" wynika, że możliwym skutkiem naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem zmodyfikowanie przetwarzanych danych osobowych.

Ze słów: „**naruszenie ochrony danych osobowych**" (...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych przesyłanych**, (...)" wynika, że czterdziestym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych **przesyłanych**.

Możliwe jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych podczas ich przesyłania od

administratora do podmiotu przetwarzającego lub od administratora lub podmiotu przetwarzającego do kogokolwiek.

Możliwe jest ujawnienie **przesyłanych** danych osobowych, które jest tylko przypadkowe i nieuprawnione – przyznam, że trudno jest znaleźć przykład, w którym ujawnienie danych osobowych jest przypadkowe i nieuprawnione ale nie jest niezgodne z prawem. Jeżeli przetwarzanie, tu ujawnienie, jest nieuprawnione, to wydaje się, że tym samym jest ono niezgodne z prawem. Z analizy przepisu wynika, że możliwe jest ujawnienie nieuprawnione i zgodne z prawem, jednak, jak stwierdziłem wyżej – o przykład trudno.

Możliwe jest ujawnienie **przesyłanych** danych osobowych, które jest tylko niezgodne z prawem i nieuprawnione - nieuprawniony do przetwarzania danych osobowych pracownik przedsiębiorstwa transportującego przesyłkę, celowo zapoznaje się z treścią stanowiącej ją wiadomości. Nieuprawniony do przetwarzania danych osobowych danej kategorii pracownik administratora, który dostarcza przesyłki na pocztę, celowo i świadomie zapoznaje się z treścią jednej z nich, zawierającej dane osobowe.

Możliwe jest ujawnienie **przesyłanych** danych osobowych, które jest przypadkowe i niezgodne z prawem i nieuprawnione - nieuprawniony do przetwarzania danych osobowych pracownik przedsiębiorstwa transportującego przesyłkę, przypadkowo zapoznaje się z treścią stanowiącej ją wiadomości. Nieuprawniony do przetwarzania danych osobowych danej kategorii pracownik administratora, który dostarcza przesyłki na pocztę, przypadkowo, np. wskutek rozdarcia koperty, zapoznaje się z treścią jednej z nich, zawierającej dane osobowe.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych** (...), **przechowywanych** lub w inny sposób przetwarzanych;" wynika, że czterdziestym pierwszym z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych **przechowywanych**.

Możliwe jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych podczas ich przechowywania przez administratora lub przez podmiot przetwarzający.

Możliwe jest ujawnienie **przechowywanych** danych osobowych, które jest tylko przypadkowe i nieuprawnione – podobnie jak

w pozycji czterdziestej – trudno jest odnaleźć w umyśle przykład na ujawnienie danych osobowych, które jest przypadkowe (to nietrudno) ale które jest też nieuprawnione i które jednocześnie nie jest niezgodne z prawem. Dopuszczam, że takie zdarzenie jest możliwe, na ten moment go sobie jednak nie wyobrażam.

Możliwe jest ujawnienie **przechowywanych** danych osobowych, które jest tylko niezgodne z prawem i nieuprawnione – nieuprawniony do przetwarzania danej kategorii danych w danym zakresie, zwłaszcza do ujawniania danych, pracownik szpitala wydaje kopię dokumentacji medycznej, osobie nieupoważnionej i nie posiadającej innego źródła uprawnienia, do dostępu do tejże dokumentacji.

Możliwe jest ujawnienie **przechowywanych** danych osobowych, które jest przypadkowe i niezgodne z prawem i nieuprawnione – pracownik administratora (danych) nieuprawniony do udostępniania danych osobowych udostępnia je w sposób przypadkowy osobie nieuprawnionej, na przykład sprzątaczka w przedsiębiorstwie wyrzuca na śmietnik dokumenty zawierające dane osobowe i ktoś się z owymi danymi zapoznaje.

Ze słów: „(...) **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem** (...) **nieuprawnionego ujawnienia** (...) **danych osobowych** (...) **lub w inny sposób przetwarzanych**;" wynika, że czterdziestym drugim z możliwych skutków naruszenia bezpieczeństwa jest przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w sposób inny niż przesyłanie lub przechowywanie.

Możliwe jest przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych podczas ich przetwarzania przez administratora lub przez PP w sposób inny niż przechowywanie lub przesyłanie.

Możliwe jest ujawnienie danych osobowych **przetwarzanych w sposób** inny niż przesyłanie lub przechowywanie, które jest tylko przypadkowe i nieuprawnione – tu również mam wątpliwość co do przykładu, nieuprawnioność ujawnienia zdaje mi się łączyć z niezgodnością z prawem tegoż ujawnienia.

Możliwe jest ujawnienie danych osobowych **przetwarzanych w sposób** inny niż przesyłanie lub przechowywanie, które jest tylko niezgodne z prawem i nieuprawnione - ujawnienie danych osobowych przez osobę, która je zbiera bez upoważnienia czy inaczej skonstruo-

wanego uprawnienia do przetwarzania i przy tym nieuważnie dane jednej osoby, od której zbiera dane ujawnia innej osobie.

Możliwe jest ujawnienie danych osobowych **przetwarzanych w sposób** inny niż przesyłanie lub przechowywanie, które jest przypadkowe i niezgodne z prawem i nieuprawnione – ze względu na prawdopodobną zbieżność ujawnienia niezgodnego z prawem z ujawnieniem nieuprawnionym, adekwatny jest tu przykład tuż wyżej.

Ogólnie – pracownik administratora (danych) przetwarza dane osobowe jednak w sposób inny niż przechowywanie i przesyłanie i przy okazji przetwarzania, ujawnia te dane osobowe mimo, że nie jest do tego uprawniony.

3. Art. 6. pkt 12. Uwagi
3.1. Art. 4. pkt 12. Uwaga 1.
Konkretyzacja obowiązku zgłoszenia naruszenia

Trafnie zauważają P. Litwiński, P. Barta i M. Kawecki,[373] że „Pojęcie naruszenia ochrony danych osobowych związane jest z obowiązkiem zgłaszania przypadków naruszenia bezpieczeństwa danych osobowych organowi nadzorczemu, o którym mowa w art. 33 RODO." Podkreślam jednak fakt, że jeżeli ma miejsce naruszenie z art. 4 pkt 12 RODO, to samo zaistnienie naruszenia bezpieczeństwa danych nie skutkuje pojawieniem się obowiązku zgłoszenia czegokolwiek organowi nadzorczemu. To czy naruszenie należy zgłosić organowi nadzorczemu czy zgłaszać go nie należy zależy od tego czy prawdopodobne jest, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli jest to mało prawdopodobne że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych to naruszenie takie nie podlega zgłoszeniu do organu nadzoru. Obowiązek zgłoszenia szerzej omawiam w kolejnej publikacji z cyklu, przy okazji omawiania art. 33 RODO i art. 34 RODO.

[373] P. Litwiński, P. Barta, M. Kawecki. [w:] P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 235.

Zachodzi naruszenie z art. 4 ust 12 RODO

- i jednocześnie naruszenie z art. 4 ust. 12 RODO nie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych lub jest to mało prawdopodobne że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
  - Administrator nie ma obowiązku zgłoszenia naruszenia. Wynika to z art. 33 ust. 1 RODO.

Zachodzi naruszenie z art. 4 ust 12 RODO

- i jednocześnie jest to prawdopodobne że naruszenie z art. 4 ust 12 RODO skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych lub naruszenie to naruszyło prawa lub wolności osób fizycznych.
  - Administrator ma obowiązek zgłoszenia naruszenia. Wynika to z art. 33 ust. 1 RODO.
- i jednocześnie naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
  - Administrator ma obowiązek bez zbędnej zwłoki zawiadomić o naruszeniu osobę, której dane dotyczą. Wynika to z art. 34 ust. 1 RODO. Obowiązek zawiadomienia osoby, której dane dotyczą nie zachodzi jeżeli zachodzi jedna z sytuacji opisanych w art. 34 ust. 3 RODO.

3.2. Art. 4. pkt 12. Uwaga 2.
Brak obowiązku zgłoszenia naruszenia praw lub wolności jednej osoby fizycznej

Istotnym problemem jest odpowiedź na pytanie o to czy należy zgłaszać naruszenie praw lub wolności jednej osoby.

Z art. 33 ust 1 RODO wynika, że jeżeli jest to prawdopodobne, że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych to administrator danych ma obowiązek zgłosić takie naruszenie ochrony danych osobowych organowi nadzorczemu.

Jeżeli zatem jest to mało prawdopodobne że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych to administrator danych ma obowiązek nie

zgłaszać takiego naruszenia, czyli po prostu nie ma obowiązku zgłaszać takiego naruszenia.

Zwracam szczególną uwagę na fakt że w artykule 33 ust. 1 RODO mowa jest o prawach i wolnościach osób fizycznych. Skoro przepis stanowi o osobach fizycznych to wynika z niego, że osób tych o których stanowi przepis musi być co najmniej dwie. Jeżeli zatem administrator danych stwierdzi że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności jednej osoby fizycznej to naruszenie takie nie podlega zgłoszeniu do organu nadzorczego.

Dyskusje prowadzone przeze mnie przy różnych okazjach przekonały mnie, że interpretacja, zgodnie z którą, z art. 33 ust. 1 RODO nie wynika obowiązek zgłoszenia naruszenia ochrony danych osobowych jeżeli skutkuje ono ryzykiem naruszenia praw lub wolności jednej osoby fizycznej, nasunęły mi myśl o dodatkowym uzasadnieniu tego poglądu. Uważam, że za interpretacją taką, moim zdaniem jedyną prawidłową, przemawia kilka argumentów, które wymieniam poniżej. Nie omawiam ich szczegółowo, zagadnienia te poruszone są również w komentarzu do art., 33 RODO.

Argument 1.

W polskiej wersji językowej RODO widnieją słowa: *(...) to skutkowało ryzykiem naruszenia praw lub wolności* ***osób*** *fizycznych (...)* (wytłuszczenie: J. Rz.).

Argument 2.

W angielskiej wersji językowej RODO widnieją słowa: *(...) is unlikely to result in a risk to the rights and freedoms of natural* ***persons*** *(...)* (wytłuszczenie: J. Rz.).

Argument 3.

W czeskiej wersji językowej RODO widnieją słowa: *(...) že by toto porušení mělo za následek riziko pro práva a svobody fyzických* ***osob*** *(...)* (wytłuszczenie: J. Rz.).

Argument 4.

W niemieckiej wersji językowej RODO widnieją słowa: *(...) zu einem Risiko für die Rechte und Freiheiten natürlicher* ***Personen*** *führt (...)* (wytłuszczenie: J. Rz.).

Jak widać, w wskazanych wersjach językowych mowa jest o osobach fizycznych, nie zaś o osobie fizycznej, co jest dla mnie argumentem podstawowym a przynajmniej jednym z kilku.

Argument. 5.

Uważam, że nie ma powodu by uznać, że ryzyko naruszenia praw lub wolności już jednej osoby fizycznej skutkuje obowiązkiem zgłoszenia tego naruszenia. Uważam tak na podstawie przytoczonych czterech wersji językowych. Dalsze studia językowe w tym kierunku uważam za niecelowe. Nie widzę argumentu, który przemawiałby za interpretowanie słowa „osób" jako „jednej osoby".

Argument 6.

Uważam, że odrzucenie wniosku zgodnie z którym ryzyko naruszenia praw lub wolności jednej osoby fizycznej nie skutkuje obowiązkiem zgłoszenia tego naruszenia nie wynika z zastosowania zasady wykładni prawa znanej jako „argumentum ad absurdum". Zasada ta w ujęciu L. Morawskiego brzmi: „Należy odrzucić taką interpretację przepisów która prowadzi do absurdalnych lub niemożliwych do zaakceptowania konsekwencji.".[374] Uważam że zasady tej nie można zastosować do takiej interpretacji komentowanego przepisu, z której wynikałoby że naruszenie praw lub wolności jednej osoby fizycznej podlega zgłoszeniu do organu nadzoru. Uważam że właśnie taka interpretacja byłaby absurdalna, prawodawca uznał że zgłoszeniu do organu nadzoru podlega naruszenie ochrony danych osobowych prowadzące do naruszenia praw lub wolności więcej niż jednej osoby fizycznej, co wydaje się jak najbardziej racjonalne. Jeżeli ma miejsce naruszenie praw lub wolności jednej osoby fizycznej i to w dodatku, o czym należy pamiętać, ma miejsce naruszenie praw lub wolności które administrator odnotował, to informowanie organu nadzoru o takim naruszeniu jest bezprzedmiotowe. Bezprzedmiotowe ponieważ naruszenie takie w gruncie rzeczy ma charakter błahy. z punktu widzenia osoby której dane dotyczą można je być może uznać za doniosłe, jednak z punktu widzenia ochrony danych u danego administratora, jak również z punktu widzenia ochrony danych rozumiane jako gałąź prawa, naruszenie takie ma charakter pomijalny i jako takie nie powinno być zgłaszane organowi nadzoru.

Argument 7.

W motywie 74 Preambuły RODO widnieją słowa: „(…) ryzyko naruszenia praw i wolności osób fizycznych (…)". Analogiczne słowa, również zawierające liczbę mnogą w odniesieniu do osób

[374] L. Morawski. *Zasady wykładni prawa.* Toruń 2006 s. 150.

fizycznych widnieją w angielskiej, czeskiej i niemieckiej wersji językowej RODO.

Argument 8.

W motywie 75 Preambuły RODO widnieją słowa: *Ryzyko naruszenia praw lub wolności osób (...) jeżeli osoby, których dane dotyczą, (...)*. Analogiczne słowa, również zawierające liczbę mnogą w odniesieniu do osób fizycznych widnieją w angielskiej, czeskiej i niemieckiej wersji językowej RODO. w wersji angielskiej widnieje: *The risk to the rights and freedoms of natural persons (...) where data subjects (...)*. Odpowiednikiem „osób, których dane dotyczą są w wersji angielskiej „data subjects" czyli podmioty danych, co merytorycznie nic nie zmienia, zwracam jednak uwagę, na fakt, że owe podmioty danych występują w liczbie mnogiej. Podobnie w wersji czeskiej widnieją: „subjekty údajů" czyli podmioty danych, również w liczbie mnogiej. Z kolei w wersji niemieckiej widnieją: „die betroffenen Personen" czyli wspomniane osoby, również zdecydowanie w liczbie mnogiej.

W motywie 76 Preambuły RODO widnieje: *Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych*, uważam jednak, że z przepisu wynika, iż przy ocenianiu ryzyka należy brać pod uwagę ryzyko naruszenia praw lub wolności każdej z osób, ponadto przepis ten raczej odnosi się do art. 34 RODO, czyli do informowania o naruszeniu osób, których dane dotyczą.

3.3. Art. 4. pkt 12.Uwaga 3.
Konkretyzacja obowiązku zgłoszenia naruszenia

Na stronie PUODO umieszczona jest definicja naruszenia ochrony danych osobowych. Uważam, ze definicja ta stanowi błędną interpretację art. 4 ust. 12 RODO. Cytuję stronę PUODO:

Aby zaistniało naruszenie muszą być spełnione łącznie trzy przesłanki:

- *naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie;*
- *skutkiem* ***naruszenia musi być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych****;* (wytłuszczenie: J. Rz.)

- naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.[375]

Podejście zaprezentowane na stronie PUODO i dostępne tam jeszcze na pewno 15 marca 2019 roku jest wygodne dla ADO i dla PUODO. Dla ADO szczególnie korzystne jest stwierdzenie: *skutkiem naruszenia musi być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych*. PUODO, jak widać reprezentuje stanowisko, zgodnie z którym naruszenie ochrony danych osobowych zachodzi, kiedy zagrożenia wymienione w przepisie się zrealizują, ja uważam, że naruszenie bezpieczeństwa zachodzi również wtedy, kiedy pojawia się jedynie ryzyko zaistnienia tych zagrożeń. W przepisie widnieją słowa: *(...) naruszenie bezpieczeństwa* ***prowadzące do*** *(...) zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych (...)* (wytłuszczenie: J. Rz.). Szczególną uwagę zwracam na słowa, które wytłuściłem, czyli: *prowadzące do*. Gdyby naruszeniem miałoby być tak jak głosi PUODO jedynie: ***zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych***, to zapewne przepis zawierałby słowa: „(…) naruszenie bezpieczeństwa, które doprowadziło **do** (…)". Jak widać nie zawiera. „Opisane tu rozumienie naruszenia jest wygodne dla PUODO, skutkuje bowiem mniejszą ilością zgłoszeń, niż gdyby naruszenie rozumiano szerzej."[376]

Trudno jest mi jednoznacznie wskazać, czy błędna definicja naruszenia ochrony danych osobowych, nadal widnieje na stronie PUODO. Podczas pisania niniejszych słów i tuż przed ostateczną redakcją niniejszego komentarza szukałem ich tam i nie znalazłem,

[375] https://uodo.gov.pl/pl/134/228 (dostęp: 2019.03.15. godz. 21.24).

[376] Rozważania od: *Na stronie PUODO umieszczona jest definicja (...)* do cytatu: *Opisane tu rozumienie naruszenia jest wygodne dla PUODO, skutkuje bowiem mniejszą ilością zgłoszeń, niż gdyby naruszenie rozumiano szerzej* swój początek mają w rozważaniach, które poprowadziłem w książce wydanej w 2019 roku. (J. Rzymowski RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora. Kraków 2019.)

Cytat zamieszczam jako swoisty znak czasu, nie wiem czy rozważania moje, prowadzone w książce czy podczas szkoleń i podczas wielu dyskusji prowadzonych na portalu Facebook miały wpływ na stanowisko PUODO, nawet jednak jeśli tak nie było, to cieszę się, że myśl pracowników PUODO poszła w tym samym kierunku co moja. Fakt ten pozwala mi również mniemać, że przyjęta przeze mnie interpretacja jest właściwa, bowiem w końcu doszli do niej (sami, czy zainspirowani) pracownicy PUODO.

przynajmniej pod adresem strony www, który wskazuję w przypisie, a który to adres funkcjonował, jak wskazuję wyżej, jeszcze 15 marca 2019 roku, kiedy kończyłem pracę nad wcześniejszą publikacją o RODO. Z punktu bezpieczeństwa procesowego polskich administratorów, nieco niepokoi, że strona zawierająca błędną definicję zniknęła. Dla systemu ochrony danych osobowych to dobrze, że PUODO nie upowszechnia wygodnej acz błędnej interpretacji. Dla administratorów – nieco gorzej.

Wydaje się, że przez czas jakiś polscy administratorzy będą mogli jednak próbować się na taką interpretację nadal powoływać, ponieważ była ona dostępna na stronie PUODO, obecnie definicja naruszenia ochrony danych osobowych zinterpretowana przez PUODO jest nadal dostępna, acz w innej postaci niż strona www. Otóż PUODO udostępnia na swojej stronie www publikacje w formacie .pdf, sformatowaną tak, by była wygodna do wydruku. Jest to o tyle niekorzystne, że publikacja ta może być łatwo drukowana i tym samym długo przechowywana przez administratorów danych, jako wiarygodny, bo pochodzący od PUODO materiał. Publikacja ta nosi tytuł: *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. wersja 1.0 czerwiec 2019*. Co ciekawe wewnątrz publikacji, w nagłówkach stron czytamy: *Wersja 1.0 Maj 2019*. Z kolei na czwartej stronie okładki czytamy: *Wersja 1.0 Maj 2019*. Różnica miesiąca w nagłówkach, na pierwszej stronie okładki i na czwartej stronie okładki nie wydaje się istotna, aczkolwiek kiedy z porównania wynika, że zarówno wersja z maja (nagłówki i czwarta strona okładki) jak i wersja z czerwca (pierwsza strona okładki), to wersja oznaczona jako *1.0*, to może pojawić się pewien niepokój, dotyczący jakości redakcji dzieła. Z dzieła nie wynika kto jest jego autorem, jednak niewątpliwe jest, że odpowiada za nie PUODO, z uwagi na warstwę graficzną dzieła, jak i na fakt, że w momencie pisania niniejszych słów jest ono dostępne ze strony www[377] PUODO. Mimo niepewnego autorstwa dzieła i ewidentnych problemów z numeracją wersji redakcyjnych, obserwuję znaczący postęp w rozumieniu definicji naruszenia ochrony danych osobowych przez anonimowego pracownika PUODO, ową definicję interpretującego. Dla zobrazowania rozwoju, definicje zestawiam niżej w tabeli a niżej jeszcze, zwracam uwagę na

[377] https://uodo.gov.pl/pl/134/1029 (dostęp 2.11.2019 godz. 3.34.)

dzielące je różnice a zwłaszcza na tę z różnic, która świadczy o rozwoju zrozumienia definicji w PUODO.

Aby zaistniało naruszenie muszą być spełnione łącznie trzy przesłanki: – naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie; – skutkiem naruszenia **musi być** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych; – naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.	Żeby zaistniało naruszenie, muszą być spełnione łącznie trzy przesłanki: – naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie; – skutkiem naruszenia **może być** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych; – naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

Różnica: aby/żeby jest niewarta omawiania. Pomijam również ewentualne różnice w interpunkcji. Między zaprezentowanymi definicjami jest naprawdę jedna duża różnica, którą z racji jej doniosłości zaznaczyłem wytłuszczeniem i podkreśleniem.

Otóż w wersji pierwotnej widniało: *skutkiem naruszenia **musi być** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych*, nie wiem czy

nadal wersja ta nie jest możliwa do odnalezienia na stronie, jak piszę wyżej – nie znalazłem.

W wersji obecnej widnieje: *skutkiem naruszenia **<u>może być</u>** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych*". Zmiana, mimo iż pozornie niewielka, jest niezwykle istotna. w wersji wcześniejszej - ze strony PUODO, dla zaistnienia naruszenia konieczne jest m.in., że skutkiem naruszenia **musi być** niezgodny z prawem wyciek lub niezgodne z prawem zniszczenie danych. w wersji późniejszej - z poradnika PUODO, dla zaistnienia naruszenia konieczne jest m.in., że skutkiem naruszenia **może być** niezgodny z prawem wyciek lub niezgodne z prawem zniszczenie danych. Naruszenie zachodzi zatem, jeżeli następuje niezgodny z prawem wyciek lub niezgodne z prawem zniszczenie danych, ale naruszenie zachodzi również jeżeli niezgodny z prawem wyciek lub niezgodne z prawem zniszczenie danych stanowią jedynie zagrożenie.

Na początku 2019 roku napisałem w książce: *Tak długo, jak błędna definicja naruszenia jest na stronie www PUODO, tak długo polscy ADO mogą rozumieć naruszenie zgodne z tą definicją, a w razie problemów bronić się tym, że działali w zaufaniu do administracji. Kiedy definicja zniknie ze strony, wtedy naruszenie trzeba będzie rozumieć szerzej, już jako zagrożenie zdarzeniami wymienionymi w art. 4 pkt 12 RODO.*, wydaje się, że czas kiedy naruszenie trzeba rozumieć szerzej już nadszedł. Słowa te piszę w połowie roku 2020.

Ciekawe stanowisko zajęli P. Litwiński, P. Barta i M. Kawecki, którzy napisali, m. in. że: „(…) skutkiem naruszenia bezpieczeństwa **powinno być** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych."[378] (wytłuszczenie: J. Rz.). Kiedy zestawimy wersje to widzimy jak poniżej:

- *skutkiem naruszenia **<u>musi być</u>** (...)* zniszczenie lub wyciek danych - wersja ze strony www PUODO,

[378] P. Litwiński, P. Barta, M. Kawecki. [w:] P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z prze adaptowanie lub modyfikowanie twarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.* Warszawa 2018. s. 235.

- *skutkiem naruszenia **<u>może być</u>** (...)* zniszczenie lub wyciek danych - wersja z poradnika PUODO,
- *skutkiem naruszenia **<u>powinno być</u>** (...)* zniszczenie lub wyciek danych - wersja P. Litwińskiego, P. Barty i M. Kaweckiego.

Stanowisko P. Litwińskiego, P. Barty i M. Kaweckiego wydaje się być podyktowane ostrożnością, jednak *powinno być* można (zapewne) w opisywanej sytuacji utożsamić z „musi być". Należy zwrócić uwagę, że wersja P. Litwińskiego, P. Barty i M. Kaweckiego dostępna była już w 2018 roku, kiedy ukazał się komentarz do RODO ich autorstwa. Być może to właśnie ta wersja stanowiła wskazówkę dla PUODO – nie wiem tego, jednak dobrze, że PUODO zamieniło swoje mylące *musi być* na zasadne *może być*, oczywiście lepiej by było gdyby PUODO takich błędów nie popełniało, ale to już raczej idealistyczny postulat niż wniosek.

Moim dodatkowym zarzutem wobec definicji z art. 4 ust. 12 RODO jest nie tylko jej niejasność i bełkotliwość, która zmusza do kilkustronicowych wywodów, ale jeden jeszcze element definicji. Otóż *naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do*... Po słowie: *do* padają nazwy zdarzeń do których naruszenie może doprowadzić. Z zasady a fortiori[379] wynika, że skoro naruszeniem jest zdarzenie, które *może doprowadzić do* ..., to tym bardziej naruszeniem jest zdarzenie które „doprowadziło do ..." ale czy naprawdę przepisu tego nie można było napisać jaśniej, w sposób zrozumiały nie tylko dla prawników i to tych zakochanych w teorii prawa.

Nowelizacje przepisu proponuję niżej w postulatach *6. Art. 6. pkt 12. Postulaty de lege ferenda*.

Bełkotliwość definicji prowadzi do używania innych pojęć, które zapewne w założeniu osób nimi się posługujących mają ułatwić komunikację. Próbę taką podjął np. M. Bochenek, który zdefiniował incydent bezpieczeństwa. Autor ten uznał, że incydent bezpieczeństwa to „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych

[379] B. Wojciechowski w: *System Prawa Administracyjnego* Red: R Hauser, Z. Niewiadomski, A Wróbel. *Tom IV. Wykładnia w prawie administracyjnym.* L. Leszczyński, B. Wojciechowski, M. Zirk-Sadowski. Warszawa 2012, s. 446.

osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Jest to także sytuacja kryzysowa związana z nieautoryzowanym dostępem do informacji chronionych, ich zniszczeniem, modyfikacją, utratą lub innym celowym działaniem naruszającym bezpieczeństwo ochrony informacji. Incydentem bezpieczeństwa jest również próba podjęcia wymienionych działań."[380]. Jak widać M. Bochenek w swojej próbie definicji umieścił w całości definicję naruszenia ochrony danych osobowych, po czym wprowadził pojęcie sytuacji kryzysowej, po czym na dobrą sprawę, powtórzył definicję naruszenia ochrony danych osobowych. Próba podjęta przez M. Bochenka nie wydaje się być próbą udaną – powtórzenie bełkotu prawodawcy, nawet dwukrotne i ze zmianą przypadków, nie czyni tego bełkotu jaśniejszym czy czytelniejszym.

4. Art. 6. pkt 12. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 12 RODO definiuje ***naruszenie ochrony danych osobowych***, zatem zgodnie z dyrektywą języka prawnego[381], każdy kto interpretuje RODO powinien rozumieć pojęcie ***naruszenie ochrony danych osobowych*** tak jak jest ono w komentowanym przepisie zdefiniowane.

Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie ***naruszenie ochrony danych osobowych*** tak jest ono zdefiniowane w art. 4 pkt. 8 RODO.

- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia ***naruszenie ochrony danych osobowych*** zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

[380] M. Bochenek *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach.* Warszawa 2019, Lex.

[381] L. Morawski *op. cit.* s. 93-99, zwłaszcza 95.

5. Art. 4. pkt 12. Konkretyzacja zasad

Artykuł 4 ust. 12 RODO sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Zdefiniowanie naruszenia ochrony danych osobowych sprzyja zapobieganiu wyciekom i niezgodnemu z prawem niszczeniu danych osobowych czyli zjawiskom naruszającym zasadę zgodności z prawem.

Realizacja **zasady rzetelności**. Przetwarzanie danych osobowych w ten sposób że osoba której dane dotyczą nie wie że jej dane są przetwarzane, może w kontekście naruszenia ochrony danych osobowych zajść w ten sposób, że samo naruszenie (wyciek lub zniszczenie danych) jest czynnością przetwarzania danych osobowych o której osoba której dane dotyczą nie została poinformowana. Może się również zdarzyć że naruszenie ochrony danych osobowych prowadzi do wycieku danych i dalszego ich przetwarzania w sposób o którym osoba której dane dotyczą nie została poinformowana czy też po prostu nie wie.

Realizacja **zasady przejrzystości**. Jeżeli dane osobowe są ujawniane lub niszczone w kontekście naruszenia ochrony danych osobowych, to czynności te są czynnościami, o szczegółach których osoba której dane dotyczą nie wie. Nawet jeżeli realizowano wobec niej obowiązek informacyjny to nie sposób wyobrazić sobie, by w ramach obowiązku informacyjnego administrator (danych osobowych) informował osobę której dane dotyczą o możliwości przetwarzania danych osobowych mającej charakter naruszenia ochrony danych osobowych.

Realizacja **zasady ograniczenia celu**. Wyciek danych z założenia jest czynnością czy też raczej zjawiskiem naruszającym zasadę ograniczenia celu. Wyciek danych może również prowadzić do dalszego przetwarzania danych z naruszeniem tej zasady. Zniszczenie danych osobowych rozumiane jako naruszenie ochrony danych osobowych narusza zasadę ograniczenia celu, ponieważ trudno sobie wyobrazić by dane osobowe były przetwarzane przez administratora w celu o charakterze naruszenia ochrony danych osobowych.

Realizacja **zasady minimalizacji**. Wyciek danych osobowych lub ich zniszczenie w kontekście naruszenia ochrony danych osobowych są zjawiskami o charakterze czynności, które dla przetwarzania danych osobowych przez pierwotnego administratora, z punktu widze-

nia którego oceniana jest zasada niezbędne nie są. Nadużyciem interpretacyjnym byłoby również wywodzenie, że wyciek lub zniszczenie danych osobowych są czynnościami adekwatnymi do celu przetwarzania przyjętego przez administratora danych osobowych.

Realizacja **zasady prawidłowości**. Niezgodne z prawem zmodyfikowanie danych osobowych to czynność skutkująca uzyskaniem danych osobowych, których przetwarzanie po takim właśnie zmodyfikowaniu narusza zasadę prawidłowości.

Realizacja **zasady ograniczenia przechowywania danych**. Wszelkie wycieki danych mogą prowadzić do przetwarzania danych niezgodnego z tą zasadą. Jeżeli ktoś uzyska dane osobowe w sposób nieuprawniony to możliwe jest że będzie je dalej przetwarzał w sposób niekontrolowany przez pierwotnego administratora, co jest prostą drogą do przetwarzania danych osobowych dłużej niż przetwarzałby je pierwotny administrator.

Realizacja **zasady integralności**. Naruszenie ochrony danych osobowych poprzez przypadkowe lub niezgodne z prawem ich zniszczeniem lub zmodyfikowanie stanowi naruszenie zasady integralności.

Realizacja **zasady poufności**. Naruszenie ochrony danych osobowych poprzez nieuprawnione ich ujawnienie lub nieuprawniony do nich dostęp narusza zasadę poufności

6. Art. 6. pkt 12. Postulaty de lege ferenda

6.1 Art. 6. pkt 12. Postulat 1. Usunięcie z przepisu błędu „nieznane przez nieznane“

Wyżej w analizie *2. Art. 4. pkt 12. Analiza* piszę, że używając słów *naruszenie bezpieczeństwa* na początku wyjaśniania definicji naruszenia ochrony danych osobowych, prawodawca popełnił błąd logiczny „nieznane przez nieznane”. Podnoszę tam również, że zastąpienie słów *naruszenie bezpieczeństwa* słowem „zdarzenie” nie zmienia nic w wykładni przepisu. Zastąpienie słów słów *naruszenie bezpieczeństwa* słowem „zdarzenie” zniosłoby, a przynajmniej złagodziło błąd „nieznane przez nieznane”, tudzież uczyniło przepis zrozumialszym.

W związku z tym postuluję nowelizację art. 4 pkt 12 RODO poprzez zastąpienie w przepisie słów: „naruszenie bezpieczeństwa” słowem „zdarzenie”.

Przepis po nowelizacji miałby postać:

„naruszenie ochrony danych osobowych” oznacza ~~naruszenie bezpieczeństwa~~ **zdarzenie** prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych” (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowo dodane.)

6.2 Art. 6. pkt 12. Postulat 2.
Rozjaśnienie treści przepisu

Wyżej w uwadze *3.3. Art. 4. pkt 12.Uwaga 3. Konkretyzacja obowiązku zgłoszenia naruszenia* analizuję szeroko skutki użycia przez prawodawcę słowa: „prowadzące do”. Analiza poprowadzona drobiazgowo, acz nie nadmiernie drobiazgowo, zajęła ok 10 tysięcy znaków. Niewłaściwie zdiagnozowane naruszenie praw lub wolności osoby fizycznej o którym mowa w art. 33 RODO może skutkować niezgłoszeniem tego naruszenia do organu nadzoru. Niezgłoszenie naruszenia do organu nadzoru może z kolei skutkować karą administracyjną. Przyczyną niewłaściwej diagnozy naruszenia praw lub wolności może być błędne rozumienie definicji naruszenia ochrony danych osobowych. Z rozumowania tego wynika że rozumienie definicji naruszenia ochrony danych osobowych ma doniosłe znaczenie dla bezpieczeństwa procesowego administratora danych osobowych. W rozumowaniu tym świadomie pomijam interesy osoby której dane dotyczą, dla których przeciwdziałanie naruszeniu ochrony danych osobowych jest również istotne.

Niezależnie od argumentów za tym przemawiających, właściwe rozumienie definicji naruszenia ochrony danych osobowych jest pożądane. W związku z tym definicję naruszenia ochrony danych osobowych należy znowelizować tak by wniosek który dziś uzyskujemy z jej analizy po długich deliberacjach, uzyskiwany był w sposób łatwy i taki sam dla każdego interpretatora.

W związku z powyższym postuluję nowelizację art. 4 pkt 12 RODO w następujący sposób: „„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa ~~prowadzące do~~ **skutkujące lub mogące skutkować** ~~przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu~~ **przypadkowym lub**

niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych." (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Przepis po nowelizacji miałby postać:
„naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa skutkujące lub mogące skutkować przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych."

6.3 Art. 6. pkt 12. Postulat 1 + postulat 2 = postulat 3. Usunięcie z przepisu błędu „nieznane przez nieznane" i rozjaśnienie treści przepisu

Jednoczesne zastosowanie postulatu *6.1 Art. 6. pkt 12. Postulat 1. Usunięcie z przepisu błędu „nieznane przez nieznane"* i postulatu *6.2 Art. 6. pkt 12. Postulat 2. Rozjaśnienie treści przepisu* jest możliwe merytorycznie. Uważam też, że jednoczesne zastosowanie obydwu postulatów jest pożądane.

W związku z powyższym postuluję nowelizację art. 4 pkt 12 RODO poprzez jednoczesne zastosowanie obydwu postulatów.

Przepis po nowelizacji miałby postać:
„naruszenie ochrony danych osobowych" oznacza zdarzenie skutkujące lub mogące skutkować przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych."

6.4 Art. 6. pkt 12. Postulat 4. Rozjaśnienie treści przepisu w inny sposób niż w Postulacie 2

Skutek osiągnięty w nowelizacji przepisu zaproponowanej w postulacie *6.2 Art. 6. pkt 12. Postulat 2. Rozjaśnienie treści przepisu***.** można osiągnąć przez inną nieco ingerencję w treść przepisu. Poniżej w wersji znowelizowanej proponuję ujęcie również zmiany z postulatu *6.1 Art. 6. pkt 12. Postulat 1. Usunięcie z przepisu błędu „nieznane przez nieznane"*. Przepis w wersji znowelizowanej może

mieć postać: „„Naruszenie ochrony danych osobowych” oznacza ~~naruszenie bezpieczeństwa~~ **zdarzenie**, ~~prowadzące do~~ **którego skutkiem może być lub jest** niezgodne z prawem zniszczenie lub ujawnienie danych osobowych przez czynności lub zdarzenia takie jak: utracenie, zmodyfikowanie, ujawnienie, dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający.” (Czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.).

Przepis po nowelizacji miałby postać:

„„Naruszenie ochrony danych osobowych” oznacza zdarzenie, którego skutkiem może być lub jest niezgodne z prawem zniszczenie lub ujawnienie danych osobowych przez czynności lub zdarzenia takie jak: utracenie, zmodyfikowanie, ujawnienie, dostęp do danych osobowych przetwarzanych przez ADO lub przez PP.”

Artykuł 4 pkt 13 RODO

„dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

1. Art. 4 pkt 13. Komentarz

W przepisie zdefiniowano dane genetyczne. Przepis traktuje zarówno o danych genetycznych uzyskanych po urodzeniu się osoby fizycznej jak i o danych uzyskanych przed urodzeniem się osoby fizycznej, czy o tzw. danych prenatalnych.

Dane genetyczne są danymi osobowymi.

Dane genetyczne to dane dotyczące cech genetycznych osoby fizycznej.

Cechy genetyczne, o których mowa w przepisie mogą być odziedziczone lub nabyte.

Dane genetyczne dotyczą cech genetycznych ujawniających informacje o fizjologii lub zdrowiu osoby, zarówno informacje, z których wynika, że ktoś jest chory jak i informacje o tym, że ktoś jest zdrowy.

Cechy genetyczne, o których mowa w przepisie mogą ujawniać informacje jedynie o fizjologii osoby fizycznej albo o zdrowiu osoby fizycznej albo o fizjologii i o zdrowiu osoby fizycznej.

Ujawniane informacje o fizjologii lub zdrowiu są niepowtarzalne.

Dane genetyczne to dane, które mogą wynikają z analizy próbki biologicznej pochodzącej od osoby fizycznej lub z innych źródeł.

2. Art. 4 pkt 13. Analiza

Ze słów wytłuszczonych: „„**dane genetyczne**” (…)” wynika, że w przepisie zdefiniowano dane genetyczne. Zwracam uwagę, że przepis traktuje o danych genetycznych w ogólności, czyli zarówno o danych genetycznych uzyskanych po urodzeniu się osoby fizycznej jak i o danych uzyskanych przed urodzeniem się osoby fizycznej, czy o tzw. danych prenatalnych.

Ze słów wytłuszczonych: „„**dane genetyczne**” **oznaczają dane osobowe** (…)” wynika, że dane genetyczne są danymi osobowymi. Nie ustanowiono tu jednak żadnego domniemania, z którego wynikałoby, że jeśli dane są danymi genetycznymi to są danymi osobowymi. Prawodawcy chodzi zapewne o to, że dane genetyczne to dane osobowe, które spełniają pewne dodatkowe warunki. Co nie jest szczególnie zręczne, bo możliwe są dane genetyczne, które nie są danymi osobowymi. Szerzej w uwadze *3.1. Art. 4 pkt 13. Uwaga 2. Dane genetyczne a dane osobowe*.

Ze słów wytłuszczonych: „„**dane genetyczne**” **oznaczają dane osobowe dotyczące** odziedziczonych lub nabytych **cech genetycznych osoby fizycznej**, (…)” wynika, że dane genetyczne to dane dotyczące cech genetycznych osoby fizycznej.

Ze słów wytłuszczonych: „(…) **odziedziczonych lub nabytych** cech genetycznych (…)” wynika, że cechy genetyczne, o których mowa w przepisie mogą być odziedziczone lub nabyte.

Ze słów wytłuszczonych: (…) cech genetycznych osoby fizycznej, **które ujawniają** niepowtarzalne **informacje o fizjologii lub zdrowiu tej osoby** (…)” wynika, że dane genetyczne dotyczą cech genetycznych ujawniających informacje o fizjologii lub zdrowiu osoby. Zwracam uwagę, że informacje o zdrowiu to zarówno informacje, z których wynika, że ktoś jest chory jak i informacje o tym, że ktoś jest zdrowy.

Z użycia funktora „**lub**” wynika, że cechy genetyczne, o których mowa w przepisie mogą ujawniać informacje jedynie o fizjologii osoby fizycznej albo o zdrowiu osoby fizycznej albo o fizjologii i o zdrowiu osoby fizycznej.

Ze słów wytłuszczonych: „(…) **niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby** (…)” wynika, że ujawniane informacje o fizjologii lub zdrowiu są niepowtarzalne.

Ze słów wytłuszczonych: „(…) **i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej**;” wynika, że dane genetyczne to dane, które wynikają „w szczególności” z analizy próbki biologicznej pochodzącej od osoby fizycznej.

Dane nie muszą koniecznie wynikać z analizy próbki biologicznej pochodzącej od osoby fizycznej, ponieważ przepis stanowi, że mają one wynikać „z analizy próbki biologicznej pochodzącej od osoby fizycznej" ale „w szczególności". W związku z tym jeżeli informacje wynikają z „z analizy próbki biologicznej pochodzącej od osoby fizycznej" to są one danymi genetycznymi (oczywiście o ile spełniają pozostałe zawarte w przepisie warunki) jeżeli jednak informacje te pochodzą z innego źródła to także są one danymi genetycznymi (oczywiście o ile spełniają pozostałe zawarte w przepisie warunki). Dane genetyczne dotyczące osoby fizycznej mogą pochodzić od członków jej rodziny.

3. Art. 4 pkt 13. Uwagi

3.1. Art. 4 pkt 13. Uwaga 1.

Dane genetyczne prenatalne

Przepis dotyczy danych genetycznych. Dane genetyczne, co wiemy z przepisu, to dane osobowe. Dane osobowe to dane dotyczące osoby fizycznej. Dane genetyczne to zatem dane dotyczące osoby fizycznej, czyli żywego człowieka. Zastanowiwszy się nad danymi prenatalnymi należy poczynić kilka uwag.

Jeżeli człowiek żyje, ponieważ się urodził to dotyczące go dane genetyczne uzyskane po jego urodzeniu są danymi osobowymi, które go dotyczą.

Jeżeli człowiek nie żyje, ponieważ się urodził, jednak później zmarł, to dotyczące go dane genetyczne uzyskane po jego urodzeniu są danymi osobowymi, które go dotyczą, jednak RODO nie chroni tych danych.

Jeżeli człowiek żyje, ponieważ się urodził, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą.

Jeżeli człowiek nie żyje, ponieważ się urodził, jednak później zmarł, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą, jednak RODO nie chroni tych danych.

Jeżeli człowiek jeszcze się nie urodził, ma jednak szansę się urodzić, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą, wydaje się jednak, że RODO dotyczy tych danych warunkowo, a mianowicie pod warunkiem, że

człowiek ten urodzi się żywy. Dane należy zatem chronić jeszcze przed urodzeniem się człowieka, jeżeli bowiem urodzi się on żywy, to dane uzyskane przed jego urodzeniem są danymi osobowymi. Jeżeli dane uzyskane przed urodzeniem zostaną jeszcze przed urodzeniem ujawnione, to uważam, że administrator nie powinien ponieść odpowiedzialności administracyjnej, ponieważ chroni go wynikająca z art. 7a KPA zasada tłumaczenia wątpliwości na korzyść uczestnika postępowania a skoro człowiek się jeszcze nie urodził i nie wiadomo czy się urodzi żywy, to nie wiadomo czy RODO chroni informacje, które go dotyczą a zebrane i ujawnione jeszcze przed jego urodzeniem. Niestety administrator danych nie jest tu w pełni bezpieczny, ponieważ informacje dotyczące tego człowieka są również informacjami dotyczącymi jego rodziców i to niezależnie od tego czy urodzi się żywy.
Jeżeli człowiek jeszcze się nie urodził, i się nie urodzi bo zmarł przed urodzeniem, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem nie są, jak się wydaje, danymi osobowymi, które go dotyczą, ponieważ byt ten, nazwany na początku zdania człowiekiem, nigdy się nie urodził, zatem nie stał się osobą fizyczną. Dane bytu, który nie urodził się żywy, „informacje związane z poronieniem, informacje dotyczące dziecka martwo urodzonego, mogą być (zależnie od sytuacji) danymi ojca, matki, matki biologicznej - surogatki, dawcy nasienia, matki genetycznej - dawczyni komórki jajowej. Kiedy dziecię urodzi się żywe to z kolei dane dotyczące wymienionych osób, są w pewnym zakresie danymi osobowymi dziecięcia. Należy również pamiętać o danych ojca, który uznał dziecię przed urodzeniem.

3.1. Art. 4 pkt 13. Uwaga 2.
Dane genetyczne a dane osobowe

W przepisie widnieją słowa: *dane genetyczne* oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;". Niepokojąco wyglądają słowa: *„dane genetyczne" oznaczają dane osobowe dotyczące (...)* niepokojąco ponieważ taka konstrukcja przepisu (w angielskiej wersji językowej jest podobna konstrukcja) może nasuwać przypuszczenie, że prawodawca ustanowił w definicji danych genetycznych domniemanie. Domniemanie zgodnie z którym dane gene-

tyczne są danymi osobowymi. Przypuszczenie to jest błędne, żadnego domniemania tu nie ustanowiono, po prostu przepis skonstruowano tak, że dane genetyczne zdefiniowano jako dane osobowe dotyczące cech genetycznych osoby fizycznej (pisząc w skrócie). W przepisie nie ustanowiono zatem domniemania zgodnie z którym dane genetyczne byłyby zawsze danymi osobowymi ale za to zdefiniowano pojęcie danych genetycznych. Pojęcie danych genetycznych zdefiniowano tak, że są to dane osobowe dotyczące cech genetycznych osoby fizycznej (skracam). Takie zdefiniowanie tego pojęcia nie wydaje się właściwe, możliwe są bowiem dane genetyczne, które nie są danymi osobowymi, ponieważ zostały uzyskane ze zanonimizowanej próbki. Sam fakt analizy próbki metodami umożliwiającymi uzyskanie informacji o genomie człowieka, od którego próbkę pobrano, nie czyni tych danych danymi osobowymi. Nie czyni, ponieważ nadal może nie być wiadomo czyje to dane.

Paweł Litwiński, P. Barta, M. Kawecki wskazali, że dane genetyczne są *jedną z kategorii danych osobowych*[382], z czym się trzeba zgodzić, z tym jednak zastrzeżeniem, że kategorią danych osobowych są dane genetyczne zdefiniowane w komentowanym przepisie. Poza tym są bowiem możliwe dane genetyczne, które danymi osobowymi nie są, więc nie są i kategorią danych osobowych.

Paweł Litwiński, P. Barta, M. Kawecki napisali też, że: *Informacja tylko wtedy może więc zostać uznana za dane genetyczne, jeżeli spełnia definicję danych osobowych zawartą w komentowanym przepisie i jednocześnie spełnia definicję danych (osobowych) genetycznych*[383]. Wskazani autorzy wprowadzają tu pewien nieład, bowiem piszą o definicji danych osobowych zawartej w komentowanym przepisie, podczas gdy piszą to w komentarzu do definicji danych genetycznych, nie zaś do definicji danych osobowych, jest to jednak drobny niuans redakcyjny. Wydaje się, że intencją wskazanych autorów było wskazanie, że dane genetyczne są jednocześnie danymi osobowymi, z czym się zgadzam, jednak z poczynionymi wyżej zastrzeżeniami.

[382] P. Litwiński, P. Barta, M. Kawecki w: P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 235.

[383] P. Litwiński, P. Barta, M. Kawecki, *loc. cit.*

4. Art. 4 pkt 13. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 13 RODO definiuje ***dane genetyczne***, zatem zgodnie z dyrektywą języka prawnego[384], każdy kto interpretuje RODO powinien rozumieć pojęcie ***dane genetyczne*** tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie ***dane genetyczne*** tak jest ono zdefiniowane w art. 4 pkt. 13 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „**dane genetyczne**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 13. Konkretyzacja zasady I

Zasada zgodności z prawem skonkretyzowana jest przez wymienione poniżej przepisy.

5.1. Art. 4 pkt 13. Podstawowa konkretyzacja zasady I

Realizacja **zasady zgodności z prawem**. Namysł nad tym czy konkretne, przetwarzane przez danego administratora dane genetyczne są danymi osobowymi może pomóc w podjęciu decyzji o zaniechaniu ich przetwarzania lub o ich anonimizacji. Anonimizacja danych genetycznych, służących do wykrycia choroby u konkretnej osoby fizycznej, nie ma sensu, zwłaszcza przed wykryciem tej choroby. Dana próbka może być jednak w późniejszym czasie zanonimizowana, kiedy jest na przykład wykorzystywana do celów naukowych.

Realizacja **zasady rzetelności**. Jeżeli administrator przetwarza dane genetyczne, będące danymi osobowymi, to powinien poinformować osobę, której dane dotyczą o fakcie przetwarzania danych, na gruncie art. 13 lub art. 14 RODO.

Realizacja **zasady przejrzystości**. Jeżeli administrator przetwarza dane genetyczne, będące danymi osobowymi, to powinien poinfor-

[384] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

mować osobę, której dane dotyczą o szczegółach przetwarzania danych, na gruncie art. 13 lub art. 14 RODO.

Realizacja **zasady ograniczenia celu**. Wyciek danych genetycznych będących danymi osobowymi, może doprowadzić, do złamania tej zasady, jeżeli bowiem dane wyciekną, to administrator traci kontrolę nad tym w jakim celu są one przetwarzane.

Realizacja **zasady minimalizacji**. Z punktu widzenia realizacji tej zasady, lepiej jest przetwarzać dane genetyczne, które nie są danymi osobowymi, czyli dane genetyczne, które nie mieszczą się w definicji z art. 4 pkt 13 RODO, nie mieszczą, ponieważ dane genetyczne zdefiniowane w art. 4 pkt 13 RODO są danymi osobowymi. Oczywiście jeżeli przetwarzanie danych genetycznych i to danych genetycznych rozumianych tak jak to zdefiniowane w art. 4 pkt 13 RODO, jest niezbędne dla osiągnięcia celu przetwarzania, to nie ma problemu z dopuszczalnością przetwarzania tych danych, patrząc z punktu widzenia zasady minimalizacji.

Realizacja **zasady ograniczenia przechowywania danych**. Jeżeli administratorowi do jego celów potrzebne są genetyczne (dane osobowe), to zawsze, w jakimś sensie naraża się na naruszenie tej zasady (jak i innych zasad), jeżeli jednak administrator używa danych genetycznych nieosobowych, czyli danych, które nie mieszczą się w definicji z art. 4 pkt 13 RODO, to problem z potencjalnym naruszeniem zasady znika.

Realizacja **zasady integralności**. Podobnie jak w przypadku poprzedniej zasady, jeżeli administrator przetwarza genetyczne dane nieosobowe, to nie grozi mu złamanie zasady.

Realizacja **zasady poufności**. i tu też, przetwarzanie genetycznych danych nieosobowych zabezpiecza przed naruszeniem zasady.

6. Art. 4 pkt 13. Postulaty de lege ferenda

6.1 Art. 4 pkt 13. Postulat 1. Usunięcie możliwego domniemania

Przepis komentowany może obecnie wprowadzać w błąd w kwestii ewentualnego domniemania jakoby dane genetyczne były danymi osobowymi.

Poza tym nawet jeśli zauważamy, że wskazanego domniemania przepis nie ustanawia, to i tak w przepisie zdefiniowano dane genetyczne właśnie jako dane osobowe, co jest niepotrzebną zmianą zakresu poję-

cia danych genetycznych. Szerzej o obydwu problemach piszę w uwadze *3.1. Art. 4 pkt 13. Uwaga 2. Dane genetyczne a dane osobowe*.

W związku z powyższym postuluję aby początek przepisu brzmiał: „„dane genetyczne" oznaczają dane ~~osobowe~~ dotyczące (…)". (Czcionką przekreśloną zaznaczam słowo usunięte.).

Przepis po nowelizacji miałby postać:

„„dane genetyczne" oznaczają dane ~~osobowe~~ dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej".

Artykuł 4 pkt 14 RODO.

„dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

1. Art. 4 pkt 14. Komentarz

W przepisie zdefiniowano dane biometryczne.

Dane biometryczne są danymi osobowymi. Oczywiście mowa tu o danych genetycznych zdefiniowanych w przepisie.

Trudno powiedzieć, czy w przepisie ustanowiono domniemanie, zgodnie z którym dane biometryczne są danymi osobowymi.

Założenie, zgodnie z którym dane biometryczne to zawsze dane osobowe byłoby jednak raczej założeniem błędnym. Dane biometryczne to dane, które wynikają ze *specjalnego przetwarzania technicznego*, czyli zdjęcie umożliwiające pomiar odległości stałych punktów twarzy nie jest jeszcze danymi biometrycznymi, dopiero po zmierzeniu tych odległości otrzymywane są dane biometryczne. Dane biometryczne to dane, które dotyczą cech osoby fizycznej w sposób opisany poniżej w pozycji: *2. Art. 4 pkt 14. Analiza*, w miejscu opatrzonym śródtytułem: *Lista danych biometrycznych.*

2. Art. 4 pkt 14. Analiza

Ze słów wytłuszczonych: „(…)„**dane biometryczne**” (…)” wynika, że w przepisie zdefiniowano dane biometryczne.

Ze słów wytłuszczonych: „(…) „**dane biometryczne**” **oznaczają dane osobowe** (…)” wynika, że dane genetyczne są danymi osobowymi. Trudno jednoznacznie powiedzieć, czy w przepisie ustanowiono domniemanie, zgodnie z którym dane biometryczne są danymi osobowymi. Trudno, ponieważ z dalszej części definicji wynika, że dane te bardzo dokładnie identyfikują człowieka, identyfikują go na podstawie jego cech. Trudno wyobrazić sobie cechy identyfikujące człowieka oderwane od człowieka. o ile próbkę biologiczna można oderwać

od człowieka w sposób niezwykle łatwy, a mianowicie analizować ją w warunkach, w których po uzyskaniu danych z próbki nie wiadomo czyje te dane są, o tyle z danymi biometrycznymi sytuacja jest nieco bardziej skomplikowana. Wydaje się, że są takie kategorie danych biometrycznych, które są analogiczne do danych genetycznych, z punktu widzenia tego czy są danymi osobowymi. Piszę tu o danych dotyczących cech fizycznych lub danych dotyczących cech fizjologicznych. Przykładem może być zdjęcie twarzy.

Przede wszystkim należy się zastanowić, czy zdjęcie, oczywiście zdjęcie nie biometryczne, to z założenia informacja dotycząca osoby fizycznej co najmniej możliwej do zidentyfikowania. Wydaje się, że tak, aczkolwiek kiedy przypomnimy sobie o miliardach ludzi zamieszkujących ziemię, to pewności w tej kwestii mieć nie można. Mam świadomość, że mogę mieć zdjęcie czyjejś twarzy, oczywiście czytelne zdjęcie i mogę nigdy nie ustalić czyja to twarz, odczuwam jednak pewien wewnętrzny sprzeciw przed pogodzeniem się z myślą, że czytelne zdjęcie twarzy nie zawsze dotyczy osoby zidentyfikowanej lub możliwej do zidentyfikowania. Mam wewnętrzne przeświadczenie, że jeżeli widzę czyjąś twarz na zdjęciu, to ta osoba, której twarz na zdjęciu widzę jest dla mnie, dla każdego, który to zdjęcie widzi, osobą zidentyfikowaną lub możliwą do zidentyfikowania. Nie wykluczam, że przeświadczenie to jest błędne. Myślę, że sprawa może być łatwiejsza do rozważania, jeżeli pojawiłoby się orzecznictwo, z którego wynikałoby czy sądy powszechnie uważają nie biometryczne zdjęcia twarzy za dane osobowe czy wręcz przeciwnie.

Jeżeli uznamy, że zdjęcie nie biometryczne, z założenia zawiera dane osobowe, to wydaje się, że zdjęcie biometryczne, tym bardziej je zawiera. Jest to rozumowanie oparte oczywiście na założeniu, że zdjęcie nie biometryczne z założenia zawiera dane osobowe. Jeżeli jest to założenie błędne, to i rozumowanie jest łatwe do podważenia.

Jeśli zastanowimy się nad innymi cechami fizycznymi osoby, takimi jak na przykład kształt dłoni, długość kroku, odciski palców itd., to wydaje się, że nie biometryczne zapisy tych cech nie zawierają danych osobowych. Zastanowić się dalej należy nad tym, czy biometryczne zapisy takich danych zawierają zawsze dane osobowe. Wydaje się, że nie. Przecież gdyby tak było, to zawsze byłoby wiadomo do kogo należy konkretny odcisk palca, a wszak nie wiadomo. Jeżeli nie posiadamy w bazie odcisku palca, z którym można zestawić odcisk pozostawiony np. na miejscu popełnienia przestępstwa, to nie usta-

limy czyj jest ten odcisk z miejsca przestępstwa. Z powyższego rozumowania wynika, a przynajmniej wydaje mi się, że wynika, że założenie, zgodnie z którym dane biometryczne to zawsze dane osobowe byłoby założeniem błędnym. Skoro tak, to słowa przepisu: *(...)„**dane biometryczne" oznaczają dane osobowe** (...)* też są błędne, budzą bowiem niepokój czy aby jednak dane biometryczne nie są zawsze danymi osobowymi lub czy może prawodawca nie ustanawia tu domniemania, zgodnie z którym dane biometryczne, danymi osobowymi są. Z prowadzonych tu rozważań, uważam, że wynika, że dane biometryczne, podobnie jak inne informacje, czasem danymi osobowymi są a czasem nie. W związku z tym ustanowienie domniemania, zgodnie z którym dane biometryczne danymi osobowymi są, byłoby, jak się wydaje, błędem. Odnoszę się do tego niżej w uwadze *3.1. Art. 4 pkt 14. Uwaga 1. Mylne domniemanie* i w postulacie *6.1 Art. 4 pkt 14. Postulat 1. Usunięcie mylnego domniemania*.

Ze słów wytłuszczonych: „(…)„**dane biometryczne**" oznaczają **dane osobowe, które wynikają ze specjalnego przetwarzania technicznego** (…)" wynika, że dane biometryczne to dane, które wynikają ze *specjalnego przetwarzania technicznego*, czyli zdjęcie umożliwiające pomiar odległości stałych punktów twarzy nie jest jeszcze danymi biometrycznymi, dopiero po zmierzeniu tych odległości otrzymywane są dane biometryczne. Nieco niepokoją słowa o specjalnym przetwarzaniu technicznym. Co to znaczy: przetwarzanie techniczne, co to znaczy: specjalne przetwarzanie techniczne. Obserwacja współczesnego świata każe kojarzyć te słowa z rozpoznawaniem twarzy jakie odbywa się w chinach a zapewne nie tylko tam, na podstawie danych zbieranych z kamer. Czynności umożliwiające takie rozpoznawanie to zapewne „specjalne przetwarzanie techniczne". Jeżeli jednak wyobrazimy sobie, że ktoś, na przykład technik zbierający ślady na miejscu popełnienia przestępstwa zbierze ślady o rozstawie czyichś zębów, na podstawie odcisku tychże w czymkolwiek, a następnie porówna te ślady z odciskiem zębów pobranym od podejrzanego, to czy technik wykonał „specjalne przetwarzanie techniczne" czy nie. Trudno powiedzieć. Przetwarzanie na pewno miało miejsce. Techniczne przetwarzanie też zapewne miało miejsce ponieważ użyto środków technicznych nie zaś jedynie przeprowadzono rozumowanie. Problemem staje się zatem odpowiedź na pytanie o to czy techniczne przetwarzanie z użyciem linijki (czy czegokolwiek czym technik mierzy odciski zębów)

jest przetwarzaniem specjalnym o jakim mowa w przepisie, czy nie. Wydaje się, że jest. Wydaje się, że jeżeli dane spełniają pozostałe warunki wymienione w przepisie, to nie należy starać się szukać różnicy między specjalnym przetwarzaniem technicznym a przetwarzaniem technicznym które specjalne nie jest. Gdyby ktoś tę różnicę wskazał, to mógłby ją wykorzystać w ten sposób, że przedkładałby, że dane przetwarzane w sposób specjalny (np. z użyciem skanera i komputera) są danymi biometrycznymi a dane przetwarzane w sposób, powiedzmy, niespecjalny – danymi biometrycznymi nie są. Rozumowanie takie mogłoby godzić w prawa i wolności osób, których dane dotyczą, na przykład w prawo do przetwarzania danych w sposób zgodny z prawem, prawo do przetwarzania danych w sposób ograniczony do tego co niezbędne.

Mowa o specjalnym przetwarzaniu jest wynikiem błędnego tłumaczenia słowa *specific*, szerzej o tym w postulacie *6.2 Art. 4 pkt 14. Postulat 2. Usunięcie mylnego domniemania*.

Przetwarzanie, o którym mowa w przepisie, to nie „szczególne przetwarzanie" a „konkretne przetwarzanie". Jeśli tak zmodyfikujemy przepis, to nabiera on sensu. Przepis miast brzmieć: „(…) „dane biometryczne" oznaczają dane osobowe, które wynikają ze **specjalnego** (wytłuszczenie J. Rz.) przetwarzania technicznego (…)", brzmieć powinien „(…)„dane biometryczne" oznaczają dane osobowe, które wynikają z **określonego** (wytłuszczenie J. Rz.) przetwarzania technicznego (…)". Kiedy „specjalne", zamieniamy na „określone", to okazuje się, że wiadomo co z przepisu wynika. Określone przetwarzanie z jakiego wynikają dane, to przetwarzanie, które się odbyło, nie jakieś przetwarzanie o szczególnych cechach, ale konkretne, to a nie inne lub przetwarzanie, które się jeszcze nie odbyło, ale wiadomo o jakie chodzi a wiadomo ponieważ jest ono określone. Na przykład w przypadku zdjęcia biometrycznego, mamy zdjęcie, zdjęcie zostaje przetworzone i po tym przetworzeniu, tym właśnie określonym przetworzeniu, otrzymujemy dane biometryczne, czyli w tym wypadku informacje dotyczące odległości i proporcji odległości stałych punktów twarzy.

Ze słów wytłuszczonych: „(…) które wynikają ze specjalnego przetwarzania technicznego, **dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby** (…)" wynika, że dane

biometryczne to dane, które dotyczą cech osoby fizycznej w sposób opisany poniżej.

Lista danych biometrycznych.

- dotyczą cech **fizycznych** osoby fizycznej i **umożliwiają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby albo

- dotyczą cech **fizjologicznych** osoby fizycznej i umożliwiają jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizjologicznych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizjologicznych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby albo

- dotyczą cech **behawioralnych** osoby fizycznej i umożliwiają jednoznaczną identyfikację tej osoby albo
- dotyczą cech **behawioralnych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **behawioralnych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby albo

- dotyczą cech **fizycznych i fizjologicznych** osoby fizycznej i umożliwiają jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych i fizjologicznych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych i fizjologicznych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych i behawioralnych** osoby fizycznej i umożliwiają jednoznaczna identyfikację tej osoby albo
- dotyczą cech **fizycznych i behawioralnych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizycznych i behawioralnych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizjologicznych i behawioralnych** osoby fizycznej i umożliwiają jednoznaczna identyfikację tej osoby albo

- dotyczą cech **fizjologicznych i behawioralnych** osoby fizycznej i p**otwierdzają** jednoznaczną identyfikację tej osoby albo
- dotyczą cech **fizjologicznych i behawioralnych** osoby fizycznej i **umożliwiają i potwierdzają** jednoznaczną identyfikację tej osoby.

Ze słów wytłuszczonych: „(…) **takie jak wizerunek twarzy lub dane daktyloskopijne**" wynika, że wizerunek twarzy i dane daktyloskopijne to dane biometryczne. Nie wiem, z uwagi na moją nikłą wiedzę kryminalistyczną, czy możliwe są poprawnie zebrane dane daktyloskopijne, które nie umożliwiając identyfikacji osoby, której dotyczą, jeżeli jednak chodzi o wizerunek twarzy, to możliwe są takie wizerunki twarzy, które nie umożliwiają identyfikacji osoby, której dane dotyczą, na przykład zdjęcie twarzy zrobione pod pewnym kątem, zdjęcie twarzy z naniesionymi naklejkami lub nakładkami, które zakrywają stałe punkty twarzy itp. Dążę tu do wniosku, że wizerunek twarzy nie zawsze jest danymi biometrycznymi czy też nawet nie zawsze takie dane zawiera. Tu właśnie pojawia się problem, a mianowicie czy wizerunek jest danymi. Z wizerunku dane raz wynikają a raz nie, ale sam wizerunek danymi nie jest. Dla potrzeb zrozumienia przepisu można przyjąć, że wizerunek twarzy jest przykładem cech fizycznych osoby fizycznej, o których mowa w przepisie a dane daktyloskopijne są przykładem danych biometrycznych.

Niestety napotykamy tu błąd tłumaczenia lub błąd przepisu. Przeprowadzam poniżej dwa rozumowania, które dla porządku numeruję.

Rozumowanie pierwsze

Lektura przepisu w wersji polskiej prowadzi do wniosku, że wizerunek twarzy jest przykładem danych biometrycznych. Pozornie informacja taka jest poprawna. Wyobrażamy sobie zdjęcie, zdjęcie jest skanowane, mierzone, dane umieszczane są w bazie danych, co umożliwia rozpoznanie osoby, której zrobiono zdjęcie, na przykład na podstawie zdjęć z kamery na ulicy. Zwracam jednak uwagę, że wszystkie czynności sobie wyobraziłem. Wyobraziłem sobie skanowanie, mierzenie itd., podczas gdy przepis wskazuje jedynie na wizerunek twarzy - a przykład zdjęcie wiszące na ścianie, ba – nawet zdjęcie w postaci pliku w pamięci komputera. Wszelkie czynności techniczne związane z tym zdjęciem ja sobie wyobraziłem, ja je wyfantazjo-

wałem i niestety odnoszę wrażenie, że podobnie uczynił prawodawca, który umieścił w przepisie wizerunek twarzy jako przykład danych biometrycznych. Jeżeli uznamy, że wizerunek twarzy jest przykładem danych biometrycznych, to po dokonaniu podstawienia wizerunku pod dane biometryczne uzyskujemy: „**wizerunek twarzy**" oznacza dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby (…).". Przeprowadzone podstawienie, zgodne z intencją prawodawcy prowadzi do absurdu. Kiedy pominiemy fantazje o mierzeniu biometrycznego zdjęcia twarzy, to uzyskujemy np. zdjęcie wiszące na ścianie czy nawet zdjęcie w pamięci komputera i wniosek, że jest ono danymi biometrycznymi (sic!). Zwracam uwagę, że zdjęcie to zdjęcie, zdjęcie może zawierać dane biometryczne lub nie, ale zdjęcie to nie dane. Oczywiście wniosek zgodnie z którym zdjęcie to dane biometryczne jest absurdalny, należy go odrzucić a przepis poprawić.

Rozumowanie drugie.

Można spróbować uratować sens przykładu wskazanego w przepisie i doszukać się błędu w polskiej wersji tłumaczenia. Przykład dotyczący wizerunku twarzy nabrałby innej wymowy, gdyby przepis wyglądał następująco: „„**dane biometryczne**" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, ~~takie~~ **takich** jak wizerunek twarzy lub dane daktyloskopijne". Jeżeli słowo *takie* zamienimy na „takich", to okazuje się, że wizerunek twarzy nie jest przykładem danych biometrycznych staje się za to przykładem „cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej". Kiedy odrzucimy cechy fizjologiczne i behawioralne, na co konstrukcja przepisu pozwala. Pozwala na to również wersja angielska przepisu. Przepis w wersji angielskiej stanowi: *'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,* ***such*** (wytłuszczenie: J. Rz) *as facial images or dactyloscopic data*. Wytłuszczone *such* można przetłumaczyć na „takie jak" ale i na „takich jak". Przepis po poprawieniu nabiera nieco sensu, w zakresie wizerunku twarzy jako przykładu już

nie danych biometrycznych a jedynie cech fizycznych. Wydaje się, że niestety ratunek dla przepisu, którego tu szukam, nie może nadejść. O ile można uznać, że wizerunek twarzy to cecha fizyczna lub cechy fizyczne, to z danymi daktyloskopijnymi już takiego rozumowania przeprowadzić nie można. Dane daktyloskopijne to nie są cechy fizyczne osoby fizycznej, są to dane, które z tych cech wynikają. Dane daktyloskopijne można, przy pewnej przychylności dla twórcy definicji, uznać za dane biometryczne na jej gruncie. Dane daktyloskopijne występują w przepisie obok wizerunku twarzy. Konstrukcja przepisu nie pozwala przyjąć, że wizerunek twarzy jest przykładem cech fizycznych a dane daktyloskopijne są przykładem danych biometrycznych, innymi słowy, zamiana *takie jak* na „takich jak" byłaby błędem tłumaczenia. Wniosek jest jeden, przepis nie jest źle przetłumaczony, przepis jest źle napisany.

3. Art. 4 pkt 14. Uwagi

3.1. Art. 4 pkt 14. Uwaga 1. Mylne domniemanie

Możliwe jest jedno wyjaśnienie słów, *(...)„**dane biometryczne" oznaczają dane osobowe** (...)*, a mianowicie, że słowami tymi prawodawca ustanawia domniemanie z mocy którego dane biometryczne to zawsze dane osobowe. Prawodawca wprowadza to domniemanie z tego powodu, ze dane biometryczne mają charakter unikatowy, są ścisłe powiązane z osoba, której dotyczą, więc zagrożeniem dla praw i wolności tej osoby byłoby traktowanie danych biometrycznych nie jak danych osobowych, nawet jeżeli nie umożliwiają ustalenia rozsądnymi metodami, której konkretnie osoby fizycznej dotyczą. Zaznaczam, że przeprowadzone powyżej rozumowanie, z którego wynika, że dane biometryczne zawsze danymi osobowymi, nie oddaje mojego poglądu w tej sprawie. Rozumowanie to prezentuję, ponieważ widzę możliwość jego przeprowadzenia i ponieważ rozumowanie takie może być uznane za uzasadnienie dla rzekomego domniemania wynikającego z przepisu, podkreślam jednak ponownie, że rozumowanie to sygnalizuję jako możliwe, jednak nie jako poprawne i nie jako oddające mój pogląd.

4. Art. 4 pkt 14. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 14 RODO definiuje *dane biometryczne*, zatem zgodnie z dyrektywą języka prawnego[385], każdy kto interpretuje RODO powinien rozumieć pojęcie dane biometryczne" tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie *dane biometryczne* tak jest ono zdefiniowane w art. 4 pkt. 14 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia *dane biometryczne* zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 14. Konkretyzacja zasady I

Artykuł 4 ust. 14 RODO sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Namysł nad tym czy konkretne, przetwarzane przez danego administratora dane biometryczne są danymi osobowymi może pomóc w podjęciu decyzji o zaniechaniu ich przetwarzania lub o ich anonimizacji. Anonimizacja danych biometrycznych, służących do otwierania zamka w drzwiach, nie ma sensu, anonimizacji danych biometrycznych wykorzystywanych do ustalenia jakiej wielkości płaszcze należy produkować w następnym sezonie, sens ma.

Realizacja **zasady rzetelności**. Jeżeli administrator przetwarza dane biometryczne, będące danymi osobowymi, to powinien poinformować osobę, której dane dotyczą o fakcie przetwarzania danych, na gruncie art. 13 lub art. 14 RODO.

Realizacja **zasady przejrzystości**. Jeżeli administrator przetwarza dane biometryczne, będące danymi osobowymi, to powinien poinformować osobę, której dane dotyczą o szczegółach przetwarzania danych, na gruncie art. 13 lub art. 14 RODO.

[385] L. Morawski, *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

Realizacja **zasady ograniczenia celu**. Wyciek danych biometrycznych będących danymi osobowymi może doprowadzić, do złamania tej zasady, jeżeli bowiem dane wyciekną, to administrator traci kontrolę nad tym w jakim celu są one przetwarzane.

Realizacja **zasady minimalizacji**. Z punktu widzenia realizacji tej zasady, lepiej jest przetwarzać dane biometryczne, które nie są danymi osobowymi. Oczywiście jeżeli przetwarzanie danych osobowych jest niezbędne dla osiągnięcia celu przetwarzania, to nie ma problemu z dopuszczalnością przetwarzania tych danych, patrząc z punktu widzenia zasady minimalizacji.

Nie powinno się tu jednak wyciągać wniosków pochopnych, czyli, że na przykład używanie zamków biometrycznych jest zawsze dopuszczalne i że wolno w celu używania takiego zamka przetwarzać dane osobowe ponieważ bez tego się nie da. Jest to rozumowanie błędne.

Użycie zamka biometrycznego należy utożsamić z przetwarzaniem biometrycznych danych osobowych i zastanowić się, czy dla czynności zabezpieczenia wejścia zamkiem, konieczne jest użycie zamka biometrycznego – to jest rozumowanie poprawne.

Realizacja **zasady ograniczenia przechowywania danych**. Jeżeli administratorowi do jego celów potrzebne są biometryczne dane osobowe, to zawsze, w jakimś sensie naraża się na naruszenie tej zasady (jak i innych zasad), jeżeli jednak administrator używa danych biometrycznych nieosobowych, to problem z potencjalnym naruszeniem zasady znika.

Realizacja **zasady integralności**. Podobnie jak w przypadku poprzedniej zasady, jeżeli administrator przetwarza biometryczne dane nieosobowe, to nie grozi mu złamanie zasady.

Realizacja **zasady poufności**. i tu też, przetwarzanie biometrycznych danych nieosobowych zabezpiecza przed naruszeniem zasady.

6. Art. 4 pkt 14. Postulaty de lege ferenda

6.1 Art. 4 pkt 14. Postulat 1. Usunięcie mylnego domniemania

W analizie słów *(...),,**dane biometryczne" oznaczają dane osobowe** (...)* przedkładam, że dane biometrzyczne czasem danymi osobowymi są, czasem nie. Zależy to po prostu od tego czy dotyczą zidentyfikowanej lub mozliwej do zidentyfikowania osoby fizycznej. Skoro tak właśnie jest, to zacytowany fragment przepisu jedynie

wprowadza w błąd. Skoro przepis wprowadza w błąd to nie pozostaje nic innego jak go zmienić, tak by już w błąd nie wprowadzał.

W związku z powyższym postuluję aby początek przepisu brzmiał: „„**dane biometryczne**" oznaczają dane ~~osobowe~~, które (…)". (Czcionką przekreśloną zaznaczam słowa usunięte.)

Z uwagi na kolejne postulaty nowelizacyjne, ostateczną wersję przepisu prezentuje po prezentacji ostatniego z postulatów.

6.2 Art. 4 pkt 14. Postulat 2. Usunięcie mylnego domniemania

Wersja angielska przepisu brzmi: *'biometric data' means personal data resulting from specific technical processing (...)*. Czeska wersja brzmi: *„biometrickými údaji" osobní údaje vyplývající z konkrétního technického zpracování (...)*. Nawet Google translator tłumaczy *konkrétního technického zpracování* na „określone przetwarzanie techniczne". Pomijając błąd w przypadku, widzimy „określone". Jak widać przetłumaczono *specific* na „konkrétního" czyli „określonego". *Specific technical processing* przetłumaczone Google translatorem brzmi „określone przetwarzanie techniczne". Można próbować uratować intencję i tłumaczyć, że wersja polska nie powstała w wynikau użycia google translatora a w wyniku użycia fachowej wiedzy tłumacza. Niestety wyjaśnienie takie jest niewiele warte. Słownik bab.la jako tłumaczenia słowa *specific* podaje „konkretny, określony, szczegółowy, specyficzny, dokładny". Jeżeli zaglądamy do źródeł papierowych to sytuacja wygląda podobnie. Słownik angielsko-polski wydawnictwa Park z 2003 roku tłumqczy *specific* na „określony, odrębny, właściwy, specyficzny".[386] Słownik wydawnictwa Graf-Punkt, na licencji wydawnictwa HarperCollins tłumaczy *specific* na „określony, ścisły, specyficzny"[387].

Wniosek z prowadzonych wyżej rozważań jest oczywisty, tłumaczenie polskie jest błędne i wymaga poprawienia.

W związku z powyższym postuluję aby początek przepisu brzmiał: „„**dane biometryczne**" oznaczają dane osobowe, które wynikają ze ~~specjalnego~~ **określonego** przetwarzania technicznego (…)".

---

[386] Redakcja merytoryczna E. Jaszczurowska, J. Marcisz. *Słownik angielsko-polski,* Bielsko-Biała 2003, s. 780.

[387] Collins. *Słownik angielsko polski* pod red. J. Fisiaka. Warszawa 2002, s. 423.

(Czcionką przekreśloną zaznaczam słowo usunięte z powodu złego tłumaczenia, czcionką wytłuszczoną zaznaczam proponowane tłumaczenie.)

6.3 Art. 4 pkt 14. Postulat 3.
Poprawienie rozłożenia przykładów w przepisie

Rozumowanie przeprowadzone wyzej w analizie słów: *Ze słów wytłuszczonych: „(...)* ***takie jak wizerunek twarzy lub dane daktyloskopijne*** prowadzi do wniosku, że *wizerunek twarzy* jest przykładem „cech fizycznych", zaś *dane daktyloskopijne* są przykładem danych biometrycznych.

W związku z powyższym postuluję aby przepis brzmiał:
„„„**dane biometryczne**" oznaczają dane osobowe **(na przykład dane daktyloskopijne)**, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych **(na przykład wizerunek twarzy)**, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, ~~takie jak wizerunek twarzy lub~~ ~~dane daktyloskopijne~~;
(Czcionką przekreśloną zaznaczam słowo usunięte z powodu złego tłumaczenia, czcionką wytłuszczoną zaznaczam proponowane tłumaczenie.)

6.3 Art. 4 pkt 14. Postulat 1+2+3=4.
Wniosek z postulatów de lege ferenda

Z uwagi na fakt, że postawiłem 3 postulaty de lege ferenda do art. 4 pkt 14 RODO oraz z uwagi na fakt, że postulaty te się nie wykluczają przedstawiam niżej wersję przepisu, która ujmuje trzy powyżej postawione postulaty.
„„„**dane biometryczne**" oznaczają dane ~~osobowe~~ **(na przykład dane daktyloskopijne)**, które wynikają ~~ze specjalnego~~ **z określonego** przetwarzania technicznego, dotyczą cech fizycznych **(na przykład wizerunek twarzy)**, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, ~~takie jak wizerunek twarzy lub~~ ~~dane daktyloskopijne~~;
(Czcionką przekreśloną i podkreśloną zaznaczam słowa usunięte z powodu złego tłumaczenia, czcionką wytłuszczoną i podkreśloną zaznaczam proponowane tłumaczenie, czcionką przekreśloną zaznaczam słowa usunięte, czcionką wytłuszczoną zaznaczam słowa dodane.)

Artykuł 4 pkt 15 RODO

„dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

1. Art. 4 pkt 15. Komentarz

Przepis definiuje dane osobowe dotyczące zdrowia.
Dane dotyczące zdrowia są danymi osobowymi.
Są to dane osobowe dotyczące zdrowia fizycznego lub psychicznego os fizycznej.
Z użycia funktora „lub" wnosimy, że dane dotyczące zdrowa są to jedynie dane dotyczące zdrowia fizycznego, lub jedynie dane dotyczące zdrowia psychicznego lub dane dotyczące obydwu tych sfer.

2. Art. 4 pkt 15. Analiza

Ze słów oznaczonych w przepisie: „„**dane dotyczące zdrowia**" **oznaczają** (...)" wynika, że przepis definiuje dane osobowe dotyczące zdrowia.
Ze słów oznaczonych w przepisie: „„**dane dotyczące zdrowia**" **oznaczają dane osobowe** o (...)" wynika, że dane dotyczące zdrowia są danymi osobowymi, czy też raczej, że przepis dotyczy tych danych dotyczących zdrowia, które są danymi osobowymi.
Ze słów oznaczonych w przepisie**:** „(...) **dane osobowe o zdrowiu** (...)" wynika, że są to dane osobowe dotyczące zdrowia.
Ze słów oznaczonych w przepisie: „(...) **zdrowiu fizycznym lub psychicznym osoby fizycznej** (...)wynika, że są to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej.
Ze słów oznaczonych w przepisie: „(...) **lub** (...)" wynika, że są to dane osobowe dotyczące zdrowia fizycznego lub psychicznego os fizycznej. Z użycia funktora lub wnosimy, że dane dotyczące zdrowa są to jedynie dane dotyczące zdrowa fizycznego, lub jedynie dane dotyczące zdrowia psychicznego lub dane dotyczące obydwu tych sfer.
Ze słów oznaczonych w przepisie: „(…) **w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia**"

wynika, że dane do danych dotyczących zdrowia, zdefiniowanych w przepisie należy zaliczyć również dane dotyczące korzystania z usług opieki zdrowotne ale tylko w sytuacji jeżeli te dane ujawniają informacje o stanie zdrowia. Pobieżna lektura może budzić wrażenie, że popełniam tu błąd, łącząc części przepisu tak jak je do omawiania połączyłem odsyłam jednak do uwagi *3.1. Art. 4 pkt 15. Uwaga 1. Niespójność przepisu* i do postulatu *6.1 Art. 4 pkt 15. Postulat 1. Poprawienie błędu w tłumaczeniu*.

Przepis zawiera tez drugi błąd translatorski, miast o korzystaniu z usług opieki zdrowotnej powinien on stanowić o tych usług udzielaniu *6.2 Art. 4 pkt 15. Postulat 2. Poprawienie kolejnego błędu w tłumaczeniu*.

Omawiam jednocześnie dwie semantyczne części przepisu, czynię to jednak dlatego, że części te są ze sobą ścisłe powiązane. Dopiero informacja o ujawnianiu informacji o stanie zdrowia osoby fizycznej konkretyzuje jakie informacje dotyczące zdrowia są danymi medycznymi. dotyczące zdrowia są danymi osobowymi. Podkreślam zatem, że z przepisu wynika, że informacje o korzystaniu z usług opieki zdrowotnej są informacjami o stanie zdrowia tylko wtedy jeżeli ujawniają informacje o stanie zdrowia osoby fizycznej. Ma to duże znaczenie dla zgodności z prawem przetwarzania takich danych. Artykuł 9 ust. 2 RODO zabrania przetwarzania (m. in.) danych dotyczących zdrowia. Przepis ten dotyczy danych zdefiniowanych w art. 4 pkt 15 RODO, z tym, że właśnie jeśli chodzi o dane o korzystaniu z usług opieki zdrowotnej, to przepis dotyczy ich tylko jeżeli ujawniają informacje o stanie zdrowia. Kwestia niestety jest w znacznej mierze ocenna. Informacja o korzystaniu z usług lekarza medycyny pracy, nie ujawnia informacji o stanie zdrowia – obowiązki w tej mierze związane są z dopuszczeniem do pracy. Informacja o wizycie u jakiegokolwiek innego lekarza może ujawniać informacje o stanie zdrowia osoby, która wizytę odbyła. Oczywiście nie musi ujawniać, jednak można przyjąć, że zwłaszcza fakt informacji o wizycie u lekarza specjalisty (pomijam specjalistę z zakresu medycyny rodzinnej), może co najmniej grozić ujawnieniem informacji o stanie zdrowia.

3. Art. 4 pkt 15. Uwagi
3.1. Art. 4 pkt 15. Uwaga 1.
Niespójność przepisu

Niestety i w omawianym przepisie nie ustrzeżono się błędu w tłumaczeniu z języka angielskiego. Przepis w języku polskim stanowi: *„**dane dotyczące zdrowia**” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia*. Lektura przepisu wskazuje na fakt, że słowa *ujawniające informacje o stanie jej zdrowia* odnoszą się do słów *dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej*, tworząc złożenie „dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (…) ujawniające informacje o stanie jej zdrowia”. Problem polega na tym, że złożenie to nie ma sensu. Nie ma przecież sensu mówić o danych o zdrowiu ujawniających informacje o stanie zdrowia. Dane o zdrowiu z założenia ujawniają informacje o stanie zdrowia. Odejście od wykładni językowej by zrozumieć o co tak na prawdę prawodawcy chodzi w przepisie i interpretacja w kierunku celowościowym nie są konieczne. Wystarczy zapoznać się z wersją anglojęzyczną. Stanowi ona: *‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*”. Zwracam zwłaszcza uwagę na słowa: *(...) including the provision of health care services, which reveal information about his or her health status*.

Purysta językowy mógłby się zastanowić dlaczego udzielanie usług opieki zdrowotnej (*the provision of health care services*) zastąpiono korzystaniem z tych usług, zostawiając to jednak na boku, zwracam uwagę, że z wersji angielskiej przepisu wynika, że *the provision of health care services* czyli zapewnienie usług opieki zdrowotnej należy do danych o stanie zdrowia, jeżeli *reveal information about his or her health status*, czyli jeżeli ujawnia informacje o stanie zdrowia. Po prostu w polskim tłumaczeniu, tłumacz nie zrozumiał przepisu, użył imiesłowu w złym przypadku i połączył w ten sposób nie te części przepisu, które trzeba. Przepis trzeba czytać następująco: „„**dane dotyczące zdrowia**” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniającym informacje o stanie jej zdrowia”. Niżej

stawiam odpowiedni postulat de lege ferenda, a to: *6.1 Art. 4 pkt 15. Postulat 1. Poprawienie błędu w tłumaczeniu*.

4. Art. 4 pkt 15. Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

- Artykuł 4 pkt 15 RODO definiuje **o dane dotyczące zdrowia**, zatem zgodnie z dyrektywą języka prawnego[388], każdy kto interpretuje RODO powinien rozumieć pojęcie „**dane dotyczące zdrowia**" tak jak jest ono w komentowanym przepisie zdefiniowane.

  Administrator, który siłą rzeczy interpretuje RODO, ma obowiązek rozumieć pojęcie „**dane dotyczące zdrowia**" tak jest ono zdefiniowane w art. 4 pkt. 15 RODO.
- Jednocześnie z przepisu wynika uprawnienie, zgodnie z którym osoba, której dane dotyczą ma prawo oczekiwać, że ADO będzie rozumiał znaczenie pojęcia „**dane dotyczące zdrowia**" zgodnie z definicją języka prawnego znajdującą się w komentowanym przepisie.

5. Art. 4 pkt 15. Konkretyzacja zasady I

Artykuł 4 ust. 14 RODO sprzyja realizacji zasad w opisany poniżej sposób.

Realizacja **zasady zgodności z prawem**. Namysł nad tym czy konkretne, przetwarzane przez danego administratora **dane dotyczące zdrowia** są danymi osobowymi może pomóc w podjęciu decyzji o zaniechaniu ich przetwarzania lub o ich anonimizacji. Anonimizacja danych dotyczących zdrowia czasem jest racjonalna, na przykład jeśli chodzi o dane przetwarzane do celów ściśle naukowych. Dane w domenie badań klinicznych też bywają anonimizowane, ale już na wysokim stopniu agregacji, kiedy dane stają się ilościowymi, wcześniej dane te są jedynie pseudonimizowane a i to tylko częściowo – w dokumentacji medycznej w ośrodku badawczym znajdują się dane niespseudonimizowane.

Realizacja **zasady rzetelności**. Jeżeli administrator przetwarza **dane dotyczące zdrowia**, będące danymi osobowymi, to powinien poinformować osobę, której dane dotyczą o fakcie przetwarzania danych, na gruncie art. 13 lub art. 14 RODO. Należy tu pamiętać, że

[388] L. Morawski. *Zasady wykładni prawa,* Toruń 2006, s. 93-99, zwłaszcza 95.

w niektórych realiach medycznych funkcjonuje zwolnienie zawarte w art. 14 ust. 5 lit. c RODO.

Realizacja **zasady przejrzystości**. Jeżeli administrator przetwarza **dane dotyczące zdrowia**, będące danymi osobowymi, to powinien poinformować osobę, której dane dotyczą o szczegółach przetwarzania danych, na gruncie art. 13 lub art. 14 RODO. Należy tu pamiętać, że w niektórych realiach medycznych funkcjonuje zwolnienie zawarte w art. 14 ust. 5 lit. c RODO.

Realizacja **zasady ograniczenia celu**. Wyciek danych dotyczących zdrowia, będących danymi osobowymi może doprowadzić, do złamania tej zasady, jeżeli bowiem dane wyciekną, to administrator traci kontrolę nad tym w jakim celu są one przetwarzane. Oczywiście bezpieczniej je pseudonimizować, jednak zwykle jest to niedopuszczalne, w większości realiów medycznych. Dopuszczalne jest to w dziedzinie badań klinicznych i tam właśnie dane takie pseudonimizowane są.

Realizacja **zasady minimalizacji**. Z punktu widzenia realizacji tej zasady, lepiej jest przetwarzać **dane dotyczące zdrowia**, które nie są danymi osobowymi. Oczywiście jeżeli przetwarzanie danych osobowych jest niezbędne dla osiągnięcia celu przetwarzania, to nie ma problemu z dopuszczalnością przetwarzania tych danych, patrząc z punktu widzenia zasady minimalizacji.

Realizacja **zasady ograniczenia przechowywania danych**. Jeżeli administratorowi do jego celów potrzebne są **dane dotyczące zdrowia** (dane osobowe), to zawsze, w jakimś sensie naraża się na naruszenie tej zasady (jak i innych zasad), jeżeli jednak administrator używa danych dotyczących zdrowia nieosobowych, to problem z potencjalnym naruszeniem zasady znika, z tym, że są to dane spoza zakresu definicji z art. 4 pkt 15 RODO.

Realizacja **zasady integralności**. Podobnie jak w przypadku poprzedniej zasady, jeżeli administrator przetwarza **dane dotyczące zdrowia** jako dane nieosobowe, to nie grozi mu złamanie zasady, z tym, że są to dane, które w definicji z art. 4 pkt 15 RODO zdefiniowane nie są. Realizacji zasady integralności sprzyja zabezpieczenie danych przed naruszeniami z art. 4 pkt 12 RODO.

Realizacja **zasady poufności**. i tu też, przetwarzanie danych dotyczących zdrowia, jako danych nieosobowych, czyli danych spoza definicji z art. 4 pkt 15 RODO, zabezpiecza przed naruszeniem zasa-

dy. Realizacji zasady integralności sprzyja zabezpieczenie danych przed naruszeniami z art. 4 pkt 12 RODO.

6. Art. 4 pkt 15. Postulaty de lege ferenda

6.1 Art. 4 pkt 15. Postulat 1. Poprawienie błędu w tłumaczeniu

Wyżej w uwadze *3.1. Art. 4 pkt 15. Uwaga 1. Niespójność przepisu* wykazałem, że w polskiej wersji przepisu użyto imiesłowu w niewłaściwym przypadku.

W związku z powyższym postuluję aby słowo *ujawniające* usunąć z przepisu i na jego miejsce wstawić słowo „ujawniającym".

Z uwagi na jeden jeszcze postulat nowelizacyjny, ostateczną wersję przepisu prezentuje po prezentacji drugiego z postulatów.

6.2 Art. 4 pkt 15. Postulat 2. Poprawienie kolejnego błędu w tłumaczeniu

Wyżej w uwadze 3.1. Art. 4 pkt 15. Uwaga 1. Niespójność przepisu zwróciłem uwagę na fakt, że niewłaściwie przetłumaczono słowa: *the provision of health care services*, czyli „zapewnienie usług och¬rony zdrowia. Pomijam nużące rozważania oparte na kolejnych słownikach, każde dziecko, które uczyło się języka Szekspira i Keitha Ri¬chardsa wie, że „to provide" oznacza „zapewniać, dostarczać" ale na pewno nie uzyskiwać. „To provide", czyli „dostarczyć, uzyskać" możemy komuś, zaś uzyskać możemy od kogoś. Tajemnicą nieodkrytą pozostanie dlaczego tłumacz tego nie wiedział. Zwracam uwagę, że czym innym są informacje o udzielaniu usług zdrowotnych a czym innym są informacje o uzyskiwaniu takowych. Informacje o udzielaniu to informacje o działaniu podmiotu medycznego, ewentualnie uzupełnione informacjami o tym komu ów podmiot usługę świadczył. Informacje o uzyskiwaniu to informacje o czynnościach osoby uzyskującej usługę, , ewentualnie uzupełnione informacjami o tym kto osobie daną usługę świadczył. Inne podmioty, inne zagrożenia. W związku z powyższym postuluję aby słowa o korzystaniu z usunąć z przepisu i na ich miejsce wstawić słowo „świadczeniu".

6.3 Art. 4 pkt 15. Postulat 1+2=3. Wniosek z postulatów de lege ferenda

Z uwagi na fakt, że postawiłem 2 postulaty de lege ferenda do art. 4 pkt 15 RODO oraz z uwagi na fakt, że postulaty te się nie wykluczają przedstawiam niżej wersję przepisu, która ujmuje obydwa powyżej postawione postulaty.

„„**dane dotyczące zdrowia**" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o k~~orzystaniu z~~ **udzielaniu** usług opieki zdrowotnej – ~~ujawniające~~ **ujawniającym** informacje o stanie jej zdrowia"

(Czcionką przekreśloną zaznaczam słowa usunięte z powodu złego tłumaczenia, czcionką wytłuszczoną zaznaczam proponowane tłumaczenie.)

Realizacja celów pracy

Realizacja celów pracy

W rozdziale niniejszym odnoszę się do realizacji celów pracy. Cele te wskazuję na początku pracy w Rozdziale 1, zatytułowanym: *Cele pracy i uzasadnienie konstrukcji pracy*. Praca nie zawiera rozdziału, w którym podsumowywałbym wnioski z pracy. Praca zawiera 114 „uwag", z którym prawie każda jest osobnym podrozdziałem, zawierającym często własne wnioski autora pracy, oraz około 50 postulatów de lege ferenda, które z założenia mają charakter wniosków. Piszę, że postulatów jest około 50, ponieważ rachunkowo jest ich 56, jednak niektóre postulaty stanowią połączenie na przykład dwóch innych postulatów, postawionych wobec tego samego przepisu, zatem wskazanie ile postulatów dokładnie jest, jest niezupełnie możliwe, na pewno jest ich właśnie ok 50. Zarówno uwagi jak i postulaty mają charakter wniosków z pracy.

Realizacja celu:

„Analiza tekstu prawnego RODO"

Na początku pracy, wskazuję, że analiza tekstu prawnego RODO nie jest podstawowym celem pracy, wskazuję, że analiza tekstu jest narzędziem, które pozwala na prowadzenie dalszych rozważań w pracy. Praca niniejsza, jak wszystkie moje prace, powstawała liniowo. Najpierw założyłem cele pracy, następnie przystąpiłem do ich realizacji. Uważam, że takie podejście jest naukowo najuczciwsze. Badacz ryzykuje w ten sposób, że celów pracy nie zrealizuje, z drugiej jednak strony uważam, że jeżeli prawnik zakłada realizację celu badawczego, to dobrze by go zrealizował, jeżeli jednak się to nie uda, lub nie uda się w pełni, to nie oznacza to wcale, że badania poniosły fiasko. Badania naukowe stanowią zawsze pewną podróż w nieznane. Badania prowadzimy po to by się czegoś dowiedzieć. Czasem tylko po to by się czegoś dowiedzieć, czasem również po to by wiedzę tę spożytkować w praktyce. Nie ukrywam, że jestem zwolennikiem łączenia tych podejść, tak by najpierw się czegoś dowiedzieć a następnie by wiedze zdobytą, w praktyce spożytkować. Oczywiście nie oznacza to, że badania musi spożytkować badacz, ważne jest jednak, by miały one jakiś praktyczny wymiar.

Mimo, że analiza tekstu prawnego nie jest podstawowym celem pracy, mimo, że analiza tekstu prawnego jest narzędziem służącym do realizacji pozostałych celów pracy, to jednak analiza tekstu prawnego jednym z celów pracy jest. W związku z tym należy ocenić, czy cel ten został zrealizowany. Analiza tekstu prawnego została przeprowadzona przy pomocy mojej autorskiej metody analizy tekstu prawnego, a mianowicie przy pomocy Etapowej Analizy Semantycznej. Jeżeli zatem zadaję sobie pytanie czy cel rozumiany jako analiza tekstu prawnego został zrealizowany, to stwierdzić muszę, że uważam iż tak się stało. Z racji wykorzystania Etapowej Analizy Semantycznej, przeanalizowane zostało w pracy niemal każde słowo przepisów, których analiza jest podstawą niniejszej pracy. Na podstawie analizy wyciągnąłem wnioski dotyczące uprawnień i obowiązków jakie wynikają z analizowanych przepisów. Analiza pozwoliła mi również na sformułowanie uwag (w podrozdziałach kategorii *Uwagi*) i na postawienie postulatów *de lege ferenda*. Analiza tekstu prawnego jest, z uwagi na przyjęte założenia badawcze, elementem badania tekstu od którego zaczynam pracę nad każdym przepisem. Uważam, że bez realizacji analizy tekstu prawnego, nie mógłbym zrealizować pozostałych celów pracy. Niżej wskazuję, że uważam, że pozostałe cele pracy zostały zrealizowane, w związku z czym, uważam że skoro zostały zrealizowane cele, do realizacji których, analiza tekstu prawnego jest etapem, to cel ujęty jako analiza tekstu prawnego, również zrealizowany został.

Realizacja celu:

„Prezentacja Etapowej Analizy Semantycznej

Cel ten realizowany jest w podrozdziałach warstwy: *Komentarz* i w podrozdziałach warstwy: *Analiza*.

Praca niniejsza składa się z rozdziałów, które dzielą się na podrozdziały, które nazwałem warstwami. Wszelkie cele pracy, których realizację omawiam niżej, uzależnione są od analizy tekstu prawnego RODO. Analiza tekstu prawnego niezbędna dla przeprowadzenia dalszych rozważań, została przeprowadzona przy użyciu Etapowej Analizy Semantycznej, czyli mojej autorskiej metody analizy przepisów. Analiza tekstu prawnego niezbędna jest dla ustalenia jakie obowiązki spoczywają na administratorze (danych) i jakie uprawnienia przysługują osobom których dane dotyczą. W sposób

tradycyjny obowiązki administratora i uprawnienia osób których dane dotyczą opisałem w podrozdziałach należących do warstwy *Komentarz*. W sposób oparty o Konceptualizm Prawniczy - Ogólną Teorię Prawa, opisałem to w podrozdziałach należących do warstwy *Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa*. Na podstawie obserwacji poczynionych na gruncie Etapowej Analizy Semantycznej sformułowałem uwagi i zamieściłem je w podrozdziałach kategorii *Uwagi*.

Postawienie postulatów *de lege ferenda*, które zamieściłem w podrozdziałach kategorii *Postulaty de lege ferenda* było możliwe dzięki drobiazgowej analizie tekstu, która pozwoliła mi na oderwanie się od konwencjonalnego pospiesznego omawiania przepisów, opartego nieraz o pewne założenia, a często o ustalenia wcześniejszych badaczy i ze względu na swoją specyfikę niejako przymusiła mnie do własnej ich analizy. Analiza ta została przeprowadzona oczywiście z wykorzystaniem Etapowej Analizy Semantycznej.

Przeprowadzenie analizy, w podrozdziałach kategorii *Analiza*, z wykorzystaniem Etapowej Analizy Semantycznej, a zwłaszcza oparcie treści pozostałych rozdziałów na wnioskach, które uzyskałem na drodze tej analizy, pozwala, jak sądzę, skonstatować, że cel, jakim przy przystępowaniu do pracy była prezentacja Etapowej Analizy Semantycznej, został zrealizowany.

Stosując metodę jako narzędzie analizy przepisów, zaprezentowałem, że pozwala ona właśnie na drobiazgową analizę tekstu prawnego. Ta drobiazgowa analiza pozwala na stosunkowo łatwe sformułowanie zdań o charakterze komentarza do analizowanych przepisów. Ta sama drobiazgowa analiza pozwala następnie, tam gdzie to potrzebne – na polemikę z poglądami doktryny, tam gdzie to wystarczające – na dyskusję z tymi poglądami, a tam gdzie to właściwe – na rozwinięcie poglądów doktryny. Drobiazgowość zastosowanej metody analizy ułatwia ogromnie ustosunkowanie się do poglądów zastanych, zwłaszcza, nie ukrywam, tam, gdzie w poglądach tych obecne są pominięcia lub uogólnienia, wyrosłe na przykład na podglebiu innych, też nie do końca przemyślanych poglądów lub na podglebiu poglądów, które narosły na gruncie poprzedniego stanu prawnego. RODO reguluje podobne sprawy jak te, które regulowała Dyrektywa 95/46/WE, jednak, co nie zawsze jest zauważane – reguluje je często inaczej. Ogromny dorobek doktryny, narosły przed pojawieniem się RODO, skłania do korzystania z tego dorobku. Dorobku

tego nie odrzucam, uważam jednak, że niewolnicze trzymanie się go może prowadzić do mylnych wniosków interpretacyjnych, kiedy przychodzi do interpretacji przepisów RODO. Dawny dorobek doktryny nie powinien być szkłem, przez które patrzymy na RODO. Mając to na uwadze, w publikacji patrzę na RODO głównie przez pryzmat wykładni prawa. Podejście takie daje mi możliwość niejako rozpoczęcia pracy od nowa. Obcuję z tekstem prawnym i ustalam co z niego wynika, dopiero kiedy już to ustalę, konfrontuję to co ustaliłem z poglądami zastanymi. Wszystko o czym tu piszę, czyli systematyczne przeszukiwanie gleby tekstu prawnego RODO, możliwe jest dzięki zastosowanie Etapowej Analizy Semantycznej. Metoda ta jest może żmudna, jednak, po biegłym jej opanowaniu, pozwala ona na wnikliwą analizę przepisów a to z kolei pozwala na realizację kolejnych celów pracy.

Realizacja celów:
„Prezentacja rozważań własnych, poczynionych na gruncie analizy przepisu”, „prezentacja poglądów doktryny”, „polemika z poglądami doktryny”

Cel ten realizowany jest w podrozdziałach warstwy: *Uwagi*.

W niniejszej publikacji znajduje się około 114 „uwag” liczonych jako podrozdziały drugiego i trzeciego rzędu w podrozdziałach warstwy *Uwagi*. W Rozdziale 1, poświęconym analizie art. 1 RODO znajduje się 9 podrozdziałów pierwszego rzędu warstwy *Uwagi* i 9 podrozdziałów drugiego rzędu warstwy *Uwagi*. Z racji konstrukcji formalnej pracy, podrozdziałów pierwszego rzędu jest jedynie 9, jednak w sumie, w Rozdziale 1, zajmują one nieco ponad 107 tysięcy znaków. Znaczny rozmiar niektórych podrozdziałów warstwy *Uwagi* w Rozdziale 1 spowodowany jest pewnym faktem. Otóż w podrozdziałach tych omawiam rzecz doniosłą dla rozumienia i stosowania wielu dalszych przepisów RODO, a mianowicie nazywam w nich i wymieniam prawa i wolności, jakie, jak uważam, są na gruncie RODO chronione. Nie widzę sensu, by w tym miejscu streszczać poszczególne podrozdziały, nie taki jest cel tej części pracy, zwracam jednak uwagę na ich treść, o tyle o ile uważam, że treść ta uzasadnia

realizację kolejnych celów pracy. Dlatego właśnie zwracam uwagę na fakt, że najpierw zajmuję się prawami, które wynikają z art. 5 ust. 1 RODO, które z racji tytułu tego przepisu (*Zasady dotyczące przetwarzania danych osobowych*) nazywam prawami zasadniczymi. Następnie zwracam uwagę na uprawnienie zasadnicze, wynikające z art. 5 ust. 2 RODO. Dalej zajmuję się prawami, które wynikają z przepisów szczegółowych RODO. Dalej jeszcze zwracam uwagę na wybrane prawa, które wynikają z Preambuły RODO, przy czym do praw tych zachowuję dystans, uważam bowiem, że powtarzają one prawa, które wynikają z przepisów szczegółowych RODO. Jeszcze dalej zajmuję się prawami, które wynikają z Karty Praw Podstawowych Unii Europejskiej. W końcu, nadal w kontekście praw, wyjaśniam dlaczego wskazanie, oznaczenie, chyba również nazwanie, praw i wolności jest tak ważne. Opracowanie kwestii praw i wolności, na gruncie RODO, jest tak ważne, ponieważ bez naukowego opracowania tej kwestii i praktycznego jej opanowania, niemożliwe jest trafne stosowanie co najmniej kilku przepisów RODO, a to przepisów, które uzależniają zaistnienie tych czy innych zjawisk od: już to naruszenia praw i wolności, już to od zagrożenia naruszeniem praw i wolności. Są to: art. 24 RODO, art. 32 RODO, art. 33 RODO, art. 34 RODO, art. 35 RODO i art. 36 RODO.

W każdym ze wskazanych przepisów znajdują się odwołania do praw i wolności, a skoro te odwołania się tam znajdują, to tak ważne jest by prawa i wolności miały charakter konkretnych, wskazanych, oznaczonych i nazwanych praw i wolności nie zaś jedynie miłego dla ucha, jednak niewiele znaczącego, zwrotu frazeologicznego. Jeśli chodzi o rozważania własne, to właśnie w ustaleniach, które dotyczą praw na gruncie RODO, widzę największą wartość, w kontekście prezentacji rozważań własnych.

Podrozdziały Rozdziału Pierwszego mają, jak widać, w dużej mierze charakter rozważań własnych. Poglądy doktryny, głównie traktowane polemicznie, pojawiają się w kilku podrozdziałach warstwy *Uwagi*, jednak główną treść tego rozdziału upatruję w rozważaniach własnych, poświęconych prawom – o czym piszę wyżej i marginalnie – obowiązkom i wolnościom. Obowiązkami i wolnościami zajmuję się szerzej (zwłaszcza obowiązkami) w pracach powstających równolegle z niniejszą, tu, z uwagi na treść przepisów, od których rozpoczynam rozważania, zajmuję się głównie prawami, rozumianymi jako uprawnienia osób fizycznych.

W Rozdziale Drugim, poświęconym analizie art. 2 RODO znajduje się 11 podrozdziałów warstwy *Uwagi*. Podrozdziały te maja charakter prezentacji poglądów własnych, spod których w kilku miejscach, niejako przebijają poglądy doktryny, nie tyle jako cel polemiki, ile raczej jako nadanie szerszego, bo nie tylko krajowego, wymiaru, prowadzonym rozważaniom

W Rozdziale Trzecim, poświęconym analizie art. 3 RODO znajdują się 4 podrozdziały warstwy *Uwagi*. Za najciekawszą cześć tego rozdziału uważam analizę relacji zachodzących przy przetwarzaniu danych osobowych przez administratorów i ich jednostki organizacyjne oraz podmioty przetwarzające i ich jednostki organizacyjne, na terenie UE lub w związku z działalnością prowadzoną na terenie UE. Proponuję tam również zapis symboliczny, mający ułatwić zapis, ale zwłaszcza szybkie odczytywanie relacji takich jak powierzenie przetwarzania danych osobowych, dalsze powierzenie przetwarzania danych osobowych czy udostępnienie danych osobowych.

W Rozdziale Czwartym, poświęconym analizie art. 4 RODO znajduje się 81 podrozdziałów warstwy *Uwagi*. Rozdział ten poświęcony jest rozważaniom definicyjnym, które uważam za fundament wszelkich rozważań, jeżeli bowiem interpretator nie rozumie zakresu pojęć, którymi się posługuje podczas rozstrzygania dylematów interpretacyjnych, to rozstrzygnięcia takie, czyli inaczej patrząc – wyniki wykładni oraz efekty subsumpcji, mają z założenia charakter co najwyżej przybliżony. W Rozdziale Czwartym poglądy doktryny są nieco bardziej obecne aniżeli w rozdziałach poprzedzających. Tu również staram się odwoływać do poglądów autorów europejskich, a to głównie do ciekawego komentarza do RODO, pod redakcją Ch. Kunera, L. A. Bygravea i Ch. Dockseya,[389], oraz, do nieznanego raczej w Polsce, a ciekawego komentarza czeskich autorów, przy podbudowaniu niektórych rozważań ustaleniami L. Morawskiego i M. Zirk-Sadowskiego, jednocześnie staram się korzystać, z bliskiej polskiemu Czytelnikowi, polskiej doktryny, zwłaszcza tam, gdzie jest to konieczne ze względów polemicznych. Z tego też względu, by

[389] The EU General *Data Protection Regulation (GDPR). A Commentary*. Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020.

ułatwić Czytelnikom śledzenie drogi ustaleń, która wiedzie czasem poza niniejszą pracę, pozostawiłem w niektórych miejscach pracy całe zapisy bibliograficzne, poświęcam w ten sposób, nieco, graficzną elegancję pracy, czyniąc jednak tym samym ukłon w kierunku ewentualnych jej Czytelników, zapisy skróciłem w miejscach, w których odnalezienie całego zapisu wiąże się z przerzuceniem kilku najwyżej kartek książki.

Rozdział Czwarty pełen jest rozmaitych drobnych uwag własnych, wyników własnych ustaleń, rozważań polemicznych, zawiera jednak też kilka momentów, które, mam nadzieję, są jaśniejszymi momentami w morzu definicyjnego bogactwa. Do momentów takich należą rozważania poświęcone różnicom miedzy administratorem, podmiotem przetwarzającym i odbiorcą. Rozważania te doprowadziły do sformułowania i przedstawienia w pracy, krokowego testu, którego wykonywanie, powinno, w sytuacjach wątpliwych, wątpliwości rozwiewać i pomagać w podejmowaniu właściwych decyzji interpretacyjnych, zwłaszcza na poziomie subsumpcji. Elementem związanym ze wskazanym testem jest wyliczenie i krótkie opisy ponad trzydziestu podmiotów, analizowanych pod kątem tego czy są administratorami czy podmiotami przetwarzającymi. Cześć tych podmiotów stanowi swoistą ciekawostkę są to bowiem podmioty, co do których problemy z ustaleniem ich roli mieli internauci w grupach fejsbukowych, w których bywam, także są to poprowadzone swoiste badania podstawowe, ale nie na poziomie wykładni, tylko na poziomie zapotrzebowania na wiedzę w konkretnym przedmiocie. Za ciekawy element uważam też analizę art. 4 pkt 12 RODO, podczas której, na drodze analizy dość krótkiego przepisu, udaje mi się uzyskać z jego treści 45 możliwych skutków naruszenia bezpieczeństwa.

W sumie praca zawiera 116 podrozdziałów warstwy *Uwagi*.

Realizacja celów:

„wskazanie błędów w RODO”,

„zaproponowanie postulatów de lege ferenda”

W pracy zamieszczono około 50 postulatów de lege ferenda, przybliżenie liczby wyjaśniam na początku części *Realizacja celów pracy*. Kiedy uświadamiam sobie, że postulaty te postawiłem wobec czterech i to nie w całości przeanalizowanych przepisów RODO, to

myślę, że mogę zaryzykować tezę, że cel drugi z tu wskazanych zrealizowałem. Niestety oczywiste staje się również, że skoro tyle postulatów udało się postawić, to nie świadczy to dobrze o jakości analizowanego aktu prawnego. Od tej właśnie myśli chciałbym przejść do myśli o wskazaniu błędów w RODO, otóż o ile niektóre z uwag warstwy *Uwagi* mogą być uważane za rewolucyjne, o tyle postulatów za takie bym nie uważał. Postulaty stawiam nie tam, gdzie widzę potrzebę szczególnej myśli prawniczej, postulaty stawiam tam, gdzie akt prawny wręcz się tego domaga, gdzie przepisy są nieporządnie zredagowane, niejasne, czasem dziwaczne. W takich sytuacjach staram się znaleźć drogę do ich poprawienia, jednak są to nie miejsca na wielką myśl prawniczą, są to zwykle miejsca, w których dokonuję poprawienia drobnych, irytujących ponieważ niepotrzebnych, błędów w RODO.

Realizacja celu: „prezentacja mojej autorskiej teorii obowiązywania i wykładni prawa, która nosi nazwę: „Konceptualizm Prawniczy jako Ogólna Teoria Prawa”"

W niniejszej pracy prezentuję głównie tę stronę Konceptualizmu Prawniczego, która poświęcona jest wykładni prawa, co pozwala mi, mam nadzieję, dowieść, że przynajmniej w tym zakresie, Konceptualizm Prawniczy nie jest teorią pustą. Jednocześnie posługiwanie się prostą, ale praktyczną, aparaturą Konceptualizmu Prawniczego, pozwala mi na sprawne odnajdywanie w przepisach, tego co jak uważam, przede wszystkim w przepisach odnaleźć wypada, a mianowicie uprawnień. Równie łatwe jest odnajdywanie obowiązków i wolności. Posługując się siatką pojęciową Konceptualizmu Prawniczego – Ogólnej Teorii Prawa zidentyfikowałem, po części nazwałem, wypisałem wiele praw, wolności i obowiązków, które są istotne dla tematyki poruszanej w pracy. Wskazane prawa, obowiązki i wolności wymienione są w Rozdziale Pierwszym pracy, w odpowiednich podrozdziałach warstwy *Uwagi*. Tu jedynie rachunkowo wskazuję, że wymieniłem tam:

- 11 praw i 11 wolności o charakterze zasadniczym, zidentyfikowanych na gruncie art. 5 RODO,

- 36 praw, 36 wolności i 36 obowiązków o charakterze szczegółowym, zidentyfikowanych na gruncie przepisów szczegółowych RODO,
- 77 praw o charakterze szczegółowym, zidentyfikowanych na gruncie Preambuły RODO, zwracam przy tym uwagę na fakt, że wiele z nich pokrywa się z prawami zidentyfikowanymi na gruncie art. 5 RODO lub na gruncie przepisów szczegółowych RODO,
- 153 prawa, zidentyfikowane na gruncie KPP UE, około 10 % tych praw pokrywa się z prawami zidentyfikowanymi na gruncie RODO.

Realizacja celu:

„ustalenie i wskazanie jakie prawa i wolności wskazane są w RODO jako istniejące”

W całości cel ten został sformułowany na początku pracy jako: *celem pracy jest ustalenie i wskazanie jakie prawa i wolności wskazane są w RODO jako istniejące*. Nie chcę w tym miejscy wdawać się w rozważania nad tym, czy owe prawa i wolności są w RODO ustanowione, czy RODO jedynie je opisuje. Faktem jest, że zapisane w RODO są, trzeba tylko umieć je znaleźć, odnaleźć klucz, z użyciem którego prawodawca je w RODO zakodował, po czym je po prostu odkodować. Wyżej, w opisie realizacji celu rozumianego jako prezentacja Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, wskazuję, z użyciem liczb, ile praw, wolności i obowiązków udało mi się zidentyfikować. By nie powtarzać wywodów – odsyłam tam.