OCHRONA DANYCH OSOBOWYCH

Poradnik praktyczny

redakcja Dominik Lubasz, Adam Szkurłat

Witold Chomiczewski, Aneta Frydrych-Romańska
Wojciech Grenda, Dominik Lubasz, Joanna Łuczak-Tarka
Kinga Maciaszczyk, Anna Majczak-Górecka, Karolina Przybysz
Adam Szkurłat, Julia Wawrzyńczak, Paulina Wirska

lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Wolters Kluwer

GDPR RISK TRACKER
by lubasz&wspólnicy

OCHRONA DANYCH OSOBOWYCH

Poradnik praktyczny

redakcja Dominik Lubasz, Adam Szkurłat

Witold Chomiczewski, Aneta Frydrych-Romańska
Wojciech Grenda, Dominik Lubasz, Joanna Łuczak-Tarka
Anna Maciaszczyk, Kinga Majczak-Górecka, Karolina Przybysz
Adam Szkurłat, Julia Wawrzyńczak, Paulina Wirska

Wolters Kluwer

WARSZAWA 2023

Stan prawny na 25 maja 2023 r.

Wydawczyni
Monika Pawłowska

Redaktor prowadząca
Katarzyna Gierłowska

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

ISBN 978-83-8328-713-3 *ISBN PDF-a: 978-83-8328-808-6*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

SŁOWO WSTĘPNE

W dniu 25.05.2023 r. minęło pięć lat od momentu, w którym rozpoczęliśmy stosowanie przepisów ogólnego rozporządzenia o ochronie danych. Choć sam akt prawny został uchwalony ponad dwa lata wcześniej, a europejski prawodawca przewidział stosownie długi okres na dostosowanie czynności przetwarzania do nowych przepisów, to wdrożenie regulacji rozporządzenia 2016/679 rodziło i rodzi nadal wiele wątpliwości i kontrowersji. Perspektywa pięciu lat stosowania nowych przepisów pozwala jednak bliżej przyjrzeć się wykładni, określić tendencje orzecznicze, zweryfikować skuteczność wytycznych oraz innych form *soft law* w obszarze ochrony danych osobowych, a także przeanalizować stosowane w tej dziedzinie praktyki. Zbliżający się w przyszłym roku komisyjny przegląd regulacji RODO determinuje także krytyczne spojrzenie na regulacje oraz próbę wskazania mankamentów, których usunięcie konieczne byłoby w przyszłości.

Warto podkreślić, że przepisy normujące zagadnienia ochrony danych osobowych to nie tylko RODO, ale również krajowe przepisy sektorowe czy unijne punktowe regulacje związane z różnymi aspektami przetwarzania danych osobowych. O ile rozporządzenie 2016/679 nie zmieniło się od momentu uchwalenia przepisów, o tyle w polskim porządku prawnym wprowadzono szereg nowych przepisów oddziałujących znacząco na zagadnienia związane z ochroną danych osób fizycznych. Nowe przepisy regulują praktyczne i kluczowe z perspektywy wielu administratorów kwestie, między innymi profilowanie, pracę zdalną czy badanie trzeźwości.

Wreszcie czynnikiem wpływającym na wzrost znaczenia zagadnień związanych z ochroną danych osobowych była pandemia COVID-19. Gwałtowna cyfryzacja, zamiana modelu pracy, w szczególności przejście do modelu pracy zdalnej, ujawniły, jak istotne są odpowiedni dobór narzędzi, zaadresowanie nowych wyzwań, zagrożeń i podatności oraz wdrożenie adekwatnych środków technicznych i organizacyjnych.

Wszystkie te aspekty zainspirowały zespół Autorów do opracowania niniejszej publikacji. W jej ramach podjęliśmy próbę zaprezentowania przepisów o ochronie danych osobowych z uwzględnieniem praktycznych aspektów ich stosowania. Publikacja została podzielona na dwie części – poświęconą zagadnieniom ogólnym oraz szczególnym problemom i obszarom przetwarzania danych osobowych. W każdej z części przybliżamy syntetycznie zapatrywania doktryny oraz poglądy prezentowane w orzecznictwie, wzbogacając je o liczne przykłady i podkreślając najistotniejsze wnioski.

Każdy z Autorów jest członkiem zespołu *Privacy & Data Protection* w kancelarii Lubasz i Wspólnicy, zaś sama publikacja stanowi efekt doświadczeń zgromadzonych przez Autorów, którzy na co dzień zajmują się praktycznym wdrażaniem przepisów o ochronie danych osobowych. Liczne wyróżnienia w branżowych rankingach, dorobek naukowy i publikacyjny oraz słowa uznania od Klientów pozwalają nam wierzyć, że wiedza, jaką dzielimy się w tej książce, będzie cenna i przydatna dla każdego z Czytelników.

Dominik Lubasz
Adam Szkurłat

Łódź, czerwiec 2023 r.

WYKAZ SKRÓTÓW

Akty prawne

EKPC	– Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2022 r. poz. 1360 ze zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2022 r. poz. 1138 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2022 r. poz. 1510 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775 ze zm.)
k.p.c.	– ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
KPP	– Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 7.06.2016 r., s. 391)
MPPOiP	– Międzynarodowy Pakt Praw Obywatelskich i Politycznych, otwarty do podpisu w Nowym Jorku 19.12.1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167)
p.p.s.a.	– ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2023 r. poz. 259 ze zm.)
pr. pras.	– ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 ze zm.)

RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1, ze zm.)
TUE	– Traktat o Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 7.06.2016 r., s. 13)
u.d.i.p.	– ustawa 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.s.o.z.	– ustawa z 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2022 r. poz. 1854)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.w.t.	– ustawa z 26.10.1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz.U. z 2023 r. poz. 165 ze zm.)

Periodyki, publikatory urzędowe, zbiory orzecznictwa

Dz.U.	– Dziennik Ustaw
Dz.Urz. UE/WE	– Dziennik Urzędowy Unii Europejskiej/Wspólnot Europejskich
MoP	– Monitor Prawniczy
M.P.	– Monitor Polski
OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
PiP	– Państwo i Prawo

Inne

CBOSA	– Centralna Baza Orzeczeń Sądów Administracyjnych, dostępna na stronie: https://orzeczenia.nsa.gov.pl
DPIA	– *data protection impact assessment* (ocena skutków dla ochrony danych)
ENISA	– Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EOG	– Europejski Obszar Gospodarczy

ePUAP	–	Elektroniczna Platforma Usług Administracji Publicznej
EROD	–	Europejska Rada Ochrony Danych
GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
IOD	–	inspektor ochrony danych
KE	–	Komisja Europejska
SA	–	Sąd Apelacyjny
SN	–	Sąd Najwyższy
SO	–	Sąd Okręgowy
TS	–	Trybunał Sprawiedliwości
UODO	–	Urząd Ochrony Danych Osobowych
UOKiK	–	Urząd Ochrony Konkurencji i Konsumentów

CZĘŚĆ OGÓLNA

Rozdział I

REGULACJE PRAWNE OCHRONY DANYCH OSOBOWYCH

1. Wprowadzenie

Z perspektywy osób zajmujących się ochroną danych osobowych, ale przede wszystkim z punktu widzenia administratorów, data 25.05.2018 r. jest kluczowa dla ustalenia, jakie przepisy, a w ślad za tym – jakie obowiązki i zadania, znajdą zastosowanie w istniejących i planowanych procesach przetwarzania danych osobowych. Z tym dniem rozpoczęto – po dwuletnim okresie przygotowawczym – stosowanie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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)[1]. Ogólna dyrektywa sformułowana w motywie 171 RODO przewiduje, że przetwarzanie, które w dniu wejścia w życie rozporządzenia, tj. dnia 24.05.2016 r., już się toczy, powinno w terminie dwóch lat od wejścia rozporządzenia w życie zostać dostosowane do jego przepisów.

[1] Dz.Urz. UE L 119, s. 1, ze zm.

2. Rola rozporządzenia 2016/679

Ogólne rozporządzenie o ochronie danych zastąpiło obowiązującą wcześniej dyrektywę 95/46/WE, a w konsekwencji również ustawę o ochronie danych osobowych z 1997 r., wprowadzając odmienny, proaktywny model ochrony, **oparty na podejściu bazującym na ryzyku** (*risk-based approach*). W ramach reformy prawa ochrony danych osobowych prawodawca odszedł od sztywnych ram regulacyjnych i precyzyjnego wskazania obowiązków, jakim powinien sprostać administrator. Były one charakterystyczne dla polskiej ustawy o ochronie danych osobowych z 1997 r. oraz rozporządzeń wykonawczych do niej, w tym zwłaszcza dla rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[2].

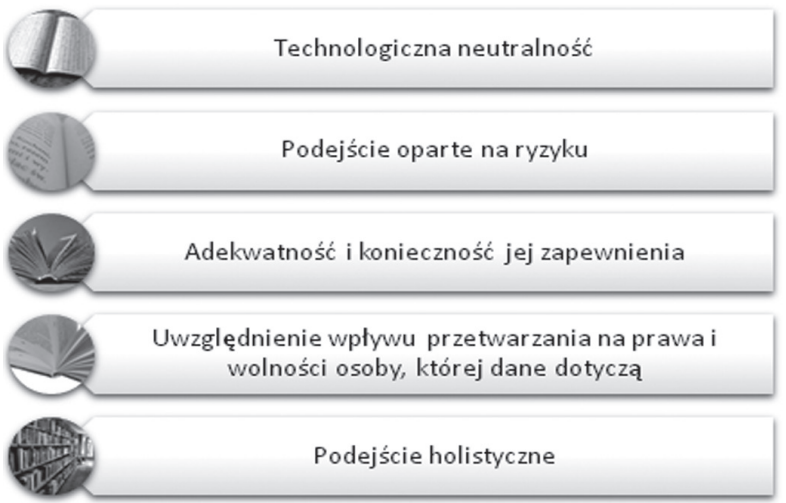
Podejście oparte na ryzyku jest kluczowe dla odczytania, zrozumienia i zrealizowania obowiązków administratora i podmiotu przetwarzającego nałożonych na nich mocą przepisów rozporządzenia 2016/679. Stało się ono istotnym elementem wielu obowiązków, w tym:

- ogólnego obowiązku zapewnienia zgodności z rozporządzeniem 2016/679, o którym mowa w jego art. 24;
- uwzględniania ochrony danych już w fazie projektowania (*data protection by design*) w myśl art. 25 ust. 1 oraz realizacji zasady domyślnej ochrony danych (*data protection by default*) zgodnie z art. 25 ust. 2;
- sporządzania określonej przepisami dokumentacji przetwarzania ujętej w ramy art. 30;
- zapewnienia bezpieczeństwa przetwarzania, w szczególności wskazanego w art. 32;
- oceny skutków przetwarzania dla ochrony danych (*data protection impact assessment*) oraz uprzednich konsultacji z organem nadzoru, o których mowa odpowiednio w art. 35 i 36.

[2] Dz.U. Nr 100, poz. 1024.

Jako podstawa przyjętej konstrukcji obowiązków wskazany mechanizm jest realizowany przez analizę ryzyka, dla której jednak brak szczegółowej regulacji w rozporządzeniu 2016/679. Decyzja w kwestii przyjmowanej metodyki, sposobu podejścia, użytych narzędzi analitycznych, jak również samego zakresu analizy została pozostawiona w rękach administratora.

Rysunek 1. Cechy regulacji zawartych w RODO



Źródło: opracowanie własne.

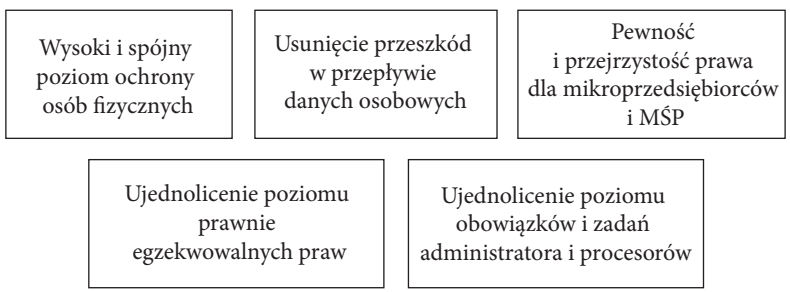
Opisane podejście jest związane ze zdiagnozowaną potrzebą unowocześnienia regulacji ochrony danych osobowych w Unii Europejskiej, zapewnienia jej neutralności technologicznej, zniwelowania negatywnych aspektów dotychczasowego wyboru środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, a wreszcie – z dostrzeżeniem wartości danych osobowych w gospodarce (*data driven economy*) i wpływu wykorzystania danych, w szczególności w ujęciu transgranicznym, na budowanie jednolitego rynku cyfrowego w Unii Europejskiej.

3. Cele reformy prawa ochrony danych osobowych

W związku z tym sformułowano **podstawowe cele**, jakie przyświecają omawianej reformie. Z jednej strony jest to **wysoki poziom ochrony praw osób fizycznych**, z drugiej jednak – poszerzenie możliwości biznesowych poprzez **ułatwienie swobodnego przepływu danych osobowych na jednolitym rynku cyfrowym**.

W założeniach nowa regulacja – między innymi poprzez technologiczną neutralność – pozostawia administratorom swobodę co do wyboru metod i środków, z wykorzystaniem których będą realizować cele i zadania związane z bezpieczeństwem informacji, co stało się ostatecznie jednym z najbardziej charakterystycznych elementów tej regulacji. Zmieniono w związku z tym stosowane rozwiązania tak, by uelastycznić podejście i zróżnicować nakładane obowiązki zależnie od warunków przetwarzania danych, podmiotów przetwarzających i skali. Miało to być także odpowiedzią na sytuację prawną oraz oczekiwania małych i średnich przedsiębiorców.

Rysunek 2. Podstawowe cele związane ze stosowaniem RODO



Źródło: opracowanie własne.

4. Zakres zastosowania RODO

Przepisy art. 2 i 3 RODO odpowiednio wyznaczają zakres przedmiotowy i zakres terytorialny zastosowania rozporządzenia.

W myśl art. 2 RODO obejmuje ono swoim zakresem zastosowania wszelkiego rodzaju przetwarzanie danych osobowych stanowiących lub mających stanowić część zbioru danych, przetwarzanych w sposób całkowicie lub tylko częściowo zautomatyzowany, a także w sposób ogóle niezautomatyzowany. W konsekwencji regulacja ta znajdzie zastosowanie do większości form przetwarzania. Równocześnie podlega ona jednak pewnym ograniczeniom poprzez sformułowane w art. 2 ust. 2 wyjątki.

Wyłączenia zastosowania rozporządzenia 2016/679 obejmują:
1) przetwarzanie w ramach działalności nieobjętej zakresem prawa Unii;
2) przetwarzanie przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;
3) przetwarzanie przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
4) przetwarzanie 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.

Zakres terytorialny zastosowania rozporządzenia 2016/679 wyznaczany jest z kolei, zgodnie z art. 3 RODO, przez związek przetwarzania danych osobowych z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii Europejskiej, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Dostrzegając słabości regulacji dyrektywy 95/46/WE, prawodawca unijny w art. 3 ust. 2 RODO rozszerzył zastosowanie rozporządzenia

również na podmioty niemające jednostek organizacyjnych w Unii, jednak przetwarzające dane osób przebywających w Unii, gdy to przetwarzanie wiąże się z:

- oferowaniem osobom przebywającym w Unii towarów lub usług (niezależnie od tego, czy wymagają one zapłaty);
- monitorowaniem zachowania osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii.

W konsekwencji rozporządzenie 2016/679 przewiduje zdecydowane rozszerzenie zakresu stosowania europejskich przepisów o ochronie danych zgodnie z koncepcją **nakierowania działalności na odbiorców w Unii Europejskiej**. Koncepcja ta wymaga, aby przy ocenie istnienia nakierowania uwzględniać takie czynniki, jak: posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii.

5. Relacja RODO do polskich regulacji

Jak już wskazano, z momentem rozpoczęcia stosowania przepisów RODO uchylone zostały dotychczasowe krajowe przepisy w obszarze ochrony danych osobowych. Trzeba przy tym podkreślić, że nieprzypadkowa jest zastosowana przez europejskiego prawodawcę forma regulacji w postaci rozporządzenia. Rozporządzenie jako akt prawa unijnego stosowane jest co do zasady bezpośrednio we wszystkich państwach członkowskich, bez konieczności jego implementacji czy sankcjonowania przepisami krajowymi. Europejski prawodawca pozostawił jednak państwom członkowskim pewną swobodę we wdrażaniu i uzupełnianiu przepisów rozporządzenia 2016/679 przez ustawodawstwo krajowe w zakresie wprost wskazanym w rozporządzeniu, tj. w przypadkach, do których rozporządzenie nie znajduje zastosowania (art. 2 ust. 2 RODO), oraz w przypadkach określonych w klauzulach kompetencyjnych, np. w art. 6 ust. 2, art. 9 ust. 4, art. 23, art. 43 i art. 84–91 RODO. Takie rozwiązane legislacyjne dopuszcza zachowanie lub wprowadzenie bardziej szczegółowych niż RODO przepisów w celu wypełnienia obowiązku prawnego, wykonania zadania reali-

zowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, w tym uregulowań sektorowych, dokładniej określających szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, oraz wprowadzanie dalszych warunków, w tym ograniczeń w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Dla zapewnienia stosowania rozporządzenia niezbędne było jednak uchwalenie krajowego aktu prawnego. Wynikało to z zasady autonomii proceduralnej państw członkowskich, w których wyłącznej kompetencji pozostaje ukształtowanie instytucjonalne oraz proceduralne krajowego systemu ochrony danych.

Ustawa z 10.05.2018 r. o ochronie danych osobowych[3] weszła w życie 25.05.2018 r., a więc w dniu rozpoczęcia stosowania przepisów ogólnego rozporządzenia o ochronie danych.

Zgodnie z art. 1 ust. 2 u.o.d.o. ustawa określa:

1) podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;
2) warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, zwanego dalej „podmiotem certyfikującym", podmiotu monitorującego kodeks postępowania oraz certyfikacji;
3) tryb zatwierdzenia kodeksu postępowania;
4) organ właściwy w sprawie ochrony danych osobowych;
5) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
6) tryb europejskiej współpracy administracyjnej;
7) kontrolę przestrzegania przepisów o ochronie danych osobowych;
8) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem;
9) odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

[3] Dz.U. z 2019 r. poz. 1781.

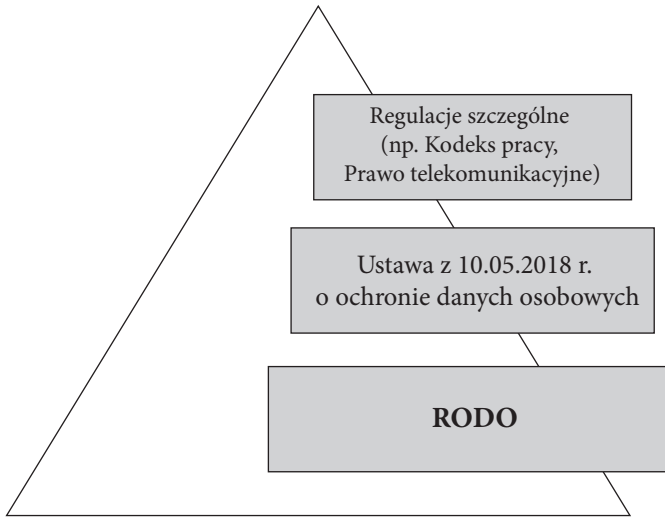
Ustawą o ochronie danych znowelizowano równocześnie niektóre przepisy szczegółowe, w tym przepisy Kodeksu pracy w zakresie dotyczącym przetwarzania danych kandydatów do pracy i pracowników, czy ustaw samorządowych dotyczące monitoringu.

Ważne:
Podkreślić należy, że ustawa o ochronie danych osobowych z 2018 r. – mimo zbieżności tytułów – nie jest znowelizowaną ustawą o ochronie danych osobowych z 1997 r. ani nie powiela zakresu RODO. Akt prawny z 2018 r. uchyla obowiązywanie ustawy z 29.08.1997 r. o ochronie danych osobowych.

Dopełnieniem systemu prawnego ochrony danych osobowych są sektorowe regulacje zawarte w wielu polskich ustawach, między innymi w Kodeksie pracy, ustawie z 18.07.2002 r. o świadczeniu usług drogą elektroniczną[4], ustawie z 16.07.2004 r. – Prawo telekomunikacyjne[5] czy innych szczegółowych przepisach wskazanych w ustawie z 21.02.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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)[6]. Ostatnia z przywołanych ustaw miała na celu dostosowanie rozwiązań przewidzianych w RODO do specyfiki krajowego systemu prawnego w części dotyczącej ochrony danych osobowych. Na jej podstawie dokonano nowelizacji 162 ustaw, a zmiany w niej zawarte przede wszystkim usuwały z porządku prawnego normy sprzeczne z RODO lub powielające rozwiązania przewidziane w tym unijnym akcie.

[4] Dz.U. z 2020 r. poz. 344.
[5] Dz.U. z 2022 r. poz. 1648 ze zm.
[6] Dz.U. poz. 730.

Rysunek 3. Relacja i struktura przepisów o ochronie danych osobowych w polskim porządku prawnym



Źródło: opracowanie własne.

Rozdział II

PODSTAWOWE POJĘCIA I ROLE W PROCESIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Wprowadzenie

Do prawidłowej interpretacji rozporządzenia 2016/679 konieczna jest znajomość wielu specyficznych pojęć związanych z ochroną danych osobowych. Pojęcia te zostały zdefiniowane w art. 4 RODO. Wśród kluczowych pojęć możemy wyróżnić pojęcia: danych osobowych, danych szczególnej kategorii, przetwarzania, administratora, podmiotu przetwarzającego, współadministratora, zgody oraz profilowania.

2. Dane osobowe

Jednym z centralnych pojęć używanych na gruncie RODO jest pojęcie danych osobowych. Dane osobowe zgodnie z art. 4 pkt 1 RODO to **wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** („osobie, której dane dotyczą"). Pojęcie to ma charakter otwarty. Mogą pojawiać się również nieznane dotychczas kategorie danych[1].

[1] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, komentarz do art. 4 RODO.

Aby dokonać omówienia tej definicji, warto podzielić ją na następujące elementy:
- „wszelkie informacje",
- „dotyczące",
- „zidentyfikowanej lub możliwej do zidentyfikowania",
- „osoby fizycznej"[2].

Pojęcie **wszelkich informacji** obejmuje wszelkie stwierdzenia na temat danej osoby, także subiektywne opinie i oceny, a nawet informacje nieprawdziwe lub niesprawdzone, niezależnie od formy ich przedstawienia (liczbowo, alfabetycznie, fotograficznie, akustycznie) i nośnika informacji (zapisane na papierze lub w pamięci komputera)[3].

Informacja musi **dotyczyć** określonej osoby, a więc musi być to informacja na temat tej osoby[4]. Związek z osobą może mieć charakter osobowy lub rzeczowy. Dane nie muszą dotyczyć bowiem ściśle określonej osoby, by uznać, że jej dotyczą. Wystarczy, że dane dotyczą przedmiotu, który należy do określonej osoby lub jest w bliskiej odległości geograficznej w stosunku do określonej osoby. Nie jest natomiast wystarczający związek wyłącznie statystyczny[5].

Wystąpienie związku można oceniać przez pryzmat **treści, celu lub skutku informacji**. Przy ustalaniu związku pomocne może być zadanie następujących pytań:
- Czy jest to informacja na temat określonej osoby (treść informacji)?
- Czy dane zostaną użyte w celu potraktowania osoby w określony sposób lub jej oceny (cel informacji)?
- Czy użycie danych będzie wpływać na prawa i interesy danej osoby (skutek informacji)?

[2] Grupa Robocza Art. 29, *Opinia 4/2007 w sprawie pojęcia danych osobowych z 20.06.2007 r.*, s. 6.

[3] Grupa Robocza Art. 29, *Opinia 4/2007*..., s. 6–7.

[4] Grupa Robocza Art. 29, *Opinia 4/2007*..., s. 9.

[5] D. Lubasz, *Informacje dotyczące osoby fizycznej* [w:] *RODO w e-commerce*, red. D. Lubasz, Warszawa 2018, s. 31.

Ważne:
Danymi osobowymi są również numery księgi wieczystej. Ujawnienie numeru księgi wieczystej pozwala bowiem pozyskać osobie zainteresowanej takie informacje, jak: numer PESEL, imię i nazwisko, imiona rodziców oraz adres nieruchomości[6].

Kolejnym elementem, który składa się na pojęcie danych osobowych, jest **fakt identyfikacji osoby fizycznej lub umożliwienie potencjalnej identyfikacji**. Osobę fizyczną uważa się za zidentyfikowaną, jeżeli można odróżnić ją od pozostałych członków grupy. Z kolei osoba możliwa do zidentyfikowania to osoba, wobec której nie dokonano jeszcze identyfikacji, ale jest to możliwe[7].

Do identyfikacji można posłużyć się różnymi informacjami, między innymi: imieniem i nazwiskiem, numerem identyfikacyjnym, danymi o lokalizacji lub identyfikatorem internetowym. Możliwe jest również dokonanie identyfikacji przy jednoczesnym wykorzystaniu kilku szczególnych czynników określających na przykład fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Połączenie kilku takich czynników może tworzyć unikalną kombinację, która będzie identyfikowała osobę fizyczną.

Identyfikacja może następować w sposób bezpośredni lub pośredni. Bezpośrednia identyfikacja najczęściej następuje poprzez nazwisko osoby fizycznej. W przypadku pospolitych imion i nazwisk konieczne może się okazać sięgnięcie do dodatkowych informacji, ponieważ samo imię i nazwisko nie będą wystarczające do jednoznacznej identyfikacji osoby fizycznej. Z kolei identyfikacja pośrednia dokonywana jest na przykład na podstawie: numeru dowodu osobistego przypisanego do danej osoby fizycznej, informacji o lokalizacji, opisu „obecny prezes zarządu spółki X", adresu IP, identyfikatora plików *cookies*.

[6] Decyzja Prezesa UODO z 24.08.2020 r., DKN.5112.13.2020, dostępna na stronie: https://uodo.gov.pl/decyzje/DKN.5112.13.2020 (dostęp: 27.04.2023 r.), utrzymana wyrokiem WSA w Warszawie z 5.05.2021 r., II SA/Wa 2222/20, LEX nr 3209059.

[7] Grupa Robocza Art. 29, *Opinia 4/2007*..., s. 12.

To, czy dana informacja pozwala na bezpośrednią, czy też na pośrednią identyfikację osoby fizycznej, zależy od okoliczności sprawy. Osoba fizyczna może zostać zidentyfikowana nawet na podstawie samego pospolitego nazwiska, gdy mamy do czynienia z niewielką grupą osób. Nie dla każdego ta sama informacja będzie stanowiła dane osobowe, ponieważ nie każdy będzie miał taką samą możliwość identyfikacji danej osoby fizycznej. Zgodnie z motywem 26 RODO w celu identyfikacji osoby bierzemy pod uwagę takie czynniki, jak **koszt identyfikacji, jej czas oraz dostępna technologia**. Jest to tak zwana relatywizacja pojęcia danych osobowych[8]. Innymi słowy, to, czy konkretna informacja stanowi dane osobowe, zależy od tego, jakimi innymi informacjami i możliwościami dysponuje osoba, która weszła w jej posiadanie. Fakt, że dodatkowe informacje, za pomocą których może nastąpić identyfikacja, znajdują się w posiadaniu osoby trzeciej nie wyklucza możliwości uznania ich za dane osobowe[9].

Przykład może stanowić adres IP, którego status jest dość niejednoznaczny. W świetle orzeczeń Trybunału Sprawiedliwości zarówno statyczny identyfikator IP[10], jak i IP dynamiczne[11] zostały uznane, w pewnych sytuacjach, za dane osobowe. W wyroku w sprawie C-70/10, Société belge des auteurs, compositeurs et éditeurs Trybunał Sprawiedliwości uznał, że adres IP to dane osobowe dla dostawcy usługi dostępu do internetu. Z kolei w sprawie C-582/14, Patrick Breyer, dotyczącej dynamicznego IP, przyjęto, że adres IP ma charakter danych osobowych dla podmiotów mających możliwość połą-

[8] D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych – o potrzebie zapewnienia spójności i roli soft law w kształtowaniu siatki pojęciowej na gruncie ogólnego rozporządzenia o ochronie danych* [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga, dodatek do MoP 2021/23, s. 1575.

[9] D. Lubasz, *Podstawowe pojęcia* [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022, s. 84.

[10] Wyrok TS z 24.11.2011 r. w sprawie C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771, pkt 51.

[11] Wyrok TS z 19.10.2016 r. w sprawie C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, pkt 44–48.

czenia go z dodatkowymi informacjami będącymi w posiadaniu na przykład dostawcy usługi dostępu do internetu.

Przykład:
Ciąg cyfr będący numerem klienta banku stanowi dane osobowe dla banku, ale nie dla postronnej osoby, która nie ma dostępu do wewnętrznego systemu danego banku i nie jest w stanie powiązać numeru klienta z konkretną osobą fizyczną.
Adres IP stanowi dane osobowe dla dostawcy usługi dostępu do internetu, ponieważ dostawca ma możliwość połączenia go z dodatkowymi informacjami będącymi w jego posiadaniu i dokonania w ten sposób pośredniej identyfikacji osoby fizycznej.

Co istotne, zidentyfikowanie osoby fizycznej, zwłaszcza w internecie, nie musi polegać na ustaleniu jej imienia i nazwiska. Do wywarcia określonego wpływu na osobę fizyczną wystarczające jest oznaczenie użytkownika na przykład za pomocą indywidualnego identyfikatora[12]. Zgodnie z motywem 30 RODO osobom fizycznym mogą zostać przypisane identyfikatory internetowe, takie jak adresy IP czy identyfikatory plików *cookies*. W konsekwencji ślady, które pozostawia w internecie użytkownik, w połączeniu z tymi unikatowymi identyfikatorami mogą być wykorzystywane do tworzenia profili i do identyfikowania osób. Choć w doktrynie postuluje się, by wszelka aktywność internetowa była traktowana jako dane osobowe[13], to przeważa stanowisko, że nie jest możliwe zakwalifikowanie określonych informacji jako danych osobowych w sposób automatyczny.

Ważne:
W orzecznictwie[14] wyrażany jest pogląd, że numery telefonów nie stanowią danych osobowych, ponieważ bez dodatkowych informacji nie pozwalają one na identyfikację abonentów przypisanych do tych numerów.

[12] D. Lubasz, *Podstawowe pojęcia* [w:] *Meritum. Ochrona danych...*, red. D. Lubasz, s. 83.

[13] A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Warszawa 2019, s. 142.

[14] Zob.: wyrok WSA w Warszawie z 13.04.2021 r., II SA/Wa 1898/20, LEX nr 3185223; wyrok WSA w Warszawie z 25.11.2022 r., II SA/Wa 710/22, CBOSA.

Ważne:
Naczelny Sąd Administracyjny w jednym z rozstrzygnięć zaprezentował również pogląd, że numer rejestracyjny pojazdu nie stanowi danych osobowych, ponieważ identyfikuje pojazd, a nie osobę[15]. Zidentyfikowanie posiadacza pojazdu może być dokonane tylko poprzez dostęp do odpowiednich rejestrów lub katalogów.

Warto zaznaczyć, że powyższa linia orzecznicza Naczelnego Sądu Administracyjnego jest sprzeczna z poglądami organów ochrony danych osobowych innych państw członkowskich, w tym z poglądem wyrażonym przez Prezesa Urzędu Ochrony Danych Osobowych przy okazji prac nad projektem ustawy o zmianie ustawy o autostradach płatnych oraz Krajowym Funduszu Drogowym oraz niektórych innych ustaw[16].

Informacje anonimowe nie stanowią danych osobowych, nie jest bowiem możliwe powiązanie ich z konkretną osobą. Podkreślić należy w tym miejscu różnicę pomiędzy informacjami zanonimizowanymi a **informacjami spseudonimizowanymi**. W przypadku danych anonimowych, w przeciwieństwie do danych spseudonimizowanych, nie jest możliwe ponowne przypisanie ich do konkretnej osoby fizycznej. Natomiast pseudominizacja jest jedną z metod zabezpieczania danych osobowych i nie pozbawia informacji cech danych osobowych[17].

Pojęcie danych osobowych ogranicza się do informacji o **osobach fizycznych**[18]. W świetle polskiego prawa osobą fizyczną jest człowiek od chwili narodzin do chwili śmierci. Nie ma przy tym znaczenia

[15] Zob.: wyrok NSA z 3.11.2022 r., III OSK 1522/21, LEX nr 3429658; wyrok NSA z 14.05.2021 r., III OSK 1466/21, LEX nr 3180401; wyrok NSA z 28.06.2019 r., I OSK 2063/17, LEX nr 2715871.

[16] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020, Druk sejmowy nr 1529, Sejm RP IX kadencji, s. 126, źródło: https://orka.sejm.gov.pl/Druki9ka.nsf/0/BCE8181D03D3DE83C1258748003131A0/%24File/1529.pdf (dostęp: 24.02.2023 r.).

[17] D. Lubasz, *Podstawowe pojęcia* [w:] *Meritum. Ochrona danych...*, red. D. Lubasz, s. 84.

[18] Grupa Robocza Art. 29, *Opinia 4/2007...*, s. 24.

czy osoba fizyczna posiada zdolność do czynności prawnych[19], jakie posiada obywatelstwo, miejsca zamieszkania ani prowadzona aktywność zawodowa[20]. Poza zakresem RODO znajduje się natomiast przetwarzanie danych dotyczących osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej oraz osób zmarłych.

3. Dane szczególnych kategorii

Wyróżnia się dwie zasadnicze kategorie danych osobowych, tj. dane zwykłe i dane szczególnych kategorii, potocznie określane jako dane wrażliwe. Zgodnie z art. 9 ust. 1 RODO jako dane szczególnych kategorii kwalifikowane są:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Katalog ten ma charakter zamknięty.

Wśród danych wrażliwych ważną kategorię stanowią dane biometryczne, które wymagają specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej i umożliwiają jej jednoznaczną identyfikację lub potwierdzenie jej tożsamości. Do takich danych zaliczane są między innymi: odciski linii papilarnych na palcach, kod DNA, skan siatkówki oka, głos.

Dane wrażliwe podlegają szczególnym, bardziej restrykcyjnym zasadom przetwarzania. Na gruncie RODO ustanowiony został ogólny

[19] P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 4 RODO.

[20] D. Lubasz, *Podstawowe pojęcia* [w:] *Meritum. Ochrona danych...*, red. D. Lubasz, s. 80–81.

zakaz przetwarzania danych wrażliwych, który może być uchylony jedynie przez określone w art. 9 ust. 2 RODO okoliczności legalizujące.

Ważne:
Zgodnie z orzecznictwem Trybunału Sprawiedliwości[21] pojęcia „szczególnych kategorii danych osobowych" i „danych wrażliwych" należy interpretować szeroko. Celem RODO jest bowiem zagwarantowanie wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych, a zwłaszcza ich życia prywatnego, w zakresie przetwarzania danych osobowych, które ich dotyczą. Przetwarzanie „zwykłych" kategorii danych osobowych, które w sposób pośredni mogą ujawnić informacje o danych wrażliwych osoby fizycznej, stanowi przetwarzanie dotyczące szczególnych kategorii danych.

4. Przetwarzanie

Artykuł 4 pkt 2 RODO stanowi, że przetwarzanie oznacza **operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych**, 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.

[21] Zob. wyrok TS z 1.08.2022 r. w sprawie C-184/20, OT v. Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601, pkt 125.

Wskazany katalog operacji przetwarzania ma charakter przykładowy. Operacjami przetwarzania danych niewymienionymi wprost w wyliczeniu są na przykład profilowanie i pseudonimizacja[22]. Warto zwrócić uwagę na to, że odzwierciedla on zarazem cały cykl życia danych osobowych, począwszy od ich zebrania, a skończywszy na ich usunięciu[23]. Operacje te mogą być wykonywane w sposób zautomatyzowany lub niezautomatyzowany. Z operacjami zautomatyzowanymi mamy do czynienia między innymi w przypadku baz danych prowadzonych w systemach komputerowych umożliwiających na przykład sortowanie treści, które w znacznym stopniu ograniczają udział człowieka[24]. Z kolei sposób niezautomatyzowany opiera się na przetwarzaniu danych osobowych bez użycia urządzeń i programów automatyzujących, w tym w sposób ręczny. W obu przypadkach decyzja o zainicjowaniu operacji na danych osobowych należy do człowieka. Nie ma przy tym znaczenia fakt, czy osoba miała świadomość i wolę przetwarzania danych osobowych[25].

Przykład:

- Zbieranie – formularze reklamacyjne wypełniane elektronicznie, rejestracja na stronie internetowej, składanie zamówienia na stronie internetowej, wypełnianie ankiet, zbieranie CV podczas rekrutacji.
- Utrwalanie – zarejestrowanie rozmowy telefonicznej klienta dzwoniącego na infolinię, rejestrowanie obrazu wideo z wizerunkiem osoby fizycznej.
- Organizowanie lub porządkowanie – układanie w sposób alfabetyczny listy klientów, kategoryzowanie danych osobowych klientów.
- Przechowywanie – zapisywanie listy klientów na nośniku danych, w chmurze, przechowywanie papierowych akt osobowych pracowników.
- Adaptowanie lub modyfikowanie – aktualizacja adresu e-mail klienta, poprawianie błędnych danych klienta.

[22] P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 4 RODO.

[23] D. Lubasz, K. Witkowska-Nowakowska, *Przetwarzanie* [w:] *RODO dla małych i średnich przedsiębiorstw*, red. D. Lubasz, Warszawa 2018, s. 26.

[24] P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 4 RODO.

[25] D. Lubasz, K. Witkowska-Nowakowska, *Przetwarzanie...*, s. 26.

- Pobieranie lub przeglądanie – analiza bazy klientów, przyglądanie karty medycznej pacjenta, przeglądanie akt osobowych pracownika.
- Wykorzystywanie – użycie bazy klientów do przeprowadzenia kampanii marketingowych i analizy rynku, przeprowadzenie procesu rekrutacji na podstawie przesłanych CV, przetwarzanie danych osobowych w celu identyfikacji zagrożeń o charakterze terrorystycznym.
- Ujawnianie – przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie – publikowanie zdjęć oraz imion i nazwisk pracowników na stronach internetowych, przesyłanie baz danych przez brokerów swoim kontrahentom.
- Dopasowywanie lub łączenie – tworzenie profili behawioralnych użytkowników stron internetowych.
- Ograniczanie, usuwanie lub niszczenie – usunięcie danych klienta z bazy danych osób zapisanych do newslettera, usunięcie danych osobowych na skutek decyzji organu nadzorczego.

5. Profilowanie „zwykłe" i profilowanie kwalifikowane

Definicja profilowania zwykłego sformułowana została w art. 4 pkt 4 RODO. Zgodnie z nią 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. Funkcją profilowania w tym znaczeniu jest identyfikacja, ocena zachowania i cech określonej osoby oraz przewidywanie jej zachowań[26].

Przykład:
Profilowaniem nie jest klasyfikacja osób fizycznych przez przedsiębiorcę ze względu na płeć, w przypadku gdy przedsiębiorstwo chce w ten sposób

[26] A. Mednis, *Prawo...*, s. 29.

dowiedzieć się, jaki jest statystyczny udział mężczyzn i kobiet wśród klientów. Celem tego działania nie jest bowiem ocena cech określonej osoby fizycznej[27].

Dokonując analizy art. 4 pkt 4 RODO, trzeba wyróżnić trzy przesłanki profilowania zwykłego:
- dotyczy danych osobowych;
- stanowi dowolną formę zautomatyzowanego przetwarzania;
- na jego podstawie powinna być dokonywana ocena czynników osobowych osoby fizycznej[28].

Profilowanie może przybrać postać niezautomatyzowaną, częściowo zautomatyzowaną oraz całkowicie zautomatyzowaną[29]. Niezautomatyzowane profilowanie oparte jest na ludzkim działaniu[30] i nie będzie wchodzić w zakres definicji art. 4 pkt 4 RODO[31]. Z kolei profilowanie częściowo zautomatyzowane pozbawione zostaje czynnika ludzkiego głównie w obszarze analiz danych[32]. Treść art. 4 pkt 4 RODO wskazuje na dowolną formę zautomatyzowanego przetwarzania, co potwierdza, że profilowanie zautomatyzowane może łączyć się z pewnymi formami ludzkiej interwencji[33]. Ostatnia, całkowicie zautomatyzowana

[27] Grupa Robocza Art. 29, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679*, 2018, s. 7.

[28] M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019, s. 83.

[29] Por. J. Niklas, *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji*, Polskie Towarzystwo Prawa Antydyskryminacyjnego, 2015, s. 3, pozyskano ze strony: http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf (dostęp: 26.02.2023 r.).

[30] Por. B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 RODO* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 88–89.

[31] M. Kibil [w:] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Warszawa 2018, s. 248.

[32] J. Niklas, *Profilowanie...*, s. 3.

[33] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 RODO* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 200–203.

forma profilowania oparta jest wyłącznie na algorytmach, które nie tylko dokonują analizy danych, ale też wyciągają z nich odpowiednie wnioski, kategoryzują je i wykorzystują do określonego celu[34]. Profilowaniem w tym znaczeniu nie będzie zatem proces, w którym człowiek będzie miał możliwość nadzoru nad wynikiem profilowania[35], na przykład przez konieczność weryfikacji zaproponowanej przez algorytm rekomendacji co do sposobu rozpatrzenia wniosku kredytowego klienta. Profilowanie całkowicie zautomatyzowane opisane zostało w art. 22 RODO.

W przypadku ostatniej przesłanki profilowania zwykłego, jaką jest ocena czynników osobowych osoby fizycznej, należy podkreślić, że zawarte w art. 22 RODO wyliczenie czynników nie jest wyczerpujące[36]. Dokonanie takiej oceny ma na celu ułatwienie zakwalifikowania danej osoby do jakiejś kategorii[37]. Uważa się jednak, że prosta kategoryzacja danych bez wnioskowania o nowych informacjach nie będzie profilowaniem w rozumieniu RODO[38].

Niekiedy profilowanie jest wykorzystywane do podejmowania decyzji wobec danej osoby, co uregulowane zostało w art. 22 RODO[39]. Podleganie takiemu profilowaniu szczególnemu podlega restrykcyjnym ograniczeniom. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Podmiot danych ma prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestiono-

[34] J. Niklas, *Profilowanie...*, s. 3.

[35] M. Gumularz, P. Kozik, *Ochrona...*, s. 87.

[36] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 RODO...*, s. 200–203.

[37] M. Kibil [w:] *RODO. Przewodnik...*, red. M. Gawroński, s. 250.

[38] M. Gumularz, P. Kozik, *Ochrona...*, s. 88.

[39] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 RODO* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2017, s. 129–132.

wania tej decyzji. Innymi słowy, jeżeli wynikiem zautomatyzowanego przetwarzania jest określona decyzja wobec osoby fizycznej, osoba ta ma swoiste prawo „odwołania się" od tej decyzji do człowieka. Ma to minimalizować ryzyko niebezpieczeństwa dla praw jednostki wynikające z rozwoju nowych technologii[40]. Obok profilowania szczególnego w art. 22 RODO wymieniono też zautomatyzowane podejmowanie decyzji, które jest kategorią szerszą od profilowania i niekoniecznie musi być z nim związane. Mogą bowiem zaistnieć sytuacje, gdy podjęcie decyzji nastąpi bez dokonywania oceny czynników osobowych danej osoby fizycznej. Niekiedy, wraz ze zmianą sposobu wykorzystania danych, działanie oparte jedynie na procesie zautomatyzowanego podejmowania decyzji może przekształcić się w działanie oparte na profilowaniu[41].

Przykład:
Zautomatyzowane nakładanie mandatów na podstawie dowodów z fotoradarów nie musi opierać się na profilowaniu. Jeśli natomiast wysokość mandatu będzie uzależniona od ilości wcześniejszych naruszeń zasad ruchu drogowego przez konkretnego kierowcę, to będziemy mieli do czynienia z profilowaniem.

Aby można było mówić o profilowaniu kwalifikowanym, konieczne jest również spełnienie następujących warunków (alternatywnie): wywarcie skutków prawnych w stosunku do osoby objętej decyzją lub też wywarcie na nią podobnego istotnego wpływu. Obie te przesłanki zostały szczegółowo wyjaśnione przez Grupę Roboczą Art. 29 ds. Ochrony Danych w wytycznych dotyczących zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679.

[40] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 22 RODO* [w:] *Rozporządzenie...*, red. P. Litwiński, s. 423–424.

[41] Grupa Robocza Art. 29, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679*, 2018, s. 8–9.

Profilowanie kwalifikowane w rozumieniu art. 22 RODO jest co do zasady dopuszczalne w przypadku wystąpienia jednej z trzech sytuacji:

1) jeżeli decyzja jest niezbędna do zawarcia lub wykonania umowy,
2) jeżeli decyzja jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, lub
3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Wyjątek stanowią dane szczególnie wrażliwe, określone w art. 9 ust. 1 RODO, które zgodnie z art. 22 ust. 4 RODO mogą być użyte do profilowania tylko w przypadku wystąpienia przesłanki zgody lub gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym.

6. Zgoda

Zgoda jest jedną z podstaw przetwarzania danych osobowych wymienionych w art. 6 RODO. Artykuł 4 pkt 11 RODO stanowi, że 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**. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (art. 7 ust. 1 RODO). Zgoda taka powinna spełniać warunki określone w art. 4 pkt 11 i art. 7 RODO, a więc powinna być dobrowolna, konkretna, świadoma, jednoznaczna i wyrażona przez oświadczenie lub wyraźne potwierdzenie działania.

Szczegółowe informacje dotyczące zgody znajdują się w dalszej części opracowania – w rozdziale IV, dotyczącym podstaw prawnych przetwarzania.

7. Administrator

Pojęcia administratora, współadministratora oraz podmiotu przetwarzającego określają rolę podmiotów z uwagi na pełnione przez nie funkcje. Status podmiotu jako administratora lub podmiotu przetwarzającego nie będzie zależeć od formalnego wyznaczenia ich na przykład w umowie, ale od analizy elementów stanu faktycznego lub okoliczności sprawy[42].

> **Ważne:**
> Administratorem nie jest konkretna osoba sprawująca kierownicze stanowisko czy pracownik, któremu powierzono zadania związane z przetwarzaniem danych. Funkcji administratora nie można na te osoby scedować.

Zgodnie z art. 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**. Innymi słowy, administrator decyduje o tym, dlaczego i jak należy przetwarzać dane. Właśnie ten element odróżnia administratora od podmiotu przetwarzającego.

W celu omówienia definicji administratora należy wyróżnić następujące elementy tej definicji:
- „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot",
- „ustala",
- „samodzielnie lub wspólnie z innymi",
- „cele i sposoby",
- „przetwarzania danych osobowych"[43].

Przechodząc do omówienia poszczególnych składowych definicji administratora, należy zauważyć, że sformułowanie **„osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot"** oznacza,

[42] Europejska Rada Ochrony Danych, *Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO*, 2021, s. 10.

[43] Europejska Rada Ochrony Danych, *Wytyczne 07/2020...*, s. 10.

że w zasadzie administratorem może być każdy. W praktyce stosunkowo rzadko administratorem danych są konkretne osoby fizyczne. Nawet jeśli organizacja wyznacza konkretną osobę fizyczną, która odpowiada za zapewnienie zgodności z RODO, a nawet decyduje o celach przetwarzania danych osobowych pod kontrolą organizacji, nie prowadzi to do uzyskania przez tę osobę przymiotu administratora danych – w dalszym ciągu jest nim sama organizacja, w imieniu której działa wyznaczona osoba fizyczna[44].

Słowo **„ustala"** oznacza, że administrator decyduje o kluczowych elementach przetwarzania. Administrowanie zwykle wynika z przepisów prawnych lub faktycznego pełnienia roli decyzyjnej.

Przykład:

- Przepisy nakładają na lokalne władze obowiązek zapewniania obywatelom świadczeń socjalnych w zależności od sytuacji finansowej oraz określają, że administratorem danych związanych z wykonaniem powyższego obowiązku są lokalne władze.
- Przedsiębiorstwo zajmuje się wysyłką newsletterów na zlecenie i zgodnie z instrukcjami podmiotu prowadzącego sklep internetowy. W umowie strony określiły, że administratorem danych jest przedsiębiorstwo zajmujące się wysyłką newsletterów. Mimo takich ustaleń umownych administratorem danych zawartych w bazie klientów jest podmiot prowadzący sklep internetowy.

Ustalanie celów i sposobów następuje **„samodzielnie lub wspólnie z innymi podmiotami"**, które określa się mianem „współadministratorów". Szerzej na temat współadministrowania w rozdziale XII.

Administrator jest podmiotem, który określa, **dlaczego odbywa się przetwarzanie** (tj. „w jakim celu", „po co") i **jak ten cel zostanie osiągnięty** (tj. jakie środki zostaną zastosowane, aby osiągnąć ten cel)[45]. Niekiedy wybór sposobów przetwarzania będzie dokonywany nie tylko przez administratora, ale także przed podmioty przetwarzające.

[44] Europejska Rada Ochrony Danych, *Wytyczne 07/2020...*, s. 11.

[45] Europejska Rada Ochrony Danych, *Wytyczne 07/2020...*, s. 15.

Dla administratora zostały zastrzeżone takie decyzje, jak:
- wybór danych, jakie będą przetwarzane;
- czas trwania przetwarzania;
- kategorie odbiorców danych;
- ustalenie, czyje dane osobowe będą przetwarzane.

Z kolei podmiot przetwarzający zwykle dokonuje mniej istotnych wyborów dotyczących sposobów przetwarzania, w tym między innymi wyboru sprzętu lub oprogramowania oraz wyboru odpowiednich środków bezpieczeństwa[46].

Przesłanka przetwarzania danych osobowych została wyjaśniona w punktach 1 i 3 tego rozdziału.

8. Podmiot przetwarzający

Zgodnie z art. 4 pkt 8 RODO podmiot przetwarzający (nazywany także procesorem) oznacza **osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora**.

Warunkiem zakwalifikowania podmiotu jako podmiotu przetwarzającego jest:
- pełnienie roli **odrębnego podmiotu w stosunku do administratora**,
- przetwarzanie danych osobowych **w imieniu administratora**.

Warunek odrębności nie zostanie spełniony w przypadku powierzenia przetwarzania wyodrębnionemu działowi w ramach tej samej organizacji. Warunek ten jest natomiast spełniony w przypadku powierzenia przetwarzania odrębnemu podmiotowi w ramach grupy kapitałowej.

[46] Europejska Rada Ochrony Danych, *Wytyczne 07/2020...*, s. 16.

Działanie w imieniu administratora polega na tym, że administrator nie sprawuje nad podmiotem przetwarzającym organizacyjnej kontroli, ale określa granice, w jakich podmiot przetwarzający może przetwarzać dane osobowe, tj. jakie dane i w jakim celu będą przetwarzane oraz jakie operacje będą mogły być dokonywane przez podmiot przetwarzający na danych osobowych[47]. Podmiot przetwarzający nie może działać wbrew instrukcjom administratora i nie może przetwarzać danych do własnych celów. W takiej sytuacji zostanie on bowiem samoistnym administratorem danych.

Ważne:
W proces przetwarzania danych może być zaangażowanych wiele podmiotów przetwarzających.

Przykład:
- Podmiot dostarczający rozwiązania IT lub usługi przechowywania danych w chmurze zwykle będzie dla swoich klientów podmiotem przetwarzającym. Z kolei klient takiego podmiotu będzie administratorem.
- Spółka X korzysta z usług księgowych spółki Y w celu wypłaty pracownikom wynagrodzeń. Spółka X przekazuje spółce Y wszelkie niezbędne informacje dotyczące wynagrodzeń. Spółka X jest w tym przypadku administratorem, a spółka Y podmiotem przetwarzającym.

Więcej informacji na temat powierzenia przetwarzania danych osobowych w rozdziale XI publikacji.

[47] D. Lubasz, K. Witkowska-Nowakowska, *Administrator i podmiot przetwarzający* [w:] *RODO dla małych i średnich przedsiębiorstw*, red. D. Lubasz, Warszawa 2018, s. 27.