Poradnik dla radców prawnych i adwokatów

Ogólne rozporządzenie o ochronie danych (RODO)

KRAJOWA IZBA
RADCÓW PRAWNYCH

Przygotowane przez:

TRAPLE
KONARSKI
PODRECKI
I WSPÓLNICY

ZESPÓŁ AUTORÓW PORADNIKA:

adw. Xawery Konarski

adw. dr Grzegorz Sibiga

r.pr. Dominika Nowak

adw. Katarzyna Syska

Iga Małobęcka

STAN PRAWNY NA DZIEŃ 20.04.2018

Spis treści

Wykaz skrótów

GIODO – Generalny Inspektor Ochrony Danych Osobowych

IOD – inspektor ochrony danych

KC – Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2017 r. poz. 459 ze zm.)

KERP – Kodeks Etyki Radcy Prawnego

KP – Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r. poz. 108 ze zm.)

KPA – Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r. poz. 1257 ze zm.)

KPC – Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2018 r. poz. 155 ze zm.)

KPK - Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2017 r. poz. 1904 ze zm.)

PPSA – Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2017 r. poz. 1369 ze zm.)

PrUODO – Projekt ustawy o ochronie danych osobowych z dnia 05 kwietnia 2018 r.

PUODO – Prezes Urzędu Ochrony Danych Osobowych

PWUODO – Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r.

RODO – Rozporządzenie 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) (Dz. Urz. UE L z 2016 r. nr 119, s. 1)

UPoA – Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (t.j. Dz. U. z 2017 r. poz. 2368 ze zm.)

URP – Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2017 r. poz. 1870 ze zm.)

UŚPZPP – Ustawa z dnia 5 lipca 2002 r. o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej (t.j. Dz. U. z 2016 r. poz. 1874)

ZZEAiGZ – Zbiór Zasad Etyki Adwokackiej i Godności Zawodu

Szanowni Państwo,

przekazujemy Państwu poradnik dotyczący stosowania ogólnego rozporządzenia o ochronie danych (RODO) w kancelarii radcy prawnego i w kancelarii adwokackiej. W publikacji przedstawiono podstawowe informacje na temat zakresu stosowania RODO w odniesieniu do działalności zawodowej radcy prawnego lub adwokata. Zaprezentowane w niej zostały także zasady przetwarzania danych osobowych oraz związane z tym obowiązki określone w RODO. W przypadku każdego z omawianych obowiązków wskazana została jego istota, odniesienie do działalności radcy prawnego lub adwokata, a następnie sposób wykonania. Załącznikami do publikacji są wzory podstawowych dokumentów wykonujących obowiązki do zastosowania w kancelarii radcy prawnego lub adwokata. Odrębną część publikacji stanowią informacje na temat mechanizmów zapewniania zgodności z RODO oraz zasad odpowiedzialności za naruszenie przepisów o ochronie danych osobowych.

Mamy nadzieję, że niniejsza publikacja okaże się Państwu przydatna w wykonywaniu czynności zawodowych, w tym we wdrażaniu ogólnego rozporządzenia o ochronie danych w Państwa kancelarii.

Zespół autorów

Traple, Konarski, Podrecki i Wspólnicy sp.j.

1. Reforma ochrony danych osobowych w Unii Europejskiej i w Polsce – geneza, cele i podstawowe założenia

Zainicjowana wnioskiem Komisji Europejskiej z dnia 25 stycznia 2012 r. reforma ochrony danych osobowych w Unii Europejskiej całkowicie zmienia stan prawny w tym obszarze zarówno w Unii Europejskiej, jak i w każdym państwie członkowskim. Z dniem 25 maja 2018 r. dotychczasowe regulacje, w tym przede wszystkim ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wykonująca dyrektywę 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, zostaną zastąpione zupełnie nowym systemem prawnym, opierającym się na ściślejszej harmonizacji ochrony danych osobowych w Unii Europejskiej.

Komisja Europejska wskazała dwa główne cele reformy. Pierwszy to zapewnienie większej stabilności i pewności prawa o ochronie danych osobowych i jego stosowania. Ma to szczególne znaczenie dla przedsiębiorców prowadzących działalność na unijnym rynku wewnętrznym, gdyż przekłada się na zwiększenie ich konkurencyjności w globalnej gospodarce. Stworzony zostaje stan pewności prawa opartego na jednym akcie w miejsce mozaiki 27 krajowych regulacji prawnych. W założeniu ma nastąpić także uproszczenie środowiska regulacyjnego (spójne działanie organów ochrony danych osobowych) i przyjęcie jasnych reguł w międzynarodowym transferze danych. Drugim celem reformy jest zagwarantowanie wysokiego poziomu ochrony praw jednostek (osób, których dane dotyczą). Ten poziom praw osoby fizycznej ma zapewnić przede wszystkim rozszerzenie praw informacyjnych jednostek oraz uprawnień gwarantujących im większą kontrolę nad przetwarzaniem ich własnych danych osobowych.

Na pakiet normatywny reformujący ochronę danych osobowych w Unii Europejskiej składają się dwa akty prawne:

1) rozporządzenie 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) oraz
2) dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (państwa członkowskie mają przyjąć i opublikować przepisy wykonujące dyrektywę do dnia 6 maja 2018 r., czyli wcześniej niż zaczyna obowiązywać RODO).

Rozporządzenie Parlamentu Europejskiego i Rady ma zasięg ogólny, wiąże w całości co do wszystkich zawartych w nim postanowień i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Ze swej natury staje się ono częścią krajowych systemów prawnych bez potrzeby dokonywania jakichkolwiek czynności transpozycyjnych i wywiera skutki bezpośrednie w stosunku do jednostek. Rozporządzenia obejmują wertykalny i horyzontalny skutek bez wyjątku. Oprócz obszaru objętego dyrektywą nr 2016/680 zniknie więc potrzeba tworzenia ustaw krajowych w zakresie stosowania

RODO, a wręcz pojawi się zakaz stosowania krajowych rozwiązań nieprzewidzianych w rozporządzeniu i niepozostawionych wyraźnie do uregulowania w prawie krajowym.

Równocześnie jednak rozporządzenie w pewnym zakresie przewiduje uzupełnienie własnych regulacji przepisami krajowymi. Zawarte w nim odesłania do prawa krajowego mają na celu przede wszystkim doprecyzowanie lub ograniczenie stosowania w tymże prawie krajowym przepisów RODO. Te ostatnie określają obligatoryjny oraz fakultatywny dla prawodawcy krajowego zakres regulacji prawnej, która uzupełnia RODO w wewnętrznym porządku krajowym. Do grupy obligatoryjnie ustanawianych przepisów krajowych zalicza się przepisy dotyczące przede wszystkim: organów nadzorczych (tj. niezależnych organów ds. ochrony danych osobowych), środków ochrony prawnej, odpowiedzialności i sankcji, a w szczególności zagadnień proceduralnych, oraz przepisy odnoszące się do certyfikacji i akredytacji w zakresie ochrony danych osobowych.

W Polsce w dniu oddania niniejszej publikacji (09 kwiecień 2018 r.) na etapie prac legislacyjnych znajdują się dwa projekty, które stanowią uzupełnienie przepisów RODO:

1) projekt ustawy o ochronie danych osobowych,
2) projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r. (poprzednia nazwa projektu: ustawa – Przepisy wprowadzające ustawę o ochronie danych osobowych).

W pierwszym z projektów znajdują się przede wszystkim przepisy wymagane przez RODO (odesłania obligatoryjne). W drugiej z przygotowywanych ustaw, nowelizującej ponad 130 kolejnych ustaw, zawarte są głównie przepisy, których przyjęcie RODO przewiduje fakultatywnie. W projekcie ustawy o zmianie niektórych innych ustaw przewiduje się m.in. nowelizację Ustawy z dnia 6 lipca 1982 r. o radcach prawnych oraz Ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze.

2. Zakres stosowania RODO i jego odniesienia do działalności zawodowej radcy prawnego lub adwokata

2.1 Pojęcie danych osobowych

Omówienie definicji

Pojęcie danych osobowych ma kluczowe znaczenie w prawie ochrony danych osobowych. Termin „dane osobowe" zdefiniowano w art. 4 pkt 1 RODO w następujący sposób: *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*.

Zakres pojęcia danych osobowych jest bardzo szeroki. Celem takiego ujęcia tego terminu jest zapewnienie osobom fizycznym jak najpełniejszej ochrony w związku z przetwarzaniem ich danych osobowych.

Można wyróżnić cztery elementy powyższej definicji:

- informacje;
- dotyczące;
- zidentyfikowanej lub możliwej do zidentyfikowania;
- osoby fizycznej.

Przez „informacje" rozumieć należy wszelkie stwierdzenia na temat osoby. Treść informacji może dotyczyć życia prywatnego *sensu stricto* danej osoby, a także wszelkich innych okoliczności, takich jak działalność zawodowa, zachowania ekonomiczne lub społeczne konkretnej osoby. Chodzi tu zarówno o informacje obiektywne (np. wiek, wzrost), jak i o informacje subiektywne (np. opinie na temat osoby fizycznej). Nie ma przy tym znaczenia, czy informacje te są prawdziwe. Informacje mogą być dostępne w jakiejkolwiek formie, w tym pisemnej (alfabetycznej, liczbowej), graficznej lub akustycznej.

Odnosząc się do określenia „dotyczące", należy przyjąć, że konkretna informacja dotyczy danej osoby, jeżeli jest to informacja na temat tej osoby. Informacja może dotyczyć osoby fizycznej w szczególności ze względu na swoją treść, ale także ze względu na swój cel lub swój skutek.

Kryterium „zidentyfikowana lub możliwa do zidentyfikowania" dotyczy możliwości odróżnienia konkretnej osoby od innych osób w danej grupie. Osoba fizyczna jest zidentyfikowana, jeśli można ją odróżnić od wszystkich innych członków grupy. Natomiast osoba fizyczna „możliwa do zidentyfikowania" nie została jeszcze zidentyfikowana, jednak jej identyfikacja jest możliwa. Najczęściej występującą informacją pozwalającą na bezpośrednią identyfikację osoby fizycznej jest jej

imię i nazwisko. W definicji danych osobowych jako czynniki identyfikujące wskazane są także: 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. Wyliczenie zawarte w definicji ma charakter przykładowy.

Ostatni element definicji – „osoba fizyczna" – wskazuje, że ochronę wynikającą z przepisów RODO stosuje się do osób fizycznych. Prawo do ochrony danych osobowych jest prawem uniwersalnym, tj. mającym zastosowanie do wszystkich ludzi, a nie tylko do – przykładowo – obywateli danego państwa. Zgodnie z tą definicją ochrona wynikająca z przepisów o ochronie danych osobowych nie przysługuje osobom prawnym.

Rodzaje danych osobowych

Na podstawie RODO można wyróżnić trzy rodzaje danych osobowych:

- tzw. dane zwykłe,
- szczególne kategorie danych osobowych,
- dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Do ostatniej kategorii zalicza się – zgodnie z art. 10 RODO – dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Szczególne kategorie danych określono w art. 9 ust. 1 RODO. Są to: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Niektóre ze szczególnych kategorii danych zdefiniowano w art. 4 pkt 13–1 5 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*;
- *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*;
- *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*.

Natomiast wszelkie inne dane osobowe określa się jako zwykłe dane osobowe. Innymi słowy, dane zwykłe są danymi osobowymi, które nie należą ani do szczególnych kategorii danych, ani nie dotyczą wyroków skazujących lub naruszeń prawa.

Przykłady danych osobowych oraz kategorii osób, których dane najczęściej przetwarzane są przez radców prawnych i adwokatów, wskazano w podrozdziale 3.1.

2.2 Przedmiotowy zakres stosowania RODO

Ogólne omówienie

Przedmiotowy zakres stosowania ogólnego rozporządzenia określono w art. 2 RODO. Zgodnie z art. 2 ust. 1 RODO ogólne 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*.

Znaczenie dla określenia przedmiotowego zakresu stosowania RODO mają zatem definicje następujących pojęć: „przetwarzanie", „dane osobowe" oraz „zbiór".

Termin „przetwarzanie" zdefiniowano w art. 4 pkt 2 RODO jako 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*. Zakres pojęciowy przetwarzania jest zatem bardzo szeroki, a wyliczenie operacji w powyższej definicji ma charakter przykładowy.

Definicję „danych osobowych" omówiono w podrozdziale 2.1.

Natomiast „zbiór danych" określono w art. 4 pkt 6 RODO w następujący sposób: *uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie*. Należy pamiętać, że pojęcie zbioru danych odnosi się tylko do ręcznego przetwarzania danych osobowych.

Na podstawie przepisu art. 2 ust. 1 RODO można wyróżnić dwa rodzaje operacji przetwarzania:

- przetwarzanie całkowicie lub częściowo zautomatyzowane, oraz
- przetwarzanie ręczne danych osobowych stanowiących część zbioru lub mających stanowić część zbioru.

Przetwarzanie całkowicie lub częściowo zautomatyzowane jest przetwarzaniem z wykorzystaniem technologii – w przeciwieństwie do przetwarzania ręcznego, którego dokonuje się bez użycia jakichkolwiek technologii. Pojęcia „zautomatyzowane przetwarzanie" nie zdefiniowano, ponieważ zgodnie z motywem 15 RODO ochrona danych osobowych powinna być neutralna pod względem

technicznym i nie powinna zależeć od stosowanych technik. Typowym przetwarzaniem zautomatyzowanym będzie przetwarzanie danych z użyciem systemów informatycznych.

Przetwarzaniem ręcznym jest natomiast przetwarzanie danych wyłącznie w formie papierowej. Należy przy tym pamiętać, że prawo ochrony danych ma zastosowanie do przetwarzania ręcznego tylko wówczas, gdy przetwarzane dane znajdują się lub mają się znaleźć w zbiorze danych. Innymi słowy chodzi o takie dane osobowe, które są uporządkowane według określonych kryteriów. Takim zbiorem danych mogą więc być na przykład akta sprawy sądowej.

Wyłączenia od stosowania RODO

Na mocy art. 2 ust. 2 RODO stosowanie RODO wyłączone jest w następujących przypadkach przetwarzania danych osobowych:

- w ramach działalności nieobjętej zakresem prawa Unii, np. działalności dotyczącej bezpieczeństwa narodowego;
- przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres wspólnej polityki zagranicznej i bezpieczeństwa Unii;
- przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
- 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.

Na szerszą uwagę zasługują dwa ostatnie przypadki.

Poprzez przetwarzanie w ramach czynności o charakterze osobistym lub domowym rozumie się przetwarzanie bez związku z działalnością zawodową lub handlową. Jako przykłady takiej działalności w motywie 18 RODO wskazano prowadzenie korespondencji osobistej i przechowywanie adresów, podtrzymywanie więzi społecznych oraz działalność internetową podejmowaną w ramach takiej działalności.

Natomiast ostatnie wyłączenie odnosi się do przetwarzania danych osobowych przez organy ścigania w ramach wykonywanych przez nie zadań dotyczących zapobiegania przestępczości, prowadzenia postępowań karnych itd. Kompleksową regulację przetwarzania danych osobowych w tym zakresie zawiera dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. Termin transpozycji tej dyrektywy do krajowych porządków prawnych mija 6 maja 2018 r.

Należy przy tym pamiętać, że przepisy dyrektywy (ustawy implementującej dyrektywę w prawie krajowym) mają zastosowanie do przetwarzania danych osobowych w ramach postępowania karnego wyłącznie przez organy ścigania, a nie przez profesjonalnych pełnomocników lub obrońców w ramach takiego postępowania.

Odniesienie do działalności radcy prawnego lub adwokata

Do działalności w kancelarii radcy prawnego i adwokata stosuje się przepisy RODO. Radca prawny lub adwokat dokonują przetwarzania danych osobowych w ramach prowadzonej działalności zawodowej. Są to chociażby dane osobowe klientów, stron postępowania lub osób zatrudnionych w kancelarii. Przetwarzanie danych przez radcę prawnego lub adwokata często może mieć charakter zautomatyzowany, czyli odbywać się przy użyciu technologii informacyjnych. Jeżeli przetwarzanie dokonywane jest w sposób ręczny, to o ile dane znajdują w zbiorze danych lub mają się w nim znaleźć, RODO również będzie mieć zastosowanie. Działalność racy prawnego lub adwokata nie mieści się także wśród typów działalności wyłączonych spod przedmiotowego zakresu stosowania RODO.

Podsumowując, na podstawie przepisów dotyczących przedmiotowego zakresu stosowania RODO należy uznać, że ogólne rozporządzenie stosuje się do działalności zawodowej radcy prawnego lub adwokata.

Niektóre obowiązki wynikające z RODO mogą być wyłączone lub ograniczone wobec radców prawnych i adwokatów, co zostanie omówione w dalszych rozdziałach poradnika.

2.3 Podmiotowy zakres stosowania RODO

Ogólne omówienie

Podmiotowy zakres stosowania RODO określono w art. 3 RODO. Zgodnie z art. 3 ust. 1 RODO ogólne rozporządzenie *ma zastosowanie do przetwarzania danych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii*.

Znaczenie dla określenia podmiotowego zakresu stosowania RODO mają definicje pojęć: „przetwarzanie danych w związku z działalnością prowadzoną przez jednostkę organizacyjną", „jednostka organizacyjna", „administrator" oraz „podmiot przetwarzający".

„Przetwarzanie danych w związku z działalnością prowadzoną przez jednostkę organizacyjną" nie oznacza, że przetwarzania musi dokonywać właśnie ta jednostka. Wystarczające jest, aby istniał związek pomiędzy czynnością przetwarzania danych a działalnością danej jednostki organizacyjnej znajdującej się na obszarze Unii Europejskiej.

„Jednostka organizacyjna" stanowi tłumaczenie angielskiego pojęcia „*establishment*". Ogólne rozporządzenie nie zawiera definicji legalnej pojęcia „jednostka organizacyjna". Pojęcia tego nie należy utożsamiać z prowadzeniem działalności gospodarczej, pojęciem siedziby, miejsca zamieszkania, oddziału lub przedstawicielstwa przedsiębiorcy. Jak wskazuje motyw 22 RODO, pojęcie „jednostka organizacyjna" zakłada skuteczne i faktyczne prowadzenie działalności gospodarczej poprzez stabilne

struktury. Forma prawna takich struktur – niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną – nie jest w tym względzie czynnikiem decydującym. W motywie tym podkreślono, że forma prawna jednostki organizacyjnej nie jest decydująca dla uznania, że dane przetwarzanie jest objęte zakresem podmiotowym stosowania RODO.

Pojęcia „administrator" oraz „podmiot przetwarzający" omówiono w podrozdziale 2.4.

Odniesienie do działalności radcy prawnego lub adwokata

Ogólne rozporządzenie ma zastosowanie do działalności prowadzonej przez radców prawnych i adwokatów w Rzeczpospolitej Polskiej jako państwie członkowskim Unii Europejskiej. RODO będzie mieć zastosowanie bez względu na formę prowadzonej działalności, jeżeli dochodzi do przetwarzania danych osobowych.

Formy prowadzenia działalności i ich wpływ na funkcję radcy prawnego lub adwokata względem przetwarzanych danych osobowych omówiono szerzej w podrozdziale 3.2.

2.4 Rodzaje podmiotów obowiązane do ochrony danych osobowych (administrator, współadministrator, podmiot przetwarzający)

Ogólne omówienie

Ogólne rozporządzenie wyróżnia trzy kategorie podmiotów obowiązanych do ochrony danych osobowych: administrator, współadministrator oraz podmiot przetwarzający.

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*. Dopuszczalne jest również określenie celów i sposobów przetwarzania w prawie Unii lub w prawie państwa członkowskiego. W takim przypadku administrator może zostać wyznaczony lub mogą zostać określone konkretne kryteria jego wyznaczania w prawie Unii lub w prawie państwa członkowskiego.

Definicja pojęcia „administrator" składa się z trzech elementów:

1) element podmiotowy, czyli adresat przepisu: osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot;
2) sposób działania dopuszczający możliwość współdecydowania o przetwarzaniu danych osobowych: samodzielnie lub wspólnie ustala cele i sposoby przetwarzania;
3) zakres decyzyjny: ustala cele i sposoby przetwarzania.

Zakres podmiotowy pojęcia „administrator" jest szeroki. Administratorem może być osoba fizyczna, osoba prawna (np. spółka akcyjna lub spółka z ograniczoną odpowiedzialnością), organ publiczny, jednostka lub inny podmiot. W zakres tych dwóch ostatnich kategorii mogą wchodzić m.in. jednostki organizacyjne nieposiadające osobowości prawnej, takie jak spółka jawna, spółka partnerska, spółka komandytowa lub spółka komandytowo-akcyjna. Aby posiadać status administratora, podmiot nie musi przetwarzać danych osobowych samodzielnie, może dokonać zlecenia przetwarzania podmiotowi

przetwarzającemu. O statusie administratora decyduje możliwość ustalania celów i sposobów przetwarzania.

„Współadministrator" jest podkategorią pojęcia „administrator". „Współadministrator" to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Konstrukcję współadministratorów dopuszcza art. 26 ust. 1 RODO, zgodnie z którym: *Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami*. Ogólne rozporządzenie w ramach współadministrowania nie narzuca sztywnych ram na ustalanie celów i sposobów przez współadministratorów. Współudział może polegać zarówno na ścisłej i skoordynowanej współpracy, jak i na częściowym współdziałaniu. Jeżeli strony ustalą, że w ramach prowadzonych przez nie działań dochodzi do współadministrowania, to powinny w sposób przejrzysty uzgodnić zakresy swojej odpowiedzialności dotyczącej wykonywania obowiązków z RODO. Uzgodnienia te powinny dotyczyć w szczególności wykonywania przez osobę, której dane dotyczą, jej praw, a także realizowania obowiązków współadministratorów co do spełniania obowiązków informacyjnych. Współadministratorzy mogą również utworzyć wspólny punkt kontaktowy dla podmiotów danych.

Zgodnie z 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*. Tak jak w przypadku pojęcia „administrator" definicja ta obejmuje szeroki zakres podmiotów.

W przeciwieństwie do poprzednich regulacji prawnych, w RODO podmiot przetwarzający (zwany również procesorem) jest bezpośrednim adresatem wielu norm – zarówno tych określających obowiązki, jak i tych regulujących sankcje zanaruszenie przepisów o ochronie danych osobowych.

Zgodnie z art. 28 ust. 1 RODO administrator odpowiada za poprawność wyboru podmiotu powierzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymogi RODO oraz chroniących prawa podmiotów danych. Na podstawie art. 28 ust. 3 lit. a) RODO podmiot przetwarzający może działać wyłącznie na udokumentowane polecenie administratora. Działanie podmiotu powierzającego w imieniu administratora oznacza również, że jest on związany celami i sposobami przetwarzania wyznaczonymi przez administratora.

Tematyka powierzenia przetwarzania danych, w tym wyboru podmiotu przetwarzającego oraz zawierania umowy powierzenia, została szczegółowo omówiona w podrozdziale 5.4.

Odniesienie do działalności radcy prawnego lub adwokata

Status radcy prawnego lub adwokata w ramach RODO z uwzględnieniem dopuszczalnych form wykonywania zawodu omówiono w podrozdziale 3.2. W tym miejscu należy wyłącznie wskazać, że w ramach prowadzonego procesu legislacyjnego nad przepisami wprowadzającymi ustawę o ochronie danych osobowych zaproponowano wprowadzenie zmian do URP oraz UPoA polegających na wyznaczeniu administratorów w ramach prawa krajowego.

W praktyce wykonywania zawodu przez radcę prawnego lub adwokata mogą wystąpić podmioty, które będą zleceniobiorcami i będą przetwarzać dane osobowe w jego imieniu, np. zewnętrzne biuro rachunkowe lub firma zapewniająca obsługę kadrowo-płacową. W takim przypadku będą one podmiotami przetwarzającymi.

3. Status radców prawnych i adwokatów w czynnościach przetwarzania danych

3.1 Typowe kategorie osób, których dane dotyczą, i typowe kategorie danych przetwarzanych przez radcę prawnego lub adwokata

Poniżej wskazano typowe czynności przetwarzania danych osobowych realizowane w kancelarii przez radców prawnych i adwokatów w ramach ich działalności zawodowej (pojęcie czynności przetwarzania omówiono szerzej w podrozdziale 4.4).

Poniższe wyliczenie ma charakter przykładowy i nie jest wyczerpujące – w zależności od formy wykonywania zawodu czy też wielkości kancelarii poszczególne czynności przetwarzania mogą się różnić.

Typowe czynności przetwarzania prowadzone przez radców prawnych i adwokatów można podzielić na dwie ogólne kategorie:

- dane przetwarzane w związku ze świadczeniem pomocy prawnej oraz
- dane przetwarzane w związku z funkcjonowaniem kancelarii prawnej lub spółki.

Kategorie osób, których dane przetwarzane są w związku ze świadczeniem pomocy prawnej:

- Klienci (osoby fizyczne)
  - Typowe cele przetwarzania: świadczenie pomocy prawnej, w tym występowanie w imieniu klienta przed urzędami i sądami, udzielanie porad prawnych, opracowywanie projektów aktów prawnych; wykonywanie umowy z klientem; podejmowanie działań związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu; spełnianie wymogów wynikających z przepisów podatkowych i o rachunkowości, w tym prowadzenie dokumentacji podatkowej oraz przechowywanie dowodów księgowych; cele archiwizacyjne;
  - Typowe kategorie danych: imię i nazwisko, adres korespondencyjny, dane kontaktowe, informacje przekazane radcy prawnemu lub adwokatowi konieczne do świadczenia pomocy prawnej (różne rodzaje informacji w zależności od charakteru udzielanej pomocy prawnej);
- Osoby reprezentujące klientów będących osobami prawnymi lub tzw. ułomnymi osobami prawnymi, w tym osoby kontaktowe
  - Typowe cele przetwarzania: kontaktowanie się z osobami reprezentującymi klienta w związku ze świadczeniem pomocy prawnej klientowi oraz z wykonywaniem umowy z klientem; cele archiwizacyjne;
  - Typowe kategorie danych: imię i nazwisko, stanowisko, służbowe dane kontaktowe;

- Inne osoby fizyczne, których dane są przetwarzanie w związku z prowadzeniem spraw klientów (w przypadku postępowania sądowego lub administracyjnego np. inne strony postępowania, świadkowie, pełnomocnicy, biegli itp.)

    - Typowe cele przetwarzania: świadczenie pomocy prawnej klientowi; cele archiwizacyjne;

    - Typowe kategorie danych: imię i nazwisko, dane kontaktowe, rola w postępowaniu sądowym lub administracyjnym, stanowisko, zawód.

Kategorie osób, których dane przetwarzane są w związku z funkcjonowaniem kancelarii lub spółki:

- Pracownicy

    - Typowe cele przetwarzania: zawarcie i wykonywanie umowy o pracę; spełnianie wymogów wynikających z przepisów prawa pracy oraz m.in. przepisów o ubezpieczeniu społecznym, ubezpieczeniu zdrowotnym, podatkach, wypadkach przy pracy, zakładowym funduszu świadczeń socjalnych, rachunkowości; organizacja pracy, zarządzanie personelem; prowadzenie szczegółowego wykazu zadań wykonanych przez pracownika na potrzeby rozliczenia z klientem;

    - Typowe kategorie danych: imię i nazwisko, adres zamieszkania, numer PESEL, informacje dotyczące doświadczenia zawodowego i wykształcenia; szczegółowy wykaz wykonanych zadań;

- Stali współpracownicy (na podstawie umowy cywilnoprawnej)

    - Typowe cele przetwarzania: zawarcie i wykonywanie umowy; spełnianie wymogów wynikających z przepisów podatkowych i rachunkowych; organizacja pracy, zarządzanie personelem; prowadzenie szczegółowego wykazu zadań wykonanych przez pracownika na potrzeby rozliczenia z klientem;

    - Typowe kategorie danych: imię i nazwisko, adres zamieszkania, numer PESEL, informacje dotyczące doświadczenia zawodowego i wykształcenia; szczegółowy wykaz wykonanych zadań;

- Osoby współpracujące sporadycznie (np. notariusze, inni radcy prawni, inni adwokaci)

    - Typowe cele przetwarzania: utrzymywanie bieżących relacji zawodowych; współpraca zawodowa, przyjmowanie i składanie ofert;

    - Typowe kategorie danych: imię i nazwisko, stanowisko, tytuł zawodowy, specjalizacja zawodowa, służbowe dane kontaktowe;

- Dostawcy towarów i usług (osoby fizyczne prowadzące działalność gospodarczą)

- Typowe cele przetwarzania: zawieranie i wykonywanie umów (np. sprzedaży, świadczenia usług); spełnianie wymogów wynikających z przepisów podatkowych i o rachunkowości, w tym prowadzenie dokumentacji podatkowej oraz przechowywanie dowodów księgowych; cele archiwizacyjne;

- Typowe kategorie danych: imię i nazwisko, rodzaj prowadzonej działalności, służbowe dane kontaktowe, NIP.

3.2 Status radcy prawnego lub adwokata oraz kancelarii w czynnościach przetwarzania danych osobowych

W stosunku do przetwarzania powyżej wskazanych kategorii danych osobowych należy określić status radcy prawnego lub adwokata.

Zgodnie z RODO radcę prawnego lub adwokata należy uznać za administratora danych osobowych, jeżeli decyduje on o celach i sposobach przetwarzania danych osobowych.

Istnieje zgodność co do tego, że radca prawny lub adwokat prowadzący własną działalność w formie kancelarii ma status administratora w zakresie, w jakim przetwarza dane osobowe m.in.:

1) swoich pracowników;

2) stałych współpracowników (na podstawie umowy cywilnoprawnej);

3) praktykantów i stażystów;

4) osób współpracujących sporadycznie (np. notariuszy, innych radców prawnych, adwokatów);

5) dostawców towarów i usług (osób fizycznych prowadzących działalność gospodarczą).

W tym zakresie nie ulega wątpliwości, że radca prawny lub adwokat decyduje o celach i sposobach przetwarzania danych osobowych i jest w związku z tym administratorem danych osobowych, podobnie jak jest nim każdy pracodawca przetwarzający dane osobowe swoich pracowników czy przedsiębiorca przetwarzający dane osobowe swoich dostawców.

Odrębnego omówienia wymaga natomiast status radcy prawnego lub adwokata w zakresie przetwarzania danych osobowych w ramach wykonywania zawodu, tj. danych osobowych klientów, osób reprezentujących klientów oraz osób trzecich przekazanych przez klienta lub zebranych z innych źródeł w ramach wykonywania czynności obsługi klienta (np. dane osobowe innych stron postępowania, świadków, pełnomocników, biegłych).

W ocenie autorów status ten zależeć będzie od formy wykonywania zawodu przez, odpowiednio, radcę prawnego lub adwokata. Formy wykonywania obydwu zawodów zostały określone odrębnie dla radców prawnych (art. 8 URP) oraz adwokatów (art. 4a UPoA).

Formy wykonywania zawodu radcy prawnego

Wykonywanie zawodu radcy prawnego odbywa się na podstawie ustawy z dnia 6 lipca 1982 r. o radcach prawnych. Zgodnie z art. 6 ust. 1 URP zawód radcy prawnego polega na świadczeniu pomocy prawnej, a w szczególności na udzielaniu porad i konsultacji prawnych, sporządzaniu opinii prawnych, opracowywaniu projektów aktów prawnych oraz występowaniu przed urzędami i sądami w charakterze pełnomocnika lub obrońcy. Pomocą prawną jest zatem w szczególności udzielanie porad i konsultacji prawnych, opinii prawnych, zastępstwo prawne i procesowe.

Zgodnie z art. 8 ust. 1 URP, radca prawny może wykonywać zawód w następujących formach:

1) w ramach stosunku pracy,

2) na podstawie umowy cywilnoprawnej,

3) w kancelarii radcy prawnego oraz

4) w spółce, której wyłącznym przedmiotem działalności jest świadczenie pomocy prawnej, w formach określonych w art. 8 ust. 1 URP, tj.:

   - spółce cywilnej lub jawnej, w której wspólnikami są radcowie prawni, adwokaci, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP;

   - spółce partnerskiej, w której partnerami są radcowie prawni, adwokaci, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP;

   - spółce komandytowej lub komandytowo-akcyjnej, w której komplementariuszami są radcowie prawni, adwokaci, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP.

Formy wykonywania zawodu adwokata

Zgodnie z art. 4 UPoA zawód adwokata polega na świadczeniu pomocy prawnej, a w szczególności na udzielaniu porad prawnych, sporządzaniu opinii prawnych, opracowywaniu projektów aktów prawnych oraz występowaniu przed sądami i urzędami.

Stosownie do art. 4a ust. 1 UPoA adwokat może wykonywać zawód w następujących formach:

1) w kancelarii adwokackiej;

2) w zespole adwokackim;

3) w spółce, której wyłącznym przedmiotem działalności jest świadczenie pomocy prawnej, w formach określonych w tym przepisie, tj.:

- cywilnej lub jawnej, w której wspólnikami są adwokaci, radcowie prawni, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP;

- partnerskiej, w której partnerami są adwokaci, radcowie prawni, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP;

- komandytowej lub komandytowo-akcyjnej, w której komplementariuszami są adwokaci, radcowie prawni, rzecznicy patentowi, doradcy podatkowi lub prawnicy zagraniczni wykonujący stałą praktykę na podstawie przepisów UŚPZPP.

Formy wykonywania zawodu a status radcy prawnego i adwokata w zakresie przetwarzania danych osobowych w ramach wykonywania zawodu

W zakresie, w jakim zawody radcy prawnego i adwokata mogą być wykonywane w tożsamych formach organizacyjnoprawnych, status osób wykonujących te zawody na gruncie przepisów o ochronie danych osobowych zostanie omówiony łącznie.

Łącznie zostanie zatem omówiony status radcy prawnego i adwokata wykonujących zawód:

1) odpowiednio, w kancelarii radcy prawnego albo kancelarii adwokackiej; oraz

2) w spółce, w formach, o których mowa, odpowiednio, w art. 8 ust. 1 URP oraz art. 4a UPoA.

W przypadku form wykonywania zawodu właściwych wyłącznie dla radcy prawnego (stosunek pracy lub umowa cywilnoprawna) albo adwokata (zespół adwokacki), statusy radcy prawnego oraz adwokata zostaną omówione odrębnie.

Status radcy prawnego i adwokata wykonujących zawód w kancelarii radcy prawnego lub kancelarii adwokackiej

Pomimo niejednoznacznych stanowisk w przeszłości co do statusu radcy prawnego i adwokata na gruncie przepisów o ochronie danych osobowych, zdaniem autorów radca prawny wykonujący zawód w kancelarii radcy prawnego oraz adwokat wykonujący zawód w kancelarii adwokackiej są administratorami danych osobowych przetwarzanych w ramach wykonywania zawodu.

Istota zawodów radcy prawnego oraz adwokata, które polegają (zgodnie, odpowiednio, z art. 6 ust. 1 URP i art. 4 ust. 1 UPoA) na świadczeniu pomocy prawnej, zakłada przetwarzanie zarówno danych osobowych klientów, jak i danych osobowych osób trzecich przekazanych przez klienta oraz zebranych z innych źródeł na potrzeby wykonania usługi. Prawidłowe wykonywanie wskazanych zawodów wymaga przy tym, aby radca prawny lub adwokat samodzielnie podejmował decyzje w ramach świadczenia pomocy prawnej, w tym w zakresie celów i sposobów przetwarzania danych osobowych przekazanych przez klienta i zebranych w toku świadczenia usługi prawnej, i nie był w tym względzie w pełni zależny od polecenia klienta.

Analizując status radcy prawnego oraz adwokata w czynnościach przetwarzania danych osobowych, należy mieć również na względzie, że sposób wykonywania tych zawodów, w tym przetwarzanie danych osobowych niezbędnych do świadczenia pomocy prawnej, kształtowany jest przez przepisy prawa powszechnie obowiązującego (m.in. URP oraz UPoA) oraz kodeksy etyki (odpowiednio: Kodeks Etyki Radcy Prawnego oraz Zbiór Zasad Etyki Adwokackiej i Godności Zawodu). Regulacje te nakładają na radcę prawnego lub adwokata szereg obowiązków związanych z wykonywaniem zawodu, w tym zobowiązują ich m.in. do zachowania tajemnicy zawodowej oraz unikania konfliktu interesów.

W związku z potrzebą wykonania wspomnianych obowiązków przedstawiciele tych zawodów podejmują samodzielne decyzje, w tym również w zakresie przetwarzania danych osobowych. Należy przy tym wskazać, że wykonywanie zawodu przez radcę prawnego lub adwokata w sposób zgodny z prawem oraz zasadami etyki nie byłoby możliwe bez przetwarzania takich danych osobowych w sposób przynajmniej częściowo niezależny od decyzji klienta.

W tym kontekście warto zwrócić uwagę na to, że w zakresie objętym tajemnicą zawodową i innymi zasadami etyki klient kancelarii nie ma już pełnego wpływu na przetwarzanie danych osobowych przez radcę prawnego lub adwokata. W przypadku przepisów ustawowych świadczy o tym nie tylko zasada ochrony tajemnicy zawodowej, ale również inne zasady ustawowe, np. przewidujące odpowiedzialność dyscyplinarną radcy prawnego lub adwokata. W postępowaniu w tym przedmiocie może bowiem okazać się niezbędne przetwarzanie wskazanych wyżej danych osobowych.

Dla przykładu klient nie może żądać od radcy prawnego lub adwokata prowadzącego jego sprawę usunięcia danych osobowych, które jednocześnie podlegają tajemnicy zawodowej. Co więcej, radca prawny lub adwokat zobowiązany jest do przechowywania takich danych, np. aby w przyszłości ustalić, czy istnieje konflikt interesów. Obowiązek unikania konfliktu interesów, będący jedną z naczelnych zasad etyki zarówno radcowskiej, jak i adwokackiej sprowadza się do tego, że w każdym wypadku, rozważając przyjęcie sprawy do prowadzenia, radca prawny lub adwokat powinien ocenić sytuację swoich potencjalnych klientów pod kątem istnienia sprzeczności ich interesów z interesami osób, którym radca prawny lub adwokat już wcześniej udzielał bądź też aktualnie udziela pomocy prawnej. Jeśli ujawni się możliwość powstania takiej sprzeczności, radca prawny lub adwokat musi odmówić takiemu klientowi przyjęcia zlecenia, pod rygorem odpowiedzialności dyscyplinarnej.

Ponadto należy podkreślić, że przyjęcie stanowiska, iż radca prawny lub adwokat jest podmiotem przetwarzającym w zakresie przetwarzania wyżej wymienionych danych, byłoby nie do pogodzenia z jego rolą jako depozytariusza ochrony tajemnicy. Status podmiotu przetwarzającego zakłada podporządkowanie w zakresie przetwarzania danych osobowych decyzjom administratora. Tymczasem ochrona tajemnicy wymaga samodzielnych decyzji jej powiernika – radcy prawnego bądź adwokata. W ocenie autorów radca prawny oraz adwokat nie są objęci dyspozycją klienta co do ujawnienia lub wykorzystania poufnych danych. Przykładowo w konkretnych przypadkach wykonanie polecenia klienta (np. upublicznienie danych osobowych osób trzecich) może prowadzić do naruszenia zasad etyki, a do tego radca prawny ani adwokat doprowadzić nie może.

Specyfika działalności radcy prawnego oraz adwokata, jak również fakt, że zawody te regulowane są przepisami prawa powszechnie obowiązującego oraz kodeksami etyki, wymaga od nich samodzielnego decydowania o celach i sposobach przetwarzania danych osobowych w ramach wykonywania zawodu.

Dotyczy to zarówno danych osobowych przekazanych przez klienta, jak i tych zebranych przez radcę prawnego czy adwokata samodzielnie w celu świadczenia klientowi pomocy prawnej.

W ocenie autorów dla statusu radcy prawnego lub adwokata jako administratora danych osobowych bez znaczenia jest przy tym rodzaj konkretnego zlecenia. W szczególności nie można się zgodzić ze stanowiskiem, zgodnie z którym radca prawny lub adwokat jest podmiotem przetwarzającym, jeżeli otrzymane od klienta zlecenie polega wyłącznie na wykonaniu audytu lub napisania umowy.

Mając powyższe uwagi na względzie, należy wnioskować, że radca prawny lub adwokat jest administratorem danych osobowych przetwarzanych w ramach wykonywania zawodu, w tym danych osobowych przekazanych przez klienta.

Status radcy prawnego i adwokata wykonujących zawód w spółce

Radca prawny oraz adwokat mogą wykonywać zawód w spółce w formach określonych odpowiednio w art. 8 ust. 1 URP oraz art. 4a UPoA. Formy prawne spółek wskazane w obu przepisach oraz wymogi stawiane takim spółkom są zasadniczo tożsame, stąd zasadne jest ich łączne omówienie.

Radca prawny oraz adwokat mogą wykonywać zawód spółce w następujących formach:

1) spółce cywilnej lub jawnej;

2) spółce partnerskiej;

3) spółce komandytowej lub komandytowo-akcyjnej.

Zdaniem autorów 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 radcy prawnego czy adwokata wykonującego w niej zawód.

Taki pogląd jest zbieżny ze stanowiskiem GIODO, zgodnie z którym administratorem danych jest sama spółka prawa handlowego, nie zaś jej organy, osoby zasiadające w organach tej spółki lub pełniące w niej funkcje kierownicze. Potwierdza je również wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 10 lipca 2006 r. (sygn. II SA/Wa 955/06), który wskazał, że *przymiot strony w postępowaniu administracyjnym posiada spółka jawna jako administrator danych, nie zaś jej wspólnicy*. Nie zmienia tego okoliczność, iż wykonywanie zawodu radcy prawnego oraz adwokata regulowane jest szczególnymi przepisami, w tym kodeksami etyki, które zobowiązują przedstawicieli tych zawodów do zachowania tajemnicy (por. także podrozdział 3.3. poniżej), ani to, że klient udziela pełnomocnictwa konkretnemu radcy prawnemu lub adwokatowi, a nie spółce.

W tym kontekście warto zauważyć, że stroną umowy o świadczenie usług prawnych w takiej sytuacji jest sama spółka osobowa, nie zaś radca prawny lub adwokat – wspólnik, partner albo komplementariusz spółki.

Natomiast w odniesieniu do wykonywania zawodu w formie spółki cywilnej, pomimo istniejących w doktrynie wątpliwości, w ocenie autorów za administratora danych należy uznać samą spółkę cywilną, a nie jej wspólników.

Istotą umowy spółki cywilnej w przypadku radcy prawnego bądź adwokata jest osiągnięcie wspólnego celu gospodarczego – świadczenia pomocy prawnej (art. 860 § 1 KC), które nieodłącznie wiąże się z przetwarzaniem danych osobowych. Mimo że wspólnicy spółki cywilnej są odrębnymi przedsiębiorcami, a spółka cywilna, w odróżnieniu od spółki osobowej, nie posiada podmiotowości prawnej, to przetwarzanie danych osobowych i decydowanie o celach oraz sposobach przetwarzania następuje w ramach jednej, wspólnej struktury organizacyjno-prawnej i z wykorzystaniem tej samej infrastruktury, stworzonej na potrzeby łączącej wspólników spółki cywilnej.

Również w przypadku spółki cywilnej pomimo iż klient podpisuje umowę o świadczenie usług ze wszystkimi wspólnikami, to wskazuje się jednocześnie, że działają oni w ramach spółki cywilnej, a nie jako niezależni od siebie przedsiębiorcy.

Warto też wskazać, że w oczach klienta to właśnie spółka cywilna, a nie kilku odrębnych radców prawnych lub adwokatów jest administratorem jego danych osobowych. Zgodnie natomiast z opinią Grupy Roboczej Art. 29 sposób postrzegania podmiotu w oczach osoby, której dane dotyczą, może dodatkowo świadczyć za uznaniem danego podmiotu za administratora danych.

Takie stanowisko jest zgodne z praktyką GIODO, który w rejestrze zbiorów danych osobowych rejestrował zbiory danych osobowych administratorów – spółek cywilnych, a nie wspólników spółki cywilnej.

Status radcy prawnego wykonującego zawód w ramach stosunku pracy

W przypadku wykonywania zawodu radcy prawnego w ramach stosunku pracy (stosunku służbowego) administratorem wymienionych wyżej danych osobowych jest pracodawca, a nie radca prawny. W takiej sytuacji radca prawny będzie przetwarzał dane osobowe z upoważnienia administratora i na podstawie jego polecenia (ang. *instructions*), o którym mowa w art. 29 RODO. Obowiązują go wówczas zasady ochrony danych, w tym wykonywania obowiązków z RODO, wprowadzone w jego jednostce organizacyjnej przez pracodawcę (administratora). Podobnie jak w przypadku czynności na danych osobowych wykonywanych przez innych pracowników, również czynności w tym zakresie dokonywane przez radcę prawnego wchodzą w zakres władztwa pracodawcy nad przetwarzaniem danych osobowych w zakładzie pracy. Jednak wydając wobec radcy prawnego „instrukcje", pracodawca powinien uwzględniać szczególne zasady wykonywania zawodu radcy prawnego wynikające z URP oraz zasad etyki, które mają swoje konsekwencje także w odniesieniu do przetwarzania i ochrony danych osobowych.

Status radcy prawnego wykonującego zawód na podstawie umowy cywilnoprawnej

URP przewiduje, że radca prawny może wykonywać zawód również na podstawie umowy cywilnoprawnej (np. umowy-zlecenia). Umowy cywilnoprawne traktuje się jako osobną formę zawodu, która w istocie wykonywana jest poza prowadzeniem kancelarii radcy prawnego oraz poza

uczestnictwem w spółkach osobowych. Nie do przyjęcia wydaje się przyjmowanie zleceń klientów poza prowadzoną kancelarią, a świadczenie pomocy prawnej w formie umowy cywilnoprawnej odnosi się wyłącznie do doraźnych zleceń klientów radcy prawnemu nieprowadzącemu kancelarii, a więc niebędącemu przedsiębiorcą. Zgodnie z prezentowanym poglądem wykonywanie zawodu radcy prawnego na podstawie umowy cywilnoprawnej jest możliwe wyłącznie wówczas, gdy usługi prawnicze mają charakter doraźny, np. gdy są wykonywane przez emeryta.

Mając na względzie powyższe stanowisko, zdaniem autorów jeżeli radca prawny wykonuje swoje zadania z zakresu świadczenia pomocy prawnej na podstawie umowy cywilnoprawnej i dokonuje przetwarzania danych w ramach struktury organizacyjnej zleceniodawcy (lub innego podmiotu, na rzecz którego radca prawny świadczy daną usługę na podstawie umowy cywilnoprawnej), przy wykorzystaniu infrastruktury i sprzętu zleceniodawcy, to należałoby go uznać za osobę upoważnioną do przetwarzania danych osobowych zgodnie z art. 29 RODO.

W takim przypadku to zleceniodawca (lub inny podmiot, na rzecz którego radca prawny świadczy daną usługę na podstawie umowy cywilnoprawnej) posiada status administratora danych i upoważnia radcę prawnego do przetwarzania danych osobowych. Radca prawny wykonujący umowę cywilnoprawną będzie zobowiązany w zakresie przetwarzania danych osobowych do przestrzegania zasad ochrony danych wprowadzonych w jednostce organizacyjnej administratora (np. zleceniodawcy), podobnie jak ma to miejsce w przypadku radcy prawnego wykonującego zawód w ramach stosunku pracy.

Jeżeli natomiast radca prawny, wykonując umowę cywilnoprawną, będzie przetwarzał dane osobowe bez spełnienia powyższych warunków i będzie podejmował decyzje co do celów i sposobów przetwarzania danych osobowych niezależnie od poleceń zleceniodawcy (lub innego podmiotu, na rzecz którego radca prawny świadczy daną usługę na podstawie umowy cywilnoprawnej), stanie się ich administratorem.

Status adwokata wykonującego zawód w zespole adwokackim

UPoA przewiduje, że adwokat może wykonywać zawód w zespole adwokackim, który posiada osobowość prawną (art. 10 UPoA). Jest to forma wykonywania zawodu przewidziana wyłącznie dla adwokatów. Zdaniem autorów, wykonywanie zawodu w zespole adwokackim nie będzie się różniło w zakresie statusu adwokata od wykonywania zawodu w spółce osobowej czy cywilnej. Podobnie jak w przypadku spółek osobowych i cywilnych, to zespół adwokacki należy uznać za administratora danych. Decyduje on bowiem o celach i sposobach przetwarzania danych osobowych przekazanych przez klienta lub zebranych w toku świadczenia pomocy prawnej. Adwokat wykonujący zawód w zespole adwokackim będzie przetwarzał takie dane osobowe z upoważnienia administratora (zespołu adwokackiego) i na podstawie polecenia, o którym mowa w art. 29 RODO.

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r.

W tym kontekście warto przywołać odpowiednie postanowienia projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r. (znanego wcześniej jako „ustawa – Przepisy wprowadzające ustawę o ochronie danych osobowych”),

który znowelizuje zarówno UPoA (art. 8 projektu) oraz URP (art. 9 projektu). Projekt przewiduje określenie statusu radcy prawnego i adwokata w zakresie przetwarzania danych osobowych w ramach wykonywania zawodu, jednak dokonuje tego w sposób niejednolity.

W stosunku do radcy prawnego przewiduje się, że radca prawny wykonujący zawód w kancelarii radcy prawnego lub spółce, o której mowa w art. 8 ust. 1, jest administratorem w przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu (projektowany art. 5a ust. 1 pkt 5 URP - art. 9 PWUODO).

Natomiast w przypadku adwokata projekt nie odnosi się do form wykonywania zawodu adwokata i stanowi, że adwokat jest administratorem w przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu (projektowany art. 16a ust. 1 pkt 5 URP - art. 8 PWUODO) .

Należy jednak wziąć pod uwagę, że prace nad projektem wciąż trwają i ostateczny tekst nowelizacji może ulec zmianie.

Wnioski

1) Radca prawny lub adwokat prowadzący własną działalność w formie kancelarii ma status administratora danych w zakresie, w jakim przetwarza dane osobowe swoich pracowników, stałych współpracowników (na podstawie umowy cywilnoprawnej), praktykantów i stażystów, osób współpracujących sporadycznie (np. notariusze, inni radcy prawni, adwokaci), dostawców towarów i usług (osób fizycznych prowadzących działalność gospodarczą) itp.

2) W przypadku, gdy radca prawny lub adwokat wykonuje zawód w innej formie, administratorem wymienionych wyżej danych będzie:

- spółka, o której mowa w art. 8 URP lub art. 4a UPoA;
- pracodawca, w przypadku gdy radca prawny wykonuje zawód w ramach stosunku pracy;
- zleceniodawca (lub inny podmiot, na rzecz którego radca prawny świadczy pomoc prawną na podstawie umowy cywilnoprawnej), w przypadku gdy radca prawny wykonuje zawód na podstawie umowy cywilnoprawnej;
- zespół adwokacki, w przypadku gdy adwokat wykonuje zawód w zespole adwokackim.

3) W przypadku gdy radca prawny lub adwokat wykonuje zawód w innej formie, administratorem wymienionych wyżej danych będzie:

- spółka, o której mowa w art. 8 URP lub art. 4a UPoA;
- pracodawca, w przypadku gdy radca prawny wykonuje zawód w ramach stosunku pracy;

- zleceniodawca (lub inny podmiot, na rzecz którego radca prawny świadczy pomoc prawną na podstawie umowy cywilnoprawnej), w przypadku gdy radca prawny wykonuje zawód na podstawie umowy cywilnoprawnej;

- zespół adwokacki, w przypadku gdy adwokat wykonuje zawód w zespole adwokackim.

W powyższych sytuacjach radca prawny lub adwokat będzie przetwarzał wskazane wyżej dane osobowe z upoważnienia administratora i na podstawie jego polecenia zgodnie art. 29 RODO.

3.3 Ochrona danych osobowych a tajemnica zawodowe (tajemnica radcowska i tajemnica adwokacka)

Tajemnica zawodowa

Zarówno na gruncie polskich, jak i zagranicznych przepisów brak jest definicji tajemnicy zawodowej. Również doktryna nie jest zgodna co do tego, jak należy rozumieć tajemnicę zawodową. W ocenie autorów tajemnicę zawodową można jednak rozumieć jako obowiązek zachowania poufności wynikający z faktu wykonywania zawodu powszechnie identyfikowanego jako tzw. zawód zaufania publicznego. Tajemnica zawodowa w przypadku zawodów zaufania publicznego, do których zalicza się zawód radcy prawnego i adwokata, uznawana jest za warunek istnienia i funkcjonowania tych zawodów. Zawody te, jako oparte na szczególnej więzi zaufania pomiędzy usługodawcą a usługobiorcą, wymagają bowiem istnienia tajemnicy zawodowej jako gwarancji tego zaufania.

Dokładny zakres tajemnicy danego zawodu określają zwykle odpowiednie ustawy zawodowe oraz dodatkowo kodeksy etyki zawodowej.

Tajemnica radcy prawnego i adwokata

Tajemnica radcy prawnego oraz tajemnica adwokacka mają swoje źródło w przepisach prawa powszechnie obowiązującego (w tym w szczególności art. 3 ust. 3 URP oraz art. 6 UPoA) oraz w kodeksach etyki.

Stosownie do art. 3 ust. 3 URP (oraz odpowiednio art. 6 UPoA) radca prawny adwokat jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej. Obowiązek ten nie może być ograniczony w czasie, a ponadto radca prawny lub adwokat nie może zostać zwolniony z obowiązku zachowania tajemnicy zawodowej co do faktów, o których się dowiedział, udzielając pomocy prawnej lub prowadząc sprawę, z wyjątkiem informacji udostępnionych na podstawie przepisów Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2017 r. poz. 1049 ze zm.) w zakresie tam określonym.

Zakres obowiązku zachowania tajemnicy doprecyzowują postanowienia kodeksów etyki zawodowej, odpowiednio KERP oraz ZZEAiGZ. Warto przy tym podkreślić, że zarówno radca prawny, jak i adwokat są zobowiązani do wykonywania zawodu nie tylko zgodnie z przepisami prawa powszechnie obowiązującego, lecz również zgodnie z zasadami etyki (odpowiednio art. 3 ust. 2 i art. 64 ust. 1 URP oraz art. 80 UPoA).

W odniesieniu do zawodu radcy prawnego art. 15 KERP stanowi, że radca prawny jest obowiązany zachować w tajemnicy wszystkie informacje dotyczące klienta i jego spraw ujawnione radcy prawnemu przez klienta bądź uzyskane w inny sposób w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i sposobu ich utrwalenia.

Tajemnica zawodowa obejmuje także wszelkie tworzone przez radcę prawnego dokumenty oraz korespondencję radcy prawnego z klientem i osobami uczestniczącymi w prowadzeniu sprawy – powstałe dla celów związanych ze świadczeniem pomocy prawnej, jak również informacje ujawnione radcy prawnemu przed podjęciem przez niego czynności zawodowych, jeżeli z okoliczności sprawy wynika, że ujawnienie nastąpiło dla potrzeb świadczenia pomocy prawnej i uzasadnione było oczekiwaniem, że radca prawny będzie ją świadczył.

Zgodnie natomiast z § 19 ZZEAiGZ adwokat zobowiązany jest zachować w tajemnicy oraz zabezpieczyć przed ujawnieniem lub niepożądanym wykorzystaniem wszystko, o czym dowiedział się w związku z wykonywaniem obowiązków zawodowych. Tajemnicą adwokacką objęte są w szczególności znajdujące się w aktach adwokackich materiały, wszystkie wiadomości, notatki i dokumenty dotyczące sprawy uzyskane od klienta oraz innych osób, niezależnie od miejsca, w którym się znajdują.

Co ważne, w przypadku obu zawodów tajemnica zawodowa uznawana jest za warunek istnienia relacji z klientem opartej na zaufaniu, a więc w ogóle możliwości skutecznego wykonywania czynności zawodowych.

Warto jednocześnie podkreślić, że w zasadach wykonywania obu zawodów znajduje się nie tylko obowiązek tajemnicy zawodowej (art. 15 KERP i § 19 ZZEAiGZ), ale również inne obowiązki, z którymi związane może być przetwarzanie danych osobowych. Przykładem jest choćby obowiązek unikania konfliktu interesów (art. 28–30 KERP i § 22 ZZEAiGZ) czy zakaz świadomego podawania nieprawdziwych informacji (art. 38 ust. 3 KERP i § 11 ZZEAiGZ). W konkretnych przypadkach może dojść do przetwarzania danych osobowych przez radcę prawnego lub adwokata, w celu ustalenia, czy jego postępowanie jest zgodne z tymi zasadami.

Tajemnica zawodowa i zasady etyki na gruncie RODO

RODO uwzględnia szczególny charakter niektórych zawodów, które zobowiązane są do zachowania tajemnicy zawodowej, i dopuszcza możliwość ograniczenia stosowania niektórych przepisów ze względu na ochronę tajemnicy zawodowej czy zapobieganie naruszeniom zasad etyki w takich zawodach. Ochrona tajemnicy zawodowej oraz zapobieganie naruszeniom zasad etyki w zawodach regulowanych mogą zatem stanowić przesłankę uzasadniającą wprowadzenie ograniczeń lub wyłączeń stosowania niektórych przepisów RODO.

Artykuł 14 ust. 5 lit. d) RODO wprost stanowi, że obowiązek informacyjny w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, nie znajdzie zastosowania w zakresie, w jakim dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Radca prawny i adwokat, którzy związani są ustawowym obowiązkiem zachowania tajemnicy, są zatem zwolnieni z obowiązku informowania osoby, której dane dotyczą, w przypadku gdy pozyskali jej dane w sposób niebezpośredni. Tytułem przykładu: jeżeli radca prawny lub adwokat uzyskał dane osobowe świadków czy innych stron postępowania np. od klienta bądź z ogólnodostępnych baz danych czy rejestrów, nie będzie musiał spełniać wobec takich osób obowiązku informacyjnego.

Również gdyby osoba trzecia (osoba, której dane dotyczą) w zakresie, w jakim wobec niej radcę prawnego lub adwokata obowiązuje tajemnica zawodowa, zażądała na podstawie art. 15 RODO, udostępnienia informacji o przetwarzaniu jej danych osobowych lub kopii jej danych osobowych, to radca prawny lub adwokat odmawia ujawnienia tych informacji lub kopii z powołaniem się na prawo swojego klienta do zachowania w tajemnicy jego danych osobowych, co znajduje podstawę w art. 15 ust. 4 RODO.

RODO przewiduje jednocześnie możliwość ograniczenia uprawnień organów nadzorczych do uzyskania od administratora lub podmiotu przetwarzającego dostępu do danych osobowych oraz do pomieszczeń (art. 58 ust. 1 lit. e) i f) RODO) na gruncie krajowych przepisów szczególnych wobec administratorów lub podmiotów przetwarzających, którzy podlegają obowiązkowi zachowania tajemnicy zawodowej (art. 90 RODO). W związku z tym w projektach nowelizacji UPoA oraz URP przewiduje się stosowne wyłączenie powyższych kompetencji organu nadzorczego w zakresie mogącym naruszyć tajemnicę zawodową radcy prawnego lub adwokata.

Wprowadzenie ograniczenia uprawnień organu nadzorczego jest dopuszczalne wyłącznie w przypadku, gdy:

- jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy;
- dotyczy wyłącznie danych osobowych, które administrator lub podmiot przetwarzający otrzymał lub pozyskał w wyniku lub w ramach działania objętego tym obowiązkiem zachowania tajemnicy.

Warto jednocześnie wskazać, że zapobieganie naruszeniom zasad etyki w zawodach regulowanych, prowadzenie postępowań w takich sprawach, ich wykrywanie oraz ściganie może stanowić podstawę wprowadzenia ograniczeń na podstawie art. 23 ust. 1 RODO (art. 23 ust. 1 lit. g) RODO).

W przypadku radcy prawnego oraz adwokata przepis ten może stanowić podstawę do wprowadzenia dalszych ograniczeń w przypadku przetwarzania przez nich danych osobowych w związku z dokonywanymi przez te podmioty czynnościami zawodowymi czy prowadzonymi przeciwko nim postępowaniami dyscyplinarnymi, jak również ma związek z ochroną tajemnicy zawodowej.

W szczególności to, iż radca prawny i adwokat są zobowiązani do zachowania tajemnicy zawodowej (tj. wszystkiego, o czym dowiedzieli się podczas wykonywania zawodu) na mocy ustaw zawodowych i odpowiednich kodeksów etyki, nie zwalnia ich z obowiązków wynikających z innych przepisów o ochronie danych osobowych. Przepisy dotyczące tajemnicy radcowskiej i adwokackiej stanowią uzupełnienie przepisów RODO i ich nie zastępują.

Tajemnica zawodowa a status radcy prawnego i adwokata w procesie przetwarzania danych osobowych

Warto wreszcie również podkreślić, że obowiązek zachowania tajemnicy zawodowej wpływa na status radcy prawnego i adwokata w procesie przetwarzania danych osobowych.

Ochrona tajemnicy wymaga od radcy prawnego i adwokata podejmowania samodzielnych decyzji w odniesieniu do informacji objętych tajemnicą, w tym danych osobowych przetwarzanych w ramach wykonywania zawodu. W tym zakresie nie może on być zależny od decyzji innego podmiotu, w tym także swojego klienta.

Z faktu związania tajemnicą zawodową wynika zatem, że radca prawny lub adwokat, jako depozytariusz tajemnicy, nie może być uznany za podmiot przetwarzający, tj. podmiot podporządkowany w zakresie przetwarzania danych osobowych decyzjom administratora (np. klienta). Role powiernika tajemnicy zawodowej oraz podmiotu przetwarzającego pozostają nie do pogodzenia ze sobą, gdy chodzi o ochronę zasad dotyczącej każdej z tych ról.

4. Podstawowe zasady ochrony danych osobowych

4.1 Zasady dotyczące przetwarzania danych osobowych (art. 5 RODO)

Ogólne omówienie

Wszystkie czynności przetwarzania danych powinny być zgodne z podstawowymi zasadami dotyczącymi przetwarzania danych osobowych, wskazanymi w art. 5 RODO. Są to:

- zasada zgodności z prawem, rzetelności i przejrzystości;
- zasada ograniczenia celu;
- zasada minimalizacji danych;
- zasada prawidłowości danych;
- zasada ograniczenia przechowywania;
- zasada integralności i poufności;
- zasada rozliczalności.

Zasada zgodności z prawem, rzetelności i przejrzystości

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Zgodność z prawem przetwarzania oznacza, że podstawą prawną przetwarzania jest jedna z przesłanek wymienionych w art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO, a także, że przetwarzanie jest zgodne z innymi przepisami o ochronie danych osobowych. Rzetelność przetwarzania interpretuje się jako jego ogólną uczciwość oraz proporcjonalność ingerencji w prywatność związaną z przetwarzaniem danych osobowych. Aby natomiast zachować zasadę przejrzystości, należy przekazywać osobom, których dane dotyczą, zrozumiałe i kompletne informacje na temat przetwarzania ich danych osobowych. Dodatkowe wymogi dotyczące zasady przejrzystości sformułowano w art. 12 RODO. Zgodnie z tym przepisem wszelkie informacje i komunikaty przekazywane osobom, których dane dotyczą, powinny być łatwo dostępne i zrozumiałe oraz napisane jasnym i prostym językiem. Celem tej zasady jest zapewnienie, aby osoby, których dane dotyczą, miały pełną wiedzę na temat operacji przetwarzania, w tym konsekwencji przetwarzania ich danych oraz przysługujących im praw związanych z przetwarzaniem danych osobowych.

Zasada ograniczenia celu

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Zasada ograniczenia celu wymusza, po pierwsze, wskazanie określonego, zgodnego z prawem celu przetwarzania w momencie zbierania danych. Po drugie, zgodnie z tą zasadą zabronione jest przetwarzanie w innym celu, chyba że: (i) dalsze przetwarzanie odbywa się na podstawie przepisów prawa unijnego lub prawa krajowego, (ii) administrator uzyskał zgodę osoby, której dane dotyczą, na dalsze przetwarzanie, lub (iii) taki wtórny cel przetwarzania nie jest niezgodny z celem pierwotnym. Zgodność wtórnego celu przetwarzania z celem pierwotnym ocenia się m.in. na podstawie kryteriów wskazanych w art. 6 ust. 4 RODO, takich jak wszelkie związki między celami, kontekst, w którym zebrano dane osobowe, charakter danych osobowych, a także ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą. Na mocy art. 5 ust. 1 lit. b) RODO dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uważane za niezgodne z pierwotnym celem przetwarzania.

Zasada minimalizacji danych

Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Zgodnie z tą zasadą administrator danych może zbierać tylko takie dane osobowe, które są mu konieczne do osiągnięcia celu ich zebrania. Zakazane jest zatem zbieranie danych niepotrzebnych w konkretnym celu, czy też zbieranie danych „na zapas". Zasada ta powiązana jest z zasadą ograniczenia celu, ponieważ to cel przetwarzania determinuje zakres danych potrzebnych do osiągnięcia tego celu.

Zasada prawidłowości danych

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane.

Powyższa zasada odnosi się do poprawności danych i ich zgodności z prawdą. Zgodnie z zasadą prawidłowości danych, jakiekolwiek nieprawidłowe (niepoprawne, nieprawdziwe) dane osobowe powinny być jak najszybciej usunięte lub poprawione.

Zasada ograniczenia przechowywania

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Zgodnie z zasadą ograniczenia przechowywania, przetwarzanie danych osobowych jest dopuszczalne tylko tak długo, jak jest to konieczne do osiągnięcia celów przetwarzania danych. Zakazane jest bowiem przechowywanie danych osobowych w nieskończoność. W konsekwencji administratorzy muszą ustalić okresy przechowywania danych lub – gdy ustalenie z góry okresu przechowywania nie jest możliwe – kryteria ustalania takich okresów.

Na podstawie art. 5 ust. 1 lit. e) RODO dopuszczalne jest przechowywanie danych osobowych po osiągnięciu (pierwotnych) celów przetwarzania, pod warunkiem że dane będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Przetwarzanie danych w tych celach po upływie pierwotnego okresu

przetwarzania wymaga jednak wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony praw i wolności osób, których dane dotyczą.

Zasada integralności i poufności

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Powyższa zasada nakłada na podmioty przetwarzające dane osobowe obowiązek odpowiedniego zabezpieczenia danych osobowych, tak aby zachowane zostały właściwości integralności i poufności danych.

Zasada rozliczalności

Zgodnie z zasadą rozliczalności administrator danych jest odpowiedzialny za przestrzeganie zasad przetwarzania danych oraz musi być w stanie wykazać ich przestrzeganie. Konieczne jest zatem wdrożenie odpowiednich wewnętrznych procedur w celu spełniania wymogów RODO oraz stworzenie dokumentacji, dzięki której można wykazać (udowodnić) spełnianie tych wymogów.

4.2 Podstawy prawne przetwarzania danych osobowych

Ogólne omówienie

Zgodnie z zasadą zgodności z prawem przetwarzanie danych osobowych musi być oparte o podstawę prawną wskazaną w RODO. W zależności od rodzaju danych osobowych zastosowanie mogą mieć różne przesłanki legalizujące przetwarzanie: inne podstawy przetwarzania mają zastosowanie do szczególnych kategorii danych, a inne – do tzw. danych zwykłych oraz danych dotyczących wyroków skazujących i naruszeń prawa (rodzaje danych osobowych omówiono w podrozdziale 2.1).

Poniżej wymienione są wszystkie możliwe podstawy prawne przetwarzania danych osobowych. Natomiast podstawy prawne mające zastosowanie do przetwarzania danych przez radcę prawnego lub adwokata przedstawiono w następnym podrozdziale.

Tzw. dane zwykłe

Podstawy prawne przetwarzania tzw. danych zwykłych uregulowano w art. 6 ust. 1 RODO. Zgodnie z tym przepisem przetwarzanie danych jest legalne, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

1) Osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.

Zgoda taka musi być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego,

przyzwala na przetwarzanie dotyczących jej danych osobowych (zgodnie z definicją zgody zawartą w art. 4 pkt 11 RODO).

2) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

W tym kontekście należy zwrócić szczególną uwagę na kryterium niezbędności danych do zawarcia lub wykonania umowy – pojęcie to powinno być interpretowane wąsko. Jeżeli zatem jakaś informacja nie jest potrzebna do zawarcia lub wykonywania umowy, podstawą jej przetwarzania nie może być powyższa przesłanka.

3) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

W tym przypadku podstawa prawna przetwarzania musi być określona w prawie unijnym lub w prawie krajowym, a cel przetwarzania powinien wynikać z tych przepisów.

4) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

5) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

W tym przypadku podstawa prawna przetwarzania musi być określona w prawie unijnym lub w prawie krajowym, a celem przetwarzania powinno być wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

6) Przetwarzanie jest 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, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Jeżeli przetwarzanie danych ma być oparte o powyższą przesłankę, konieczne jest przeprowadzenie tzw. testu równowagi, czyli analizy, czy w danej sytuacji interes administratora w przetwarzaniu danych jest nadrzędny wobec interesów, praw i wolności osoby fizycznej.

Dane dotyczące wyroków skazujących i naruszeń prawa

Podstawy prawne przetwarzania danych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa są takie same, jak wymienione wyżej podstawy przetwarzania danych zwykłych.

Jednakże zgodnie z art. 10 RODO przetwarzania tych danych *wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą*. Brzmienie tego przepisu sugeruje, że należy brać pod uwagę przepisy prawa krajowego dotyczące przetwarzania danych o wyrokach skazujących i naruszeniach prawa.

Szczególne kategorie danych

Przetwarzanie szczególnych kategorii danych (np. danych o stanie zdrowia, danych ujawniających pochodzenie etniczne lub poglądy religijne) jest co do zasady zabronione.

Na zasadzie wyjątku od ogólnego zakazu przetwarzanie szczególnych kategorii danych dozwolone jest w następujących przypadkach:

1) Osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach.

2) Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem unijnym bądź krajowym lub porozumieniem zbiorowym na mocy prawa krajowego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.

3) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

4) Przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą.

5) Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

6) Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

7) Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa unijnego lub krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

8) Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa unijnego lub krajowego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem dodatkowych warunków i zabezpieczeń.

9) Przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa unijnego lub krajowego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

10) Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa unijnego lub krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

4.3 Podstawy przetwarzania danych osobowych przez radcę prawnego lub adwokata

Podstawy prawne przetwarzania tzw. danych zwykłych przez radcę prawnego lub adwokata

W ramach wykonywania zawodu przez radcę prawnego lub adwokata znajdą zastosowanie w szczególności następujące przesłanki:

1) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit. b) RODO).

2) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) RODO).

3) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d) RODO).

4) Przetwarzanie jest 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, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f) RODO).

Przesłanka z art. 6 ust. 1 lit. b) RODO znajdzie zastosowanie w ramach wykonywania zawodu przez radcę prawnego lub adwokata w zakresie, w jakim przetwarzanie danych jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą. W praktyce oznacza to, że przetwarzanie danych

klienta jest dopuszczalne w takim zakresie, w jakim jest ono niezbędne do wykonania umowy. Poprzez wykonanie umowy należy rozumieć realizację praw i obowiązków, które mają swoje źródło w umowie lub w przepisach uzupełniających treść umowy. Podstawa ta obejmuje przetwarzanie danych przez radcę prawnego lub adwokata w związku z udzielaniem porad prawnych czy sporządzaniem opinii prawnych. Ta podstawa będzie również właściwa do przetwarzania danych zleceniobiorców i dostawców towarów lub usług potrzebnych do funkcjonowania kancelarii.

Przesłanka z art. 6 ust. 1 lit. c) RODO znajdzie zastosowanie w ramach wykonywania zawodu przez radcę prawnego lub adwokata w zakresie, w jakim przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. W przypadku działalności prowadzonej przez radcę prawnego lub adwokata chodzi w szczególności o przepisy proceduralne wskazujące zakres danych, który powinien być podany w związku z konkretną czynnością procesową, np.:

- art. 126 § 1 i 2 KPC, który określa zakres danych osobowych wymaganych w piśmie procesowym w postępowaniu cywilnym;
- art. 63 § 2–3a KPA, który określa zakres danych osobowych wymaganych w piśmie w postępowaniu administracyjnym (żądaniu, wyjaśnieniu, odwołaniu, zażaleniu).

Ponadto na tej podstawie prawnej adwokat lub radca prawny będzie przykładowo przetwarzał dane swoich pracowników w związku z art. 22^1 § 1 i 2 KP, który określa zakres danych przetwarzanych legalnie przez pracodawcę.

Przesłanka z art. 6 ust. 1 lit. d) RODO znajdzie zastosowanie w ramach wykonywania zawodu przez radcę prawnego lub adwokata w zakresie, w jakim przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej. Jak wynika z motywu 46 RODO, żywotny interes innej osoby fizycznej powinien być zasadniczo podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania nie da się oprzeć na innej podstawie prawnej. W przypadku ustania przyczyny wywołującej brak zdolności fizycznej lub prawnej (np. ustanie choroby) należy poszukiwać innej podstawy prawnej legitymizującej przetwarzanie. Szczegółowo przesłankę tę omówiono w podrozdziale dotyczącym przetwarzania szczególnych kategorii danych (art. 9 ust. 2 lit. c) RODO).

Przesłanka z art. 6 ust. 1 lit. f) RODO znajdzie zastosowanie w ramach wykonywania zawodu przez radcę prawnego lub adwokata w szczególności w przypadku przetwarzania danych osobowych w celu zapobiegania oszustwom, zapewnienia bezpieczeństwa sieci i informacji bądź dochodzenia roszczeń (np. przetwarzanie danych w celu zlecenia podmiotowi zewnętrznemu wyegzekwowania należności z niezapłaconej przez klienta faktury).

Podstawy prawne przetwarzania danych dotyczących wyroków skazujących i naruszeń prawa przez radcę prawnego lub adwokata

Jak już wskazano w podrozdziale 4.2., podstawy prawne przetwarzania danych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa są takie same jak podstawy przetwarzania danych zwykłych. W konsekwencji jeżeli radca prawny lub adwokat w ramach wykonywania zawodu będzie przetwarzał dane dotyczące wyroków skazujących oraz naruszeń prawa, to podstawy legalizacyjnej należy szukać w art. 6 ust. 1 RODO. Przetwarzania tego rodzaju danych

dokonują w szczególności radcy prawni i adwokaci, którzy specjalizują się w reprezentowaniu klientów w postępowaniach karnych w roli zarówno obrońcy, jak i pełnomocnika.

Przetwarzania takich danych można dokonywać pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Przetwarzanie danych pod nadzorem nie oznacza, że podmiot nadzorujący musi być administratorem danych o wyrokach skazujących lub naruszeniach, a w konsekwencji można uznać, że przetwarzanie danych przez radcę prawnego lub adwokata odbywa się pod nadzorem ministra sprawiedliwości oraz właściwego samorządu zawodowego.

Podstawy prawne przetwarzania szczególnych kategorii danych przez radcę prawnego lub adwokata

Jak już wskazano w podrozdziale 4.1, przetwarzanie szczególnych kategorii danych jest co do zasady zabronione. Jednakże w działalności radcy prawnego lub adwokata bezsprzecznie dochodzi do sytuacji, w których konieczne jest przetwarzanie danych takich jak dane dotyczące zdrowia, dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przynależność do związku zawodowego, przekonania religijne lub światopoglądowe.

W ramach wykonywania zawodu radca prawny lub adwokat w zależności od kontekstu przetwarzania może je oprzeć o jedną z następujących podstaw prawnych:

1) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 9 ust. 2 lit. c) RODO);
2) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy (art. 9 ust. 2 lit. f) RODO).

Przesłanka z art. 9 ust. 2 lit. c) RODO dotyczy sytuacji, gdy osoba, której dane dotyczą, ze względów fizycznych (np. choroby zakaźnej, psychicznej lub stanu śpiączki) lub też prawnych (np. brak zdolności do czynności prawnych ze względu na ubezwłasnowolnienie całkowite) nie może wyrazić zgody na przetwarzanie swoich danych osobowych. Przez żywotne interesy należy rozumieć interesy o dużym znaczeniu, takie jak zdrowie, życie, a w pewnych przypadkach nawet interesy majątkowe. Są to takie interesy, które przeważają nad interesami nakazującymi zachowanie danych osobowych w poufności. Jak wynika z motywu 46 RODO, żywotny interes innej osoby fizycznej powinien być zasadniczo podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania nie da się oprzeć na innej podstawie prawnej. W przypadku ustania przyczyny wywołującej brak zdolności fizycznej lub prawnej (np. ustanie choroby) należy poszukiwać innej podstawy prawnej legitymizującej przetwarzanie szczególnych kategorii danych z art. 9 ust. 2 RODO.

Przesłanka z art. 9 ust. 2 lit. f) RODO dotyczy sytuacji, w których przetwarzanie danych osobowych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy. W ramach wykonywania zawodu przez radcę prawnego lub adwokata przesłanka ta zasługuje na szczególną uwagę. Jak wskazuje motyw 52, przesłanka ta obejmuje przetwarzanie danych osobowych, gdy jest ono niezbędne do ustalenia, dochodzenia lub obrony

roszczeń zarówno w postępowaniu sądowym, administracyjnym, jak i też innym postępowaniu pozasądowym.

5. Szczegółowe obowiązki administratora

5.1 Zastrzeżenie dotyczące możliwości ograniczenia obowiązków administratora związanych z uprawnieniami osób, których dane dotyczą, w prawie krajowym

Artykuł 23 RODO wprowadza możliwość ograniczenia w prawie państw członkowskich lub Unii Europejskiej zakresu niektórych obowiązków i praw przewidzianych w RODO.

Zgodnie z art. 23 ust. 1 RODO prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 (prawa osób, których dane dotyczą) i w art. 34 (zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych), a także w art. 5 RODO (zasady dotyczące przetwarzania danych osobowych) – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 RODO – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;

f) ochronie niezależności sądów i postępowania sądowego;

g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;

h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g);

i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;

j) egzekucji roszczeń cywilnoprawnych.

Chociaż art. 23 ust. 1 RODO dopuszcza możliwość ograniczenia określonych obowiązków i praw w drodze krajowych przepisów prawnych, to jednocześnie art. 23 ust. 2 RODO stawia podstawie prawnej takich ograniczeń szereg wymagań. Stosownie do tego przepisu podstawa prawna wprowadzająca

ograniczenia praw i obowiązków, o których mowa w art. 23 ust. 1 RODO, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

a) celach przetwarzania lub kategorii przetwarzania;

b) kategoriach danych osobowych;

c) zakresie wprowadzonych ograniczeń;

d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;

e) określeniu administratora lub kategorii administratorów;

f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

W przypadku radcy prawnego lub adwokata podstawę do ewentualnego ograniczenia obowiązków wynikających z RODO może w określonym zakresie stanowić art. 23 ust. 1 lit. e) (ważne cele leżące w ogólnym interesie publicznym), lit. g) (zapobieganie naruszeniom zasad etyki w zawodach regulowanych, prowadzenie postepowań w takich sprawach, ich wykrywanie oraz ściganie) oraz lit. h) RODO (funkcje kontrolne i regulacyjne związane ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. e) oraz g)).

Na podstawie art. 23 RODO w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r. proponuje się ograniczenie niektórych obowiązków radcy prawnego oraz adwokata wynikających z RODO, w zakresie, w jakim przetwarzają oni dane osobowe w ramach wykonywania zawodu.

Projekt, który wprowadza zmiany odpowiednio do URP oraz UPoA (projektowany art. 5a ust. 2 i 4 URP oraz art. 16a ust. 2 i 4 UPoA), przewiduje, że do przetwarzania danych osobowych przez radcę prawnego i adwokata w ramach wykonywania zawodu nie znajdą zastosowania następujące przepisy:

- art. 13 RODO (obowiązek informacyjny w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą);

- art. 14 RODO (obowiązek informacyjny w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą);

- art. 15 ust. 1 i 3 RODO (prawo dostępu oraz prawo do uzyskania kopii danych osobowych);

- art. 18 (prawo do ograniczenia przetwarzania);

- art. 19 RODO (obowiązek poinformowania o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania);

- art. 21 RODO (prawo do sprzeciwu wobec przetwarzania danych osobowych;

- art. 16 RODO (prawo do sprostowania danych), pod warunkiem że przepisy szczególne przewidują odrębny tryb sprostowania.

Należy wskazać, że proponowane w projekcie wyłączenia dotyczą jedynie przetwarzania danych osobowych w ramach wykonywania zawodu i jedynie takich danych osobowych, które są niezbędne do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień (projektowany art. 5a ust. 3 URP oraz art. 16a ust. 3 UPoA). W zakresie pozostałej działalności radca prawny lub adwokat nie będzie podlegał wymienionym powyżej wyłączeniom.

Oznacza to – przykładowo – że radca prawny czy adwokat będzie zobowiązany przekazać wszystkie informacje wymagane w art. 13 RODO swojemu pracownikowi.

Zwracamy jednocześnie uwagę, że prace nad PWUODO wciąż trwają i ostateczny zakres ograniczeń lub wyłączeń może ulec zmianie.

5.2 Obowiązki informacyjne

Ogólne omówienie obowiązku

Jednym z głównych obowiązków administratora danych na podstawie RODO jest przekazanie osobom, których dane dotyczą, informacji na temat przetwarzania ich danych osobowych.

Na podstawie art. 13 i 14 RODO można wyróżnić dwie sytuacje spełniania obowiązku informacyjnego:

- kiedy dane zbierane są bezpośrednio od osoby, której dane dotyczą (tę sytuację reguluje art. 13 RODO), oraz

- kiedy dane zbierane są od podmiotu trzeciego (tę sytuację reguluje art. 14 RODO).

W zależności od sposobu zbierania danych (bezpośrednio czy niebezpośrednio) różnią się:

- zakres informacji, które należy przekazać osobie, której dane dotyczą;

- moment przekazania informacji; oraz

- okoliczności wyłączające obowiązek informacyjny.

Katalog informacji, które należy przekazać osobie, której dane dotyczą, zostanie szczegółowo omówiony w dalszej części niniejszego podrozdziału.

Jeśli chodzi o moment spełnienia obowiązku informacyjnego, w sytuacji gdy dane zbierane są bezpośrednio od osoby, której dane dotyczą, administrator musi jej przekazać informacje dotyczące przetwarzania danych w momencie zbierania danych.

Natomiast jeżeli dane zbierane są od osoby trzeciej, wówczas zgodnie z art. 14 ust. 3 RODO obowiązek informacyjny powinien być spełniony w rozsądnym terminie po pozyskaniu danych osobowych, biorąc pod uwagę konkretne okoliczności przetwarzania danych osobowych, ale nie później niż w ciągu miesiąca od uzyskania danych. Jeżeli dane osobowe mają być wykorzystane do komunikacji z osobą, której dane dotyczą, wówczas obowiązek informacyjny należy spełnić przy pierwszej komunikacji z osobą, której dane dotyczą, nawet jeżeli nie upłynął jeszcze miesiąc od uzyskania danych. Podobnie jeżeli administrator planuje ujawnić dane osobowe innemu odbiorcy, obowiązek informacyjny powinien być spełniony najpóźniej przy pierwszym ujawnieniu danych, nawet jeżeli nie upłynął jeszcze miesiąc od uzyskania danych.

W przypadku gdy administrator zbiera dane bezpośrednio od osoby, której dane dotyczą, obowiązek informacyjny jest wyłączony tylko w jednej sytuacji – jeżeli osoba ta już dysponuje wszystkimi informacjami, które mają być jej przekazane na mocy art. 13 ust. 1–2 RODO.

Natomiast art. 14 ust. 5 RODO – dotyczący zbierania danych od podmiotu trzeciego – przewiduje cztery sytuacje, w których spełnienie obowiązku informacyjnego nie jest wymagane:

- osoba, której dane dotyczą, dysponuje już informacjami wymienionymi w art. 14 ust. 1–2 RODO;
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
- pozyskiwanie lub ujawnianie danych osobowych jest wyraźnie uregulowane prawem unijnym lub krajowym przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie unijnym lub krajowym, w tym ustawowym obowiązkiem zachowania tajemnicy.

Odniesienie do działalności radcy prawnego lub adwokata

Na podstawie przepisów RODO radca prawny lub adwokat będący administratorem danych musi spełniać obowiązek informacyjny w sytuacji, w której zbiera dane bezpośrednio od osoby, której dane dotyczą (chyba że osoba ta dysponuje już informacjami na temat przetwarzania jej danych). Mogą to być na przykład klienci, osoby reprezentujące klientów, pracownicy, dostawcy będący osobami fizycznymi.

Natomiast w przypadku zbierania danych osobowych od podmiotów trzecich, radca prawny lub adwokat nie będzie musiał spełniać obowiązku informacyjnego w takim zakresie, w jakim przekazane mu informacje muszą pozostać poufne w związku z tajemnicą radcowską lub adwokacką (na podstawie

art. 14 ust. 5 lit. d) RODO). Radca prawny lub adwokat nie będzie zatem musiał spełniać obowiązku wobec – przykładowo – osób fizycznych, których dane są przetwarzane w związku z prowadzeniem spraw klientów (np. inne strony postępowania sądowego lub administracyjnego, świadkowie, pełnomocnicy, biegli).

Wykonanie obowiązku

Poniżej wymieniono elementy obowiązku informacyjnego wraz z krótkim omówieniem niektórych z nich. Wskazano też elementy, których zawarcie jest wymagane tylko w przypadku zbierania danych od podmiotów trzecich.

Zgodnie z art. 13 ust. 1–2 i art. 14 ust. 1–2 RODO klauzula informacyjna powinna zawierać:

1) Tożsamość i dane kontaktowe administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe przedstawiciela.

Chodzi tutaj o wskazanie imienia i nazwiska lub nazwy administratora danych. Jako dane kontaktowe można podać np. adres siedziby, inny adres korespondencyjny, numer telefonu, adres email, adres strony internetowej.

2) Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych.

Jeżeli administrator danych wyznaczył inspektora ochrony danych, w klauzuli informacyjnej powinien podać jego dane kontaktowe. Może to być np. adres pocztowy, adres email, numer telefonu. Nie zachodzi obowiązek podawania imienia i nazwiska IOD w klauzuli informacyjnej.

3) Cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania.

Cele przetwarzania powinny być wyraźne, określone i zgodne z prawem. Należy wskazać wszystkie cele, dla których dane mogą być przetwarzane. Powinno się także wskazać podstawę prawną przetwarzania, przy czym chodzi tylko o te przesłanki legalizujące, które mają zastosowanie w danym przypadku.

4) Kategorie odnośnych danych osobowych.

Chodzi tutaj o podanie kategorii danych osobowych, które są przetwarzane. Ten element jest obowiązkowy tylko w sytuacji zbierania danych od podmiotu trzeciego. W takiej sytuacji osoba, której dane dotyczą, nie ma bowiem świadomości, jakie informacje o niej są przekazywane administratorowi. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba ta sama przekazuje dane administratorowi, a zatem zdaje sobie sprawę, jaki jest ich zakres.

5) Jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f) RODO) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią.

Konieczne jest określenie prawnie uzasadnionego interesu realizowanego przez administratora danych lub stronę trzecią, który to interes w ocenie administratora pozwala na przetwarzanie danych osobowych.

6) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

Należy pamiętać, że w rozumieniu RODO odbiorcami danych są nie tylko inni administratorzy, ale także podmioty przetwarzające dane osobowe w imieniu administratora (np. dostawcy usług IT). Definicja odbiorcy znajduje się w art. 4 pkt 9 RODO.

7) Gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub, w przypadku przekazania na podstawie odpowiednich zabezpieczeń (art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO), wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii dokumentu zabezpieczeń lub o miejscu udostępnienia danych.

Konieczne jest wskazanie państwa trzeciego lub organizacji międzynarodowej, do której będą przekazywane dane osobowe. Należy też podać podstawę prawną transferu, tj. decyzję Komisji Europejskiej w sprawie uznania państwa trzeciego lub organizacji międzynarodowej za zapewniającą odpowiedni stopień ochrony danych, lub tzw. odpowiednie zabezpieczenia. Odpowiednimi zabezpieczeniami mogą być np. standardowe klauzule ochrony danych, wiążące reguły korporacyjne, zatwierdzony kodeks postępowania. Ponadto w klauzuli informacyjnej należy wskazać, w jaki sposób osoba, której dane dotyczą, może uzyskać kopię dokumentu zabezpieczeń. Należy zwrócić uwagę, że w tym zakresie w polskim tłumaczeniu RODO znajduje się błąd, bowiem w przepisie art. 13 ust. 1 lit. f) RODO oraz art. 14 ust. 1 lit. f) RODO mowa jest o możliwości uzyskania kopii danych lub miejsce udostępnienia danych. Porównanie polskiej wersji językowej RODO do innych wersji językowych (angielskiej, francuskiej) pozwala jednak na ustalenie, że chodzi tutaj o kopię odpowiednich zabezpieczeń lub miejsce udostępnienia zabezpieczeń.

8) Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.

Jeżeli to możliwe, należy wskazać konkretny okres, przez który dane osobowe będą przetwarzane (np. 5 lat). Jeżeli ustalenie konkretnego okresu przetwarzania nie jest możliwe, należy podać kryteria ustalania okresu przechowywania danych (np. okres przedawnienia roszczeń).

9) Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.

Informację o prawach przysługujących osobie, której dane dotyczą, należy dostosować do okoliczności przetwarzania. W celu zachowania zasady przejrzystości osobę, której dane dotyczą, należy poinformować tylko o tych prawach, które będą miały do niej zastosowanie. Przykładowo, prawo

sprzeciwu stosuje się tylko wówczas, gdy podstawą przetwarzania danych jest prawnie uzasadniony interes lub wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Natomiast z prawa przenoszenia danych można korzystać tylko w sytuacji, gdy dane są przetwarzane w sposób zautomatyzowany.

10) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Informację o prawie do wycofania zgody należy zawrzeć tylko w sytuacji, gdy jest ona podstawą prawną przetwarzania danych.

11) Informacje o prawie wniesienia skargi do organu nadzorczego.

Aby zapewnić większą przejrzystość informacji, można wskazać nazwę organu nadzorczego, do którego można złożyć skargę związaną z przetwarzaniem danych osobowych.

12) Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Informację tę podaje się tylko w przypadku zbierania danych od podmiotów trzecich. Osoba, której dane dotyczą, musi być bowiem poinformowana, jaki podmiot przekazał administratorowi jej dane osobowe.

13) Informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Powyższą informację należy umieścić w klauzuli informacyjnej tylko w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą. Chodzi o to, aby osoba, której dane dotyczą, miała świadomość istnienia obowiązku podania przez nią danych osobowych oraz konsekwencji niepodania danych.

14) Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli dochodzi do zautomatyzowanego podejmowania danych osobowych, w klauzuli informacyjnej należy umieścić szczegółową informację o tym. Chodzi tutaj m.in. o przedmiot decyzji, konsekwencje decyzji, dane wykorzystywane do podjęcia decyzji, sposoby zakwestionowania decyzji.

Najczęstszym sposobem spełniania obowiązku informacyjnego jest sposób pisemny (za pośrednictwem informacji pisemnej), w tym elektronicznie. Dopuszczalne jest także spełnianie obowiązku informacyjnego ustnie.

Szczególnie w przypadku spełniania obowiązku informacyjnego w środowisku elektronicznym rekomenduje się stosowanie tzw. warstwowej klauzuli informacyjnej. W pierwszej warstwie przedstawione są w formie skrótowej podstawowe informacje dotyczące przetwarzania (np. sama nazwa administratora, krótko określony cel przetwarzania). Natomiast w warstwie szczegółowej podane są szczegółowe informacje dotyczące przetwarzania, zgodnie z treścią art. 13 ust. 1–2 albo art. 14 ust. 1–2 RODO. Dzięki temu osoba, której dane dotyczą, może się szybko zorientować, na czym ma polegać przetwarzanie jej danych osobowych – za pomocą warstwy podstawowej. Jednocześnie osoba, której dane dotyczą, może zapoznać się z pełną wersją klauzuli informacyjnej, jeżeli chce uzyskać bardziej szczegółowe informacje.

Załącznik

Załącznikiem do niniejszego poradnika jest wzór klauzuli informacyjnej z przykładem dotyczącym zbierania danych kandydata do pracy. Wzór klauzuli informacyjnej podzielony jest na warstwę podstawową i szczegółową zgodnie z powyższym opisem.

5.3 Obowiązki związane z realizacją uprawnień osób, których dane dotyczą

Rodzaje uprawnień osób, których dane dotyczą

Oprócz prawa do informacji, które zostało omówione powyżej, osobie, której dane dotyczą, przysługują uprawnienia, o których mowa w art. 15–22 RODO. Należą do nich:

- prawo dostępu, w tym prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu (art. 15 RODO);
- prawo do sprostowania lub uzupełnienia danych (art. 16 RODO);
- prawo do usunięcia danych („prawo do bycia zapomnianym") (art. 17 RODO);
- prawo do ograniczenia przetwarzania (art. 18 RODO);
- obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO);
- prawo do przenoszenia danych (art. 20 RODO);
- prawo do sprzeciwu (art. 21 RODO)
- prawo do niepodlegania zautomatyzowanej decyzji, w tym profilowaniu (art. 22 RODO).

Powyższe uprawnienia rodzą po stronie administratora określone obowiązki, w tym generalny obowiązek ułatwienia osobie, której dane dotyczą, wykonania przysługujących jej na mocy art. 15–22 RODO praw.

Jak wskazano w części 5.1, niektóre z obowiązków radcy prawnego lub adwokata związane z realizacją praw osób, których dane dotyczą, mogą zostać ograniczone lub wyłączone na gruncie polskiej ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 w zakresie, w jakim radca prawny lub adwokat przetwarza określone dane osobowe w ramach wykonywania zawodu.

Niemniej jednak wciąż nie jest znany ostateczny zakres wyłączeń, ponieważ nie doszło do uchwalenia stosownej ustawy, stąd poniżej pokrótce omówione zostaną wszystkie obowiązki przewidziane w RODO.

Należy przy tym pamiętać, że na gruncie projektu ustawy potencjalnemu wyłączeniu spod niektórych obowiązków przewidzianych w RODO radca prawny lub adwokat będzie podlegał jedynie w zakresie, w jakim przetwarza dane osobowe w związku z wykonywanym zawodem (świadczeniem pomocy prawnej), tj. dane osobowe klientów, osób reprezentujących klientów będących osobami prawnymi lub tzw. ułomnymi osobami prawnymi, w tym osób kontaktowych, oraz innych osób fizycznych, których dane są przetwarzane w związku z prowadzeniem spraw klientów.

Przetwarzanie danych osobowych w związku z funkcjonowaniem kancelarii prawnej lub spółki (tj. danych osobowych pracowników, stałych współpracowników, osób współpracujących sporadycznie, dostawców towarów i usług) nie będzie podlegać takim ograniczeniom.

Tryb realizacji uprawnień

RODO określa nie tylko rodzaje uprawnień przysługujących osobom, których dane dotyczą, lecz również tryb, w jakim administrator powinien je realizować. Artykuł 12 RODO wskazuje, w jaki sposób administrator powinien prowadzić komunikację z podmiotami danych, oraz wprowadza terminy, w jakich administrator zobowiązany jest do podjęcia działań w odpowiedzi na żądanie podmiotu danych dotyczące przyznanych mu praw.

Komunikacja z osobą, której dane dotyczą

Przede wszystkim administrator, komunikując się z osobą, której dane dotyczą, w zakresie przysługujących jej na mocy art. 15–22 RODO uprawnień, powinien udzielać jej niezbędnych informacji w zwięzłej, przejrzystej i łatwo zrozumiałej formie. Powinien używać jasnego i prostego języka oraz unikać skomplikowanych struktur językowych, tak aby dla osoby, której dane dotyczą, jasny był sens kierowanego do niej komunikatu.

Administrator może udzielić informacji osobie, której dane dotyczą, na piśmie lub w inny sposób, w tym elektronicznie. Na wyraźne żądanie osoby, której dane dotyczą, administrator może udzielić jej informacji ustnie, pod warunkiem że potwierdzi jej tożsamość w inny sposób (tj. nie ustnie). Co do zasady jeżeli osoba, której dane dotyczą, zgłasza swoje żądanie na podstawie art. 15–22 RODO elektronicznie, to administrator powinien udzielić jej odpowiedzi w tej samej formie, chyba że osoba ta zażąda innej formy.

Terminy odpowiedzi na żądania osób, których dane dotyczą

W odpowiedzi na żądanie osoby, której dane dotyczą, administrator powinien bez zbędnej zwłoki – nie później jednak niż w terminie jednego miesiąca od otrzymania żądania – udzielić jej informacji o działaniach podjętych w związku z tym żądaniem.

Administrator powinien zatem w terminie jednego miesiąca dokonać oceny zasadności żądania i je zrealizować (np. dokonać sprostowania danych) lub odmówić realizacji.

Ze względu na skomplikowany charakter żądania lub liczbę żądań, jednomiesięczny termin można wydłużyć o dodatkowe dwa miesiące. Administrator ma zatem maksymalnie trzy miesiące na udzielenie odpowiedzi na żądanie podmiotu danych.

Powinien on jednak poinformować osobę, której dane dotyczą, o przedłużeniu terminu i jego przyczynach w ciągu jednego miesiąca od otrzymania żądania.

Jeżeli w związku z żądaniem osoby, której dane dotyczą, administrator nie podejmuje żadnych działań, to zobowiązany jest do niezwłocznego (najpóźniej w terminie jednego miesiąca od otrzymania żądania) poinformowania osoby, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Weryfikacja tożsamości osoby zgłaszającej żądanie

Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej, która zgłasza żądanie na podstawie art. 15–22 RODO, może zażądać od niej dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.

Możliwość pobierania opłat

Co do zasady komunikacja i działania podejmowane na podstawie art. 15–22 RODO przez administratora są wolne od opłat. Od tej zasady RODO przewiduje dwa wyjątki. Jeżeli żądania osoby, której dane dotyczą, są (i) ewidentnie nieuzasadnione lub (ii) nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
- odmówić podjęcia działań w związku z żądaniem.

Ciężar wykazania, że zgłoszone żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

Jeżeli administrator zdecydował się odmówić podjęcia działań objętych treścią żądania, powinien wskazać przyczyny takiej decyzji i poinformować o nich osobę, która zgłosiła żądanie.

Odmowa realizacji żądania osoby, której dane dotyczą

Administrator może odmówić podjęcia działań w odpowiedzi na żądanie osoby, której dane dotyczą, w dwóch przypadkach:

1) jeśli mają one ewidentnie nieuzasadniony lub nadmierny charakter; lub

2) jeżeli administrator dokonuje przetwarzania niewymagającego identyfikacji i wykaże, iż nie jest w stanie zidentyfikować występującej z takim żądaniem osoby.

5.4 Zakres obowiązków radcy prawnego lub adwokata związanych z realizacją praw osób, których dane dotyczą

Prawo dostępu do danych osobowych (art. 15 RODO)

Ogólne omówienie obowiązku

Zgodnie z art. 15 RODO osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do tych danych oraz następujących informacji:

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości – planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe – kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

i) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej – informacje o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Elementem prawa dostępu jest także również prawo do uzyskania od administratora kopii danych osobowych podlegających przetwarzaniu. Co do zasady realizacja prawa do uzyskania kopii danych osobowych nie powinna wiązać się z koniecznością ponoszenia opłat przez osobę, której dane dotyczą. Niemniej jednak administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych za wszelkie kolejne kopie, o które zwróci się podmiot danych. Realizując prawo dostępu do danych osobowych, osoba, której dane dotyczą, może uzyskać kopię danych osobowych we wskazanym przez siebie formacie. Jeżeli jednak zwróci się ona o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, administrator udziela informacji powszechnie stosowaną drogą elektroniczną. Prawo do uzyskania kopii nie może jednak niekorzystnie wpływać na prawa i wolności innych.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat będący administratorem jest zobowiązany do realizacji uprawnień osoby, której dane dotyczą, wskazanych w art. 15 RODO.

Odnosząc się natomiast do zakresu danych osobowych przetwarzanych w ramach wykonywania zawodu, należy wskazać, że w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego obowiązku (art. 15 ust. 1 i 3 RODO). Najprawdopodobniej zatem radca prawny i adwokat będą zwolnieni z obowiązku realizacji żądań w tym zakresie.

Wykonanie obowiązku

W odniesieniu do danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki, w zależności od zakresu żądania osoby, której dane dotyczą, radca prawny lub adwokat jako administrator danych zobowiązany jest do:

- udzielenia osobie, której dane dotyczą, informacji, czy przetwarzane są jej dane osobowe, a także innych informacji wskazanych w art. 15 ust. 1–2 RODO;
- udzielenia tej osobie dostępu do tych danych;
- dostarczenia tej osobie kopii danych osobowych podlegających przetwarzaniu.

W zakresie prawa do uzyskania kopii radca prawny lub adwokat powinien zweryfikować, czy realizacja tego uprawnienia nie będzie niekorzystnie wpływać na prawa i wolności innych osób, i na tej podstawie zdecydować o realizacji albo odmowie realizacji tego prawa.

Jeżeli radca prawny bądź adwokat nie przetwarza danych osobowych osoby, która zgłasza żądanie, musi ją o tym poinformować (tj. nie może pozostawić jej żądania bez odpowiedzi).

Jeżeli żądanie osoby, której dane dotyczą, obejmuje dane osobowe przetwarzane w ramach wykonywania zawodu, a ustawa zwolni radcę prawnego albo adwokata z realizacji obowiązku

związanego z prawem dostępu do danych w tym zakresie, to radca prawny lub adwokat nie będzie musiał dokonywać czynności, o których mowa powyżej.

Jednak nawet jeżeli radca prawny czy adwokat będzie zwolniony z omawianego obowiązku na mocy ustawy, w każdym przypadku należy poinformować osobę, która wniosła żądanie, o rozstrzygnięciu jej żądania, w tym o przyczynach ewentualnej odmowy realizacji żądania, tj. np. zwolnieniu radcy prawnego bądź adwokata z obowiązku realizacji prawa dostępu w zakresie danych osobowych przetwarzanych w ramach wykonywania zawodu.

Prawo do sprostowania lub uzupełnienia danych (art. 16 RODO)

Ogólne omówienie obowiązku

Zgodnie z art. 16 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Przepis ten przyznaje zatem osobie, której dane dotyczą, dwa typy uprawnień:

1) uprawnienie do sprostowania nieprawidłowych danych osobowych,

2) uprawnienie do uzupełnienia niekompletnych danych osobowych.

Związany z omawianym uprawnieniem obowiązek administratora nie ma charakteru bezwzględnego – administrator w określonych sytuacjach może odmówić sprostowania danych. Dla przykładu: stosownie do art. 11 ust. 2 RODO administrator nie musi realizować żądania sprostowania, jeżeli może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, a która zgłasza żądanie. W takiej sytuacji art. 16 RODO nie znajdzie zastosowania, chyba że osoba, której dane dotyczą, w celu wykonania przysługującego jej prawa dostarczy dodatkowe informacje, które pozwolą ją zidentyfikować.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat będący administratorem jest zobowiązany do sprostowania lub uzupełnienia danych osobowych na żądanie osoby, której dane dotyczą.

Natomiast w zakresie danych osobowych przetwarzanych w ramach wykonywania zawodu należy wskazać, że w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego obowiązku, w sytuacji gdy przepisy szczególne przewidują odrębny tryb sprostowania. Jeżeli natomiast przepisy szczególne nie przewidują odrębnego trybu sprostowania, radca prawny lub adwokat zobowiązany będzie sprostować dane osobowe objęte żądaniem zgodnie z RODO.

Wykonanie obowiązku

Jeżeli żądanie osoby, której dane dotyczą, obejmuje:

- dane osobowe przetwarzane w związku z funkcjonowaniem kancelarii prawnej lub spółki, jak również
- dane osobowe przetwarzane w ramach wykonywania zawodu, dla których przepisy szczególne nie przewidują odrębnego trybu sprostowania (przy założeniu, że projekt ustawy we wskazanym brzmieniu zostanie przyjęty),

a żądanie to jest uzasadnione, radca prawny lub adwokat jako administrator danych musi sprostować lub uzupełnić dane objęte żądaniem i poinformować o tym osobę, która wniosła żądanie. Jeżeli natomiast żądanie osoby, której dane dotyczą, jest nieuzasadnione, należy poinformować o tym osobę, która wniosła żądanie i wskazać przyczyny odmowy jego realizacji.

W przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu, jeżeli przepisy szczególne przewidują odrębny tryb sprostowania, radca prawny lub adwokat będzie musiał poinformować osobę, która wniosła żądanie, o przyczynach odmowy realizacji żądania, tj. o odrębnym trybie sprostowania danych osobowych przetwarzanych w ramach wykonywania zawodu przewidzianym w przepisach szczególnych.

Prawo do usunięcia danych („prawo do bycia zapomnianym") (art. 17 RODO)

Ogólne omówienie obowiązku

Artykuł 17 RODO przyznaje osobie, której dane dotyczą, prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, tzw. prawo do bycia zapomnianym. Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe objęte żądaniem, jeżeli:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane, lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi na mocy art. 21 ust. 1 RODO sprzeciw wobec przetwarzania danych osobowych jej dotyczących i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub wnosi na mocy art. 21 ust. 2 RODO sprzeciw wobec przetwarzania danych osobowych jej dotyczących na potrzeby marketingu bezpośredniego;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w przepisach prawa, którym podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

Jeżeli administrator upublicznił dane osobowe (np. opublikował je na ogólnodostępnej stronie internetowej), a na mocy art. 17 RODO ma obowiązek je usunąć, to zobowiązany jest do podjęcia rozsądnych działań, aby poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Obowiązek powiadomienia dotyczy przy tym nie tylko osób trzecich, którym dane zostały ujawnione przez administratora, ale także administratorów, którzy uzyskali dane w inny sposób (tj. z innego źródła niż administrator, na którym spoczywa obowiązek przekazania informacji).

Zgodnie z art. 17 ust. 3 RODO powyższe obowiązki są wyłączone w zakresie, w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy przepisów prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h)–i) oraz art. 9 ust. 3 RODO;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat będący administratorem jest zobowiązany do usunięcia danych na żądanie osoby, której dane dotyczą.

Natomiast w zakresie danych osobowych przetwarzanych w ramach wykonywania zawodu, należy wyróżnić dwie sytuacje:

1) jeżeli przetwarzanie danych osobowych objętych żądaniem jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń (art. 17 ust. 3 lit. d) RODO), radca prawny lub adwokat będący administratorem może skorzystać z wyłączenia przewidzianego w RODO, tj. nie będzie zobowiązany do usunięcia takich danych osobowych;

2) w pozostałych przypadkach, radca prawny lub adwokat byłby co do zasady zobowiązany do realizacji prawa do usunięcia danych w zakresie ustalonym w art. 17 RODO. Jak jednak wskazano powyżej, w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego uprawnienia w przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu. Najprawdopodobniej

zatem radca prawny i adwokat będą zwolnieni z obowiązku realizacji żądań usunięcia danych w tym zakresie.

Wykonanie obowiązku

W zakresie, w jakim radca prawny lub adwokat jako administrator danych będzie finalnie zobowiązany do realizacji prawa do usunięcia danych, w odpowiedzi na żądanie osoby, której dane dotyczą, będzie musiał zweryfikować, czy zachodzi przesłanka usunięcia danych osobowych (art. 17 ust. 1 lit. a)–f) RODO). Jeżeli tak, będzie zobowiązany do usunięcia danych osobowych objętych żądaniem. Jeżeli żadna z przesłanek nie znajdzie zastosowania, radca prawny lub adwokat będzie musiał poinformować o tym osobę, której dane dotyczą. Nawet jeżeli radca prawny lub adwokat będzie zwolniony z tego obowiązku na mocy ustawy, w każdym przypadku powinien poinformować osobę, która wniosła żądanie, o rozstrzygnięciu jej żądania, w tym o przyczynach ewentualnej odmowy jego realizacji.

Prawo do ograniczenia przetwarzania (art. 18 RODO)

Ogólne omówienie obowiązku

Na mocy art. 18 RODO osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania, jeżeli:

a) kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Zgodnie z art. 4 pkt 3 RODO przez ograniczenie przetwarzania należy rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Sprowadza się to do tego, że jeżeli przetwarzanie zostało ograniczone, to administrator nie może dokonywać na danych innych operacji niż przechowywanie.

Dane osobowe mogą być w takim przypadku przetwarzane wyłącznie:

- za zgodą osoby, której dane dotyczą, lub
- w celu ustalenia, dochodzenia lub obrony roszczeń, lub

- w celu ochrony praw innej osoby fizycznej lub prawnej, lub
- z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

W przypadku ograniczenia przetwarzania dane osobowe nie mogą być przetwarzane w celu, dla którego zostały zebrane.

Przed uchyleniem ograniczenia przetwarzania administrator zobowiązany jest do poinformowania o tym osobę, która zgłosiła żądanie ograniczenia przetwarzania.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat będący administratorem jest zobowiązany do ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą.

Natomiast w zakresie danych osobowych przetwarzanych w ramach wykonywania zawodu, jak wskazano powyżej, w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego obowiązku. Najprawdopodobniej zatem radca prawny i adwokat będą zwolnieni z obowiązku realizacji żądań w tym zakresie.

Wykonanie obowiązku

W przypadku gdy żądanie osoby, której dane dotyczą, obejmuje ograniczenie przetwarzania danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki (tj. poza wykonywaniem zawodu), a żądanie to jest uzasadnione (tj. spełnia przesłanki wskazane w art. 18 ust. 1 lit. a)–d) RODO), radca prawny lub adwokat jako administrator danych musi ograniczyć przetwarzanie danych osobowych, tj. nie może dokonywać na danych innych operacji niż przechowywanie, o czym informuje osobę zgłaszającą żądanie.

Jeżeli natomiast radca prawny lub adwokat uzna, że żądanie osoby, której dane dotyczą, nie jest uzasadnione, musi ją o tym poinformować i podać przyczyny odmowy realizacji jej żądania.

Z kolei jeżeli żądanie osoby, której dane dotyczą, obejmuje ograniczenie przetwarzania danych osobowych przetwarzanych w ramach wykonywania zawodu, a ustawa zwolni radcę prawnego lub adwokata z realizacji tego obowiązku, to radca prawny lub adwokat nie będzie musiał dokonywać ograniczenia przetwarzania. Będzie musiał natomiast poinformować tę osobę o przyczynach odmowy realizacji żądania, tj. o tym, że ustawa zwalnia go z realizacji prawa do ograniczenia przetwarzania w zakresie danych osobowych przetwarzanych w ramach wykonywania zawodu.

<u>Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO)</u>

Ogólne omówienie obowiązku

Na mocy art. 19 RODO jeżeli administrator dokona, na żądanie osoby, której dane dotyczą:

- sprostowania nieprawidłowych danych osobowych,
- uzupełnienia niekompletnych danych osobowych,
- usunięcia danych osobowych lub
- ograniczenia przetwarzania danych osobowych,

zobowiązany jest do poinformowania każdego odbiorcy, któremu ujawniono dane osobowe, o dokonanej zmianie. Przez odbiorcę danych rozumie się przy tym osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (w tym podmiotem przetwarzającym lub innym administratorem, któremu udostępniono dane osobowe). Odbiorcami danych nie są natomiast organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania na mocy przepisów prawa (np. sąd).

Obowiązek ten skorelowany jest z innym obowiązkiem administratora, wyrażonym w art. 5 ust. 1 lit. d) RODO, tj. zapewnieniem prawidłowości przetwarzanych danych osobowych, w tym również w zakresie, w jakim dane te zostały ujawnione odbiorcom. Stąd jeżeli treść lub zakres danych osobowych przetwarzanych przez administratora ulega zmianie, powinien o tym wiedzieć również odbiorca tych danych osobowych.

Obowiązek ten nie znajdzie jednak zastosowania, jeżeli powiadomienie okaże się niemożliwe lub będzie wymagać od administratora niewspółmiernie dużego wysiłku. Niemniej warto pamiętać, że ciężar wykazania, iż powiadomienie odbiorców jest niemożliwe lub wymaga niewspółmiernie dużego wysiłku, obciąża administratora.

Jednocześnie administrator zobowiązany jest również do poinformowania osoby, której dane dotyczą, o tych odbiorcach, jeżeli osoba ta tego zażąda.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat jako administrator danych jest zobowiązany do realizacji obowiązku z art. 19 RODO w następstwie dokonania sprostowania, usunięcia lub ograniczenia przetwarzania zgodnie z art. 16, art. 17 oraz art. 18 RODO.

W odniesieniu do danych osobowych przetwarzanych w ramach wykonywania zawodu, jak wskazano powyżej, w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego obowiązku. Najprawdopodobniej radca prawny i adwokat nie będą zatem zobowiązani do jego realizacji.

Wykonanie obowiązku

Radca prawny lub adwokat, który dokonał sprostowania, usunięcia lub ograniczenia przetwarzania zgodnie z art. 16, art. 17 oraz art. 18 RODO musi poinformować o tym każdego odbiorcę, któremu ujawnił dane osobowe, chyba że wykaże, iż takie poinformowanie jest niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Jest również zobowiązany w tym zakresie do poinformowania osoby, której dane dotyczą, na jej żądanie, o tych odbiorcach.

Prawo do przenoszenia danych (art. 20 RODO)

Ogólne omówienie obowiązku

Artykuł 20 RODO przyznaje osobie, której dane dotyczą, prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Prawo to znajduje zastosowanie, wyłącznie jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Prawo do przenoszenia danych nie może jednocześnie niekorzystnie wpływać na prawa i wolności innych osób. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych, o którym mowa w art. 17 RODO.

Prawo do przenoszenia danych nie znajdzie zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Odniesienie do działalności radcy prawnego lub adwokata

Radca prawny lub adwokat jako administrator danych osobowych jest zobowiązany do realizacji prawa do przenoszenia danych jedynie w sytuacji, gdy przetwarza dane osobowe na podstawie zgody lub umowy z osobą, której dane dotyczą, i wyłącznie pod warunkiem, że przetwarzanie to odbywa się w sposób zautomatyzowany. W ocenie autorów sytuacji, w których przetwarzanie danych osobowych przez radcę prawnego lub adwokata spełni obie przesłanki, będzie stosunkowo niewiele.

Wykonanie obowiązku

Jeżeli jednak obie przesłanki zostaną spełnione i radca prawny lub adwokat jako administrator danych będzie zobowiązany do realizacji prawa do przenoszenia danych, powinien on, w zależności od żądania osoby, której dane dotyczą:

- przekazać tej osobie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, jednak wyłącznie te, które sama dostarczyła administratorowi;
- przesłać te dane bezpośrednio innemu administratorowi, wskazanemu przez osobę, której dane dotyczą, o ile będzie to technicznie możliwe.

Jednocześnie radca prawny lub adwokat, spełniając obowiązek wynikający z prawa do przenoszenia danych, powinien zapewnić odpowiednie zabezpieczenia przekazywanym lub przesyłanym danym osobowym, w szczególności jeżeli są objęte tajemnicą zawodową (radcowską lub adwokacką).

Radca prawny lub adwokat musi również dokonać oceny, czy realizacja prawa do przenoszenia danych nie wpłynie niekorzystnie na prawa i wolności innych osób. Jeżeli dojdzie do wniosku, że realizacja tego prawa może niekorzystnie wpłynąć na prawa i wolności innych osób, to albo:

- odmówi realizacji żądania w pełnym zakresie i poinformuje o tym osobę, której dane dotyczą, wraz z podaniem przyczyn takiej odmowy, albo
- spełni żądanie tylko w zakresie, w jakim jego realizacja nie wpłynie niekorzystnie na prawa i wolności innych, i jednocześnie poinformuje o przyczynach odmowy realizacji żądania w pozostałym zakresie.

Prawo do sprzeciwu (art. 21 RODO)

Ogólne omówienie obowiązku

Artykuł 21 RODO przyznaje osobie, której dane dotyczą, uprawnienie do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych. Osoba, której dane dotyczą, może wnieść sprzeciw:

1) wobec przetwarzania danych osobowych, w tym profilowania, którego podstawą prawną jest:

    a) niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi bądź

    b) niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,

z przyczyn związanych z jej szczególną sytuacją. W razie wniesienia sprzeciwu administrator nie może już przetwarzać tych danych osobowych, chyba że wykaże on 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.

2) wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w dowolnym momencie, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania danych osobowych do celów marketingu bezpośredniego, administrator nie może ich dalej przetwarzać do takich celów.

3) wobec przetwarzania danych osobowych do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z przyczyn związanych z jej szczególną sytuacją, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Skorzystanie przez osobę, której dane dotyczą, z prawa do sprzeciwu co do zasady uniemożliwia przetwarzanie danych o osobie, której dane dotyczą.

W przypadku sprzeciwu wobec przetwarzania danych osobowych do celów marketingu bezpośredniego, w tym związanego z nim profilowania, administrator zobowiązany jest bezwzględnie do zaprzestania przetwarzania danych objętych sprzeciwem w celach marketingowych (art. 21 ust. 2 RODO). W pozostałych sytuacjach administrator może wykazać istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, które są nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń (art. 21 ust. 1 RODO) – dochodzi zatem do ważenia podstaw do przetwarzania, na które powołuje się administrator, z interesami, prawami i wolnościami osoby, której dane dotyczą.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, administrator wyraźnie informuje się ją o prawie do sprzeciwu, oraz przedstawia je jasno i odrębnie od wszelkich innych informacji.

Osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Odniesienie do działalności radcy prawnego lub adwokata

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki radca prawny lub adwokat jako administrator danych jest zobowiązany do realizacji obowiązku z art. 21 RODO.

W odniesieniu do danych osobowych przetwarzanych w ramach wykonywania zawodu, jak wskazano powyżej, w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 planuje się wyłączenie tego obowiązku. Najprawdopodobniej radca prawny i adwokat nie będą zatem zobowiązani do jego realizacji.

Wykonanie obowiązku

W odniesieniu do danych osobowych przetwarzanych w związku z funkcjonowaniem kancelarii prawnej lub spółki, jeżeli osoba, której dane dotyczą, zgłosiła sprzeciw na zasadach wskazanych w art.

21 ust. 2 RODO, radca prawny lub adwokat musi bezwzględnie zaprzestać przetwarzania objętych żądaniem danych osobowych w celach marketingowych.

W przypadkach pozostałych sprzeciwów radca prawny lub adwokat może albo uczynić zadość żądaniu i zaprzestać przetwarzania danych osoby zgłaszającej żądanie, albo dalej przetwarzać przedmiotowe dane osobowe, jeżeli stwierdzi i jest w stanie wykazać, że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

W każdym przypadku radca prawny lub adwokat musi jednocześnie poinformować osobę, której dane dotyczą, o sposobie realizacji jej żądania albo odmowie jego realizacji, podając przyczyny tej odmowy.

Jeżeli osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych, które wchodzą w zakres danych osobowych przetwarzanych w ramach wykonywania zawodu, radca prawny lub adwokat informuje tę osobę o tym, że jej żądanie nie zostanie zrealizowane ze względu na istniejące na mocy ustawy zwolnienie w tym zakresie.

Prawo do niepodlegania zautomatyzowanej decyzji, w tym profilowaniu (art. 22 RODO)

Ogólne omówienie obowiązku

Stosownie do art. 22 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która:

- opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, oraz
- wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Uprawnienie to nie znajdzie zastosowania, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadku gdy decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem lub gdy opiera się ona na wyraźnej zgodzie osoby, której dane dotyczą, administrator zobowiązany jest do wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

W przypadku szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, RODO przewiduje generalny zakaz podejmowania zautomatyzowanych decyzji w oparciu o takie dane. Niemniej jednak dozwolone jest zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach w oparciu o szczególne kategorie danych, pod warunkiem że istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a przetwarzanie takich danych odbywa się na podstawie art. 9 ust. 1 lit. a) RODO (wyraźna zgoda osoby, której dane dotyczą) lub art. 9 ust. 2 lit. g) RODO (przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym).

Odniesienie do działalności radcy prawnego lub adwokata

Podejmowanie decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu w rozumieniu art. 22 RODO, w ramach wykonywania zawodu radcy prawnego lub adwokata będzie dopuszczalne jedynie w przypadku, gdy taka decyzja:

- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W ocenie autorów radca prawny lub adwokat stosunkowo rzadko, o ile w ogóle, będzie dokonywać w ramach swojej działalności zautomatyzowanego przetwarzania danych osobowych i podejmować decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu.

Jeżeli jednak radca prawny czy adwokat będzie dokonywać takich czynności zgodnie z art. 22 ust. 2 RODO, będzie zobowiązany do realizacji obowiązku wynikającego z tego przepisu, jeżeli decyzja taka wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Wykonanie obowiązku

W ograniczonym zakresie, w jakim radca prawny lub adwokat podejmować będzie decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, będzie zobowiązany do realizacji prawa osoby, której dane dotyczą, do tego, by nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu. Jeżeli taka decyzja wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, radca prawny lub adwokat zobowiązany jest do zapewnienia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, w tym co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. W każdym przypadku radca prawny lub adwokat będzie zobowiązany do poinformowania osoby, która zgłosiła żądanie, o sposobie jego rozstrzygnięcia.

5.5 Powierzenie przetwarzania danych osobowych

Ogólne omówienie obowiązku

Powierzenie przetwarzania danych ma miejsce, jeżeli administrator zleca przetwarzanie danych w swoim imieniu innemu podmiotowi – tzw. podmiotowi przetwarzającemu (zwanemu też procesorem). Status podmiotu przetwarzającego omówiono szerzej w części 2.4.

Jeżeli administrator ma zamiar powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu, zgodnie z art. 28 RODO musi podjąć dwa rodzaje działań:

- W pierwszej kolejności administrator powinien zweryfikować, czy podmiot, któremu ma zamiar powierzyć przetwarzanie danych, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

- W przypadku pozytywnej weryfikacji administrator musi zawrzeć z podmiotem przetwarzającym umowę powierzenia przetwarzania. Umowa ta powinna zawierać wszystkie elementy określone w art. 28 ust. 3 RODO (omówione poniżej).

RODO nie zawiera żadnych przepisów wyłączających powyższe obowiązki.

Odniesienie do działalności radcy prawnego lub adwokata

Radca prawny lub adwokat – jako administrator danych – musi dokonać weryfikacji potencjalnego podmiotu przetwarzającego oraz zawrzeć z nim umowę zgodną z wymogami art. 28 ust. 3 RODO, jeżeli chce zlecić przetwarzanie danych podmiotowi przetwarzającemu. RODO nie przewiduje bowiem wyjątków od tych obowiązków. Przykładami sytuacji, w których dochodzi do powierzenia przetwarzania danych osobowych, są outsourcing usług wsparcia IT czy obsługi kadrowo-księgowej.

Wykonanie obowiązku

Pierwszym obowiązkiem związanym z powierzeniem przetwarzania jest weryfikacja potencjalnego podmiotu przetwarzającego. Sprawdzenie dotyczy tego, czy taki podmiot wdrożył odpowiednie środki techniczne i organizacyjne odpowiadające wymogom RODO. Ocena podmiotu powinna być dokonywana w szczególności w zakresie jego wiedzy fachowej, wiarygodności oraz zasobów. W praktyce weryfikacja podmiotu przetwarzającego może odbyć się poprzez przesłanie takiemu podmiotowi pytań dotyczących stosowania wymogów RODO (w tym zasobów, wiedzy fachowej i wiarygodności) oraz analizę przekazanych odpowiedzi. Można także przeprowadzić audyt w powyższym zakresie. Zgodnie z art. 28 ust. 5 RODO podmiot przetwarzający może wykazać zapewnianie wystarczających gwarancji wdrożenia RODO m.in. poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji. Na chwilę pisania niniejszego poradnika nie ma żadnych zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji.

Weryfikacja potencjalnego podmiotu przetwarzającego powinna być oczywiście dokonywana przed powierzeniem przetwarzania danych temu podmiotowi, tj. przed przekazaniem mu danych do przetwarzania.

Po pozytywnej weryfikacji podmiotu przetwarzającego administrator powinien zawrzeć z nim umowę. Zgodnie z art. 28 ust. 3 RODO umowa ta powinna zawierać następujące elementy:

- przedmiot przetwarzania;
- czas trwania powierzonego przetwarzania;
- charakter powierzonego przetwarzania;
- cel powierzonego przetwarzania;
- kategorie osób, których dane dotyczą, oraz rodzaj danych osobowych powierzonych do przetwarzania;
- zobowiązanie podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora;
- zobowiązanie podmiotu przetwarzającego do zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- zobowiązanie podmiotu przetwarzającego do podejmowania wszelkich środków wymaganych na mocy art. 32 RODO, tj. wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa danych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych;
- zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (tzw. subprocesora), o których mowa w art. 28 ust. 2 i 4 RODO, tj. obowiązku uzyskania szczegółowej lub ogólnej pisemnej zgody administratora na podpowierzenie danych podwykonawcy oraz obowiązku zawarcia umowy z podwykonawcą, która przewidywałaby takie same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym;
- zobowiązanie podmiotu przetwarzającego – biorąc pod uwagę charakter przetwarzania – do pomagania administratorowi, w miarę możliwości i poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III RODO;
- zobowiązanie podmiotu przetwarzającego – uwzględniając charakter przetwarzania oraz dostępne informacje – do pomagania administratorowi w wywiązywaniu się z obowiązków określonych w art. 32–36 RODO, tj. obowiązków związanych z szacowaniem ryzyka i doborem środków organizacyjnych i technicznych, obowiązków związanych ze zgłaszaniem naruszeń

organowi nadzorczemu i zawiadamianiem osób fizycznych dotkniętych naruszeniem o naruszeniu oraz obowiązków związanych z przeprowadzaniem oceny skutków dla ochrony danych;

- zobowiązanie podmiotu przetwarzającego do usunięcia lub zwrotu danych osobowych administratorowi oraz usunięcia wszelkich ich istniejących kopii po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, chyba że prawo unijne lub krajowe nakazuje przechowywanie danych osobowych;

- zobowiązanie podmiotu przetwarzającego do udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w RODO oraz umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniania się do nich;

- zobowiązanie podmiotu przetwarzającego do niezwłocznego informowania administratora, jeżeli zdaniem podmiotu przetwarzającego wydane mu polecenie stanowi naruszenie RODO lub innych przepisów unijnych lub krajowych o ochronie danych osobowych.

W art. 28 ust. 7 i 8 RODO przewidziana jest możliwość przyjęcia przez Komisję Europejską lub organ nadzorczy standardowych klauzul umownych dotyczących powierzenia przetwarzania. Na chwilę pisania niniejszego poradnika takich standardowych klauzul nie przyjęto.

Załącznik

Załącznikiem do niniejszego poradnika jest wzór umowy powierzenia przetwarzania danych.

5.6 Przetwarzanie danych na polecenie administratora

Ogólne omówienie obowiązku

W art. 29 RODO przewiduje się, że każda osoba działająca z upoważnienia administratora i mająca dostęp do danych osobowych przetwarza dane wyłącznie na polecenie administratora, chyba że inaczej wynika z wymogów określonych w przepisach prawa (prawa krajowego lub prawa Unii Europejskiej).

Bezpośrednio przepis ten wyznacza obowiązek każdej osoby wewnątrz jednostki organizacyjnej – niezależnie od rodzaju łączącego ją z administratorem stosunku prawnego – do wykonywania czynności na danych jedynie w zakresie poleceń administratora. Jednak wcześniej administrator musi ustalić, kto i w jakim zakresie pozostaje upoważniony do przetwarzania danych osobowych w jego jednostce organizacyjnej. Taki obowiązek ustalenia osób upoważnionych do przetwarzania danych osobowych wynika również z generalnej zasady integralności i poufności, zgodnie z którą przetwarzanie powinno się odbywać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f) RODO).

Odniesienie do działalności radcy prawnego lub adwokata

W swojej kancelarii radca prawny lub adwokat upoważnia w sferze wewnętrznej kancelarii osoby do przetwarzania danych osobowych, ustalając, kto i w jakim zakresie może mieć dostęp do danych osobowych i dalej je przetwarzać. Osoby przetwarzające dane osobowe w kancelarii (osoby upoważnione do przetwarzania danych) podlegają w tym względzie poleceniom radcy prawnego lub adwokata.

Wykonanie obowiązku

Jednym ze standardów zarządzania bezpieczeństwem informacji jest zapewnienie kontroli dostępu do informacji chronionej. Jako główne podstawy kontroli dostępu wskazuje się zasadę wiedzy koniecznej oraz zasadę potrzeby koniecznej:

1) zasada wiedzy koniecznej – osoba przetwarzająca powinna mieć zapewniony dostęp tylko do informacji potrzebnych jej do wykonywania powierzonych jej zadań (różne zadania w jednostce organizacyjnej oznaczają różną potrzebę wiedzy koniecznej do ich wykonania, a tym samym inny profil dostępu),
2) zasada potrzeby koniecznej – osoba przetwarzająca powinna mieć zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, aplikacji, procedur, pomieszczeń), które są jej niezbędne do wykonywania jej pracy (zadania) związanego z przetwarzaniem informacji prawnie chronionej.

Działania radcy prawnego lub adwokata powinny polegać na przypisaniu każdej osobie wykonującej czynności w kancelarii zadań, jakie ma wykonywać w procesie przetwarzania danych osobowych, i wyszczególnieniu zakresu danych osobowych, jaki jest niezbędny dla ich realizacji. Konsekwencją wyszczególnienia operacji na danych osobowych, jakie upoważniona osoba może wykonywać, jest działanie polegające na rejestracji upoważnionej osoby w systemie informatycznym i przypisaniu jej odpowiedniego profilu uprawnień w tym systemie.

W RODO bezpośrednio nie nakazuje się wprowadzania formalnych procedur upoważniania do przetwarzania danych osobowych oraz samego dokumentu upoważnienia do przetwarzania. Jednak administrator – w celu realizacji obowiązku i jego „rozliczenia" (art. 5 ust. 2 RODO) – może wprowadzić przedmiotową procedurę oraz wydawać dokument upoważnienia.

Załącznik

Wzór przykładowego dokumentu upoważnienia do przetwarzania danych osobowych stanowi załącznik.

5.7 Rejestrowanie czynności przetwarzania

Ogólne omówienie obowiązku

Obowiązek prowadzenia rejestru czynności określono w art. 30 RODO dla administratora (ust. 1) oraz dla podmiotu przetwarzającego (ust. 2). Celem prowadzenia rejestrów jest przede wszystkim:

1) w przypadku rejestru administratora – identyfikacja czynności przetwarzania, za które

administrator jest odpowiedzialny, oraz opis podstawowych zagadnień dotyczących tych czynności w celu zapewnienia zgodności z RODO;

2) w przypadku rejestru podmiotu przetwarzającego – identyfikacja administratorów oraz czynności przetwarzania, w związku z którymi nastąpiło powierzenie przetwarzania danych osobowych, wraz z podstawowymi informacjami dotyczącymi tych czynności w celu zapewnienia zgodności z RODO.

Zgodnie z art. 30 ust. 5 RODO obowiązek jest wyłączony w stosunku do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że występuje przynajmniej jedna z trzech wymienionych sytuacji: 1) przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą; 2) przetwarzanie nie ma charakteru sporadycznego; 3) przetwarzanie obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Odniesienie do działalności radcy prawnego lub adwokata

Radca prawny lub adwokat będący administratorem ma obowiązek prowadzenia rejestru czynności administratora, ponieważ nawet w przypadku zatrudnienia w kancelarii mniej niż 250 pracowników czynności przetwarzania nie mają charakteru sporadycznego, a w przypadku czynności związanych z wykonywaniem zawodu często dotyczą one danych szczególnie chronionych określonych w art. 9 i art. 10 RODO.

Wykonanie obowiązku

Przedmiotem rejestracji jest czynność przetwarzania danych, które to sformułowanie nie zostało zdefiniowane w RODO. Czynność przetwarzania danych to pewien ciąg czynności, który wyodrębnia się przede wszystkim ze względu na cel tych czynności: cel przetwarzania danych, kategorie osób, których dane dotyczą, i zakres przetwarzanych danych. Przykładowe czynności przetwarzania w działalności radcy prawnego oraz adwokata wskazano w podrozdziale 3.1.

W rejestrze czynności zamieszcza się obowiązkowo następujące rodzaje informacji dla każdej z czynności przetwarzania (zakres minimalny wpisów w rejestrze):

1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora;
2) imię i nazwisko lub nazwę oraz dane kontaktowe współadministratorów (jeżeli występują);
3) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (jeżeli został wyznaczony);
4) cele przetwarzania;
5) opis kategorii osób, których dane dotyczą;
6) zakres przetwarzanych danych osobowych dla określonej kategorii osób, których one dotyczą;
7) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
8) informacja o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
9) planowane terminy usunięcia poszczególnych kategorii danych (jeżeli jest to możliwe);

10) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych osobowych (jeżeli jest to możliwe).

W art. 30 ust. 1 RODO określono minimalne wymagane elementy rejestru, ale administrator prowadzący rejestr może wprowadzać do rejestru dodatkowe informacje w zależności od jego potrzeb, biorąc pod uwagę cel rejestru, jakim jest zapewnienie zgodności przetwarzania danych z RODO. We wzorze rejestru proponujemy dodatkowo podanie niewymaganej wprost w art. 30 RODO informacji o podstawie prawnej przetwarzania.

Rejestr musi być prowadzony w formie pisemnej, do której RODO zalicza także formę elektroniczną (art. 30 ust. 3 RODO). Oprócz celów wewnętrznych rejestr jest udostępniany przez administratora organowi nadzorczemu na jego żądanie (art. 30 ust. 4 RODO). Administrator nie ma natomiast obowiązku innego ujawniania rejestru oraz informacji w nim zawartych.

Przykładowy wzór rejestru wraz ze wskazówkami w zakresie jego wypełnienia został opublikowany przez GIODO w jego serwisie internetowym pod adresem https://giodo.gov.pl/pl/1520281/10449.

Załącznik

Załącznikami do poradnika są przykładowe wypełnienia rejestru – na wzorze rekomendowanym przez GIODO – dla dwóch czynności: w zakresie funkcjonowania kancelarii (rekrutacja pracowników) oraz wykonywania zawodu (obsługa spraw sądowoadministracyjnych).

5.8 Zabezpieczenie danych osobowych

RODO wprowadza do ochrony danych osobowych dwie naczelne zasady: zasadę podejścia opartego na ryzyku (ang. *risk-based approach*) oraz zasadę rozliczalności. Zasada podejścia opartego na ryzyku zakłada, że im większe jest ryzyko związane z przetwarzaniem danych osobowych, tym większy powinien być zakres obowiązków ciążących na administratorze. Jednocześnie RODO nie zawiera (w przeciwieństwie do obecnych polskich przepisów o ochronie danych osobowych) wyliczenia konkretnych środków zabezpieczających dane osobowe, które powinny zostać zastosowane w danej sytuacji. Zasadę rozliczalności omówiono w podrozdziale 4.1.

Artykuł 32 ust. 1 RODO, dotyczący bezpieczeństwa przetwarzania, wskazuje wyłącznie na czynniki, które zarówno administrator, jak i podmiot przetwarzający powinien brać pod uwagę przy doborze odpowiednich (adekwatnych do ryzyka) środków technicznych i organizacyjnych. Te czynniki to:

a) stan wiedzy technicznej;
b) koszt wdrożenia;
c) charakter, kontekst i cele przetwarzania;
d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

RODO zawiera w art. 32 ust. 1 listę przykładowych środków technicznych i organizacyjnych, jednak to do administratora lub podmiotu przetwarzającego zależy wybór środków, jakie zostaną zastosowane. Administrator lub podmiot przetwarzający powinien dobierać środki adekwatnie do potrzeb wynikających z szacowania ryzyka.

Przykładowe środki to:

a) pseudonimizacja (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 – art. 4 pkt 5 RODO) i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Odniesienie do działalności radcy prawnego lub adwokata

Każdy administrator jest zobowiązany do doboru technicznych i organizacyjnych środków bezpieczeństwa, a następnie wdrożenia ich do stosowania. W praktyce wymaga to samodzielnego opracowania mechanizmów takiego doboru oraz skorzystania z usług oferujących odpowiedni poziom zabezpieczeń podwykonawców, którzy w swojej działalności poprawnie wdrożyli obowiązki określone w art. 32 RODO.

Zastosowanie norm ISO w działalności radcy prawnego lub adwokata

Przy wdrażaniu zabezpieczeń przetwarzanych danych osobowych w kancelarii radcy prawnego lub adwokata mogą być również wykorzystywane normy ISO. Pomocne w tym zakresie mogą być trzy rodziny norm:

1) normy dotyczące ochrony danych identyfikujących osobę (PII) – serii ISO/IEC 29100;
2) normy dotyczące zarzadzania bezpieczeństwem informacji – serii ISO/IEC 27000;
3) normy dotyczące zarządzania ryzykiem – serii ISO 31000.

Zapewnienie bezpieczeństwa danych powinno się odbywać z zastosowaniem w szczególności norm ISO/EIC serii 29100 odnoszących się do ochrony danych osobowych w związku z normami serii ISO/IEC 27000. Normy te powinny stanowić podstawę do wdrażania zabezpieczeń ze względu na to, że koncepcja ochrony danych z RODO jest oparta właśnie o standardy dotyczące zarządzania bezpieczeństwem informacji.

Norma ISO/IEC 29100

Norma ISO/IEC 29100, dotycząca „Ram prywatności", została wydana w roku 2011, w trakcie prac nad pierwszym projektem RODO, opublikowanym przez Komisję Europejską 25 stycznia 2012 r. Norma ta definiuje pojęcia, które następnie wprowadzono do RODO, takie jak „pseudonimizacja". Właśnie ta norma określa proces zarządzania ryzykiem prywatności. Jednym z wyników zarządzania ryzykiem może być ocena przetwarzania danych osobowych na prywatność osób, których dane dotyczą. Norma dotyczy w szczególności zgodności z wymogami prawnymi odnoszącymi się do ochrony prywatności i

danych osobowych oraz oceny wpływu nowych lub zmodyfikowanych technologii IT lub operacji przetwarzania na prywatność osób, których dane dotyczą.

Norma ta ma zastosowanie do osób i organizacji uczestniczących w projektowaniu, opracowywaniu, testowaniu, utrzymywaniu, administrowaniu i korzystaniu z systemów lub usług informatycznych. Celem wdrożenia tej normy w organizacji jest wprowadzenie zasad prywatności do przetwarzania danych osobowych oraz rozwój systemów zarządzania prywatnością. Zasady określone w normie ISO/IEC 29100 należy stosować w trakcie projektowania, opracowywania i wdrażania polityk prywatności oraz mechanizmów kontroli prywatności.

W działalności radcy prawnego lub adwokata norma ISO/IEC 29100 może w praktyce znaleźć zastosowanie w przypadku tworzenia i wdrażania polityk ochrony danych, a także w przypadku wyboru przez administratora lub przez podmiot przetwarzający mechanizmów kontroli prywatności.

Norma ISO 31000

Kolejnym standardem mogącym służyć zapewnieniu bezpieczeństwa przetwarzanych danych jest norma ISO 31000, która przedstawia ogólny schemat zarządzania ryzykiem składający się z następujących etapów:

1) ustanowienie kontekstu;
2) szacowanie ryzyka: szacowanie, analiza i ocena;
3) postępowanie z ryzykiem;
4) monitorowanie i przegląd ryzyka;
5) poinformowanie i konsultowanie ryzyka.

Norma ISO/IEC 27005

Na bazie normy ISO 31000 powstały szczegółowe wytyczne dotyczące zarządzania ryzykiem dla zapewnienia bezpieczeństwa informacji, które znalazły się w normie ISO/IEC 27005. Wytyczne zawarte w tym standardzie mają w szczególności zastosowanie do szacowania ryzyka w celu dostosowania poziomu zabezpieczeń w ramach systemu zarządzania bezpieczeństwem informacji określonego w normie ISO/IEC 27001. ISO/IEC 27005 nie zawiera jednak konkretnej metody szacowania ryzyka. Co istotne z perspektywy kancelarii radcy prawnego lub adwokata, podejście do szacowania ryzyka musi być wyborem każdej organizacji. Kształt wypracowanego podejścia zależy od zakresu systemu zarządzania bezpieczeństwem informacji, w tym rodzaju informacji objętych tym systemem, w tym danych osobowych. Norma ISO/EIC 27005 określa szczegółowo etapy procesu szacowania ryzyka w bezpieczeństwie informacji:

1) określenie kontekstu (co ma być objęte szacowaniem) i określenie podstawowych kryteriów, zakresu i granic oraz organizacji procesu zarządzania ryzykiem
2) szacowanie ryzyka:
   a) identyfikowanie ryzyka,
      - zidentyfikowanie aktywów,
      - zidentyfikowanie zagrożeń dla aktywów,
      - zidentyfikowanie istniejących zabezpieczeń,
      - zidentyfikowanie podatności,

- zidentyfikowanie następstw (scenariusze incydentów);

b) dokonanie analizy ryzyka:
   - oszacowanie następstw,
   - oszacowanie prawdopodobieństwa incydentu,
   - określenie poziomu ryzyka;

c) ocena ryzyka;

3) postępowanie z ryzykiem:
   a) ustalenie planu postępowania z ryzykiem,
   b) warianty postępowania z ryzykiem,
      - modyfikowanie ryzyka – minimalizacja poprzez wdrożenie określonych zabezpieczeń,
      - zachowanie ryzyka,
      - unikanie ryzyka,
      - dzielenie ryzyka;
4) szacowanie ryzyka szczątkowego;
5) akceptowanie ryzyka;
6) monitorowanie i przegląd ryzyka.

Zasady zawarte w tej normie mogą być stosowane do szacowania ryzyka naruszenia praw i wolności osób, których dane dotyczą, przy doborze środków zabezpieczeń, o których mowa w tym podrozdziale, przy ocenie skutków dla ochrony danych, o której mowa w podrozdziale 5.9., jak również przy spełnianiu wymogów z art. 24 RODO (obowiązki administratora) oraz z art. 25 RODO (uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych).

Norma ISO/IEC 29151

W związku z doborem zabezpieczeń dla ochrony danych osobowych należy również brać pod uwagę normę ISO/IEC 29151, która określa wytyczne w tym zakresie. Standard opiera się na podstawowych zasadach ochrony prywatności określonych w normie ISO/IEC 29100, o której mowa powyżej. Głównymi źródłami wymagań dla ochrony danych osobowych są zgodnie z tą normą:

1) wymagania prawne, statutowe lub kontraktowe związane z ochroną danych osobowych;
2) szacowanie ryzyk dla organizacji oraz dla osoby, której dane dotyczą;
3) polityki korporacyjne.

Norma ISO/IEC 27002

Norma ISO/IEC 27002 określa wytyczne dotyczące standardów bezpieczeństwa informacji, w tym ich wdrażania i zarządzania zabezpieczeniami. Dobór zabezpieczeń powinien uwzględniać środowiska, w których w danej organizacji występuje ryzyko w bezpieczeństwie informacji.

Norma zawiera wytyczne do następujących kategorii zabezpieczeń informacji:

1) polityki bezpieczeństwa informacji,
2) organizacja bezpieczeństwa informacji,
3) bezpieczeństwo zasobów ludzkich,
4) zarządzanie aktywami,
5) kontrola dostępu,

6) kryptografia,
7) bezpieczeństwo fizyczne i środowiskowe,
8) bezpieczna eksploatacja,
9) bezpieczeństwo komunikacji,
10) pozyskiwanie i rozwój systemów,
11) relacje z dostawcami,
12) zarządzanie incydentami związanymi z bezpieczeństwem informacji,
13) aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania,
14) zgodność (rozliczalność).

5.9 Obowiązki związane z naruszeniami ochrony danych

Ogólne omówienie

Rozporządzenie ogólne przewiduje również obowiązki administratora w przypadku naruszenia ochrony danych osobowych. Pod pojęciem „naruszenie ochrony danych" rozumie się *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* (art. 4 pkt 12 RODO).

Obowiązki administratora związane z naruszeniami można podzielić na trzy kategorie:
1) zgłaszanie przez administratora naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1–4 RODO);
2) dokumentowanie przez administratora naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO);
3) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO).

Zgłaszanie przez administratora naruszenia ochrony danych osobowych organowi nadzorczemu

Artykuł 33 ust. 1 RODO przewiduje, że w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia – zgłasza je właściwemu organowi nadzorczemu. W przypadku dokonania zgłoszenia po upływie 72 godzin od stwierdzenia naruszenia administrator powinien załączyć wyjaśnienie przyczyn opóźnienia.

Zgłoszenie nie jest wymagane, jeżeli jest mało prawdopodobne, że naruszenie skutkowałoby naruszeniem praw lub wolności osób fizycznych, co oznacza, że obowiązek zgłaszania naruszeń nie ma charakteru bezwzględnego. Jednakże to na administratorze ciąży obowiązek oceny, czy doszło do naruszenia praw lub wolności osób fizycznych. Jako przykłady sytuacji, w których bez wątpienia dochodzi do takiego naruszenia, należy wymienić sytuacje, w których dochodzi do:
- utraty kontroli nad własnymi danymi,
- negatywnych konsekwencji wizerunkowych,
- negatywnego odbioru społecznego związanego z upublicznieniem danych osobowych.

Minimalne wymogi treści zgłoszenia naruszenia ochrony danych osobowych

Zgodnie z art. 33 ust. 3 RODO zgłoszenie naruszenia ochrony danych osobowych musi co najmniej:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

W przypadku gdy nie jest możliwe udzielenie wszystkich wyżej wskazanych informacji w jednym zgłoszeniu, administrator może przekazywać te dane organowi nadzorczemu sukcesywnie bez zbędnej zwłoki (art. 33 ust. 4 RODO).

Z perspektywy wykonywania zawodu przez radcę prawnego lub adwokata istotne jest, że wymagana treść zgłoszenia naruszenia do organu nadzorczego z art. 33 ust. 3 RODO nie zawiera treści samych danych osobowych, co oznacza, że tajemnica radcowska lub adwokacka nie jest przeszkodą do zgłoszenia naruszenia dotyczącego danych osobowych nią objętych.

Dokumentowanie przez administratora naruszeń ochrony danych osobowych

Artykuł 33 ust. 5 RODO przewiduje obowiązek administratora dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym w szczególności okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Sporządzona dokumentacja musi umożliwić organowi nadzorczemu weryfikację przestrzegania obowiązków z art. 33 RODO. Obowiązek ten jest przejawem zasady rozliczalności z art. 5 ust. 2 RODO, omówionej w podrozdziale 4.1.

W praktyce regulacja ta oznacza, że administrator powinien przewidzieć w ramach wewnętrznej procedury dotyczącej zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu procedurę rejestrowania naruszeń w rejestrze, który spełni określone wyżej wymagania.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Kolejnym obowiązkiem nałożonym na administratora w związku z naruszeniem ochrony danych osobowych jest zawiadomienie osoby, której dane dotyczą. Zgodnie z art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Konieczność zawiadomienia osoby, której dane dotyczą, aktualizuje się, jeżeli zostaną kumulatywnie spełnione dwie przesłanki: zaistnieje ryzyko naruszenia praw lub wolności oraz to ryzyko jest wysokie. Ogólne rozporządzenie nie precyzuje pojęcia „wysokie ryzyko”.

Wymogi co do treści zawiadomienia osoby, której dane dotyczą

Zawiadomienie skierowane do osoby, której dane dotyczą, powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych (art. 33 ust. 2 RODO). Zawiadomienie osoby, której dane dotyczą, musi co najmniej:

- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wyłączenia co do zawiadamiania osoby, której dane dotyczą

Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, jeżeli wystąpi co najmniej jeden z trzech wymienionych przypadków (art. 34 ust. 3 RODO):

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- wymagałoby ono niewspółmiernie dużego wysiłku – w takim przypadku wydaje się publiczny komunikat lub stosuje się podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

W przypadku gdy administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy może (biorąc pod uwagę prawdopodobieństwo, że naruszenie spowoduje wysokie ryzyko naruszenia):

- zażądać zawiadomienia osoby, której dane dotyczą, lub
- stwierdzić, że został spełniony jeden z warunków wyłączających obowiązek zawiadomienia.

Odniesienia do działalności radcy prawnego lub adwokata

Każdy administrator, w tym radca prawny lub adwokat, powinien wdrożyć wewnętrzną procedurę dotyczącą wykrywania, a następnie zgłaszania naruszeń oraz zawiadamiania osób, których dane dotyczą, o takim naruszeniu. Procedura powinna być dostosowana do wielkości kancelarii. W opinii autorów wykonywanie wymogów zgłaszania i zawiadamiania o naruszeniach nie może następować z uchybieniem obowiązkowi zachowania tajemnicy zawodowej, co w szczególności odnosi się do treści zgłoszenia bądź zawiadomienia.

5.10 Ocena skutków dla ochrony danych i uprzednie konsultacje

Ogólne omówienie regulacji dotyczącej oceny skutków

Ogólne rozporządzenie znosi ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych, który był przewidziany w dyrektywie 95/46/WE. Na gruncie prawa polskiego oznacza to zniesienie obowiązku rejestracji zbiorów danych do organu nadzorczego. Jak wskazano w motywie 89 RODO, obowiązek zawiadamiania o przetwarzaniu danych osobowych powodował obciążenia finansowe i administracyjne, a mimo to nie przyczyniał się w oczekiwanym zakresie do poprawy ochrony danych osobowych. W konsekwencji prawodawca unijny uznał, że ogólne obowiązki zawiadamiania należy zastąpić skutecznymi procedurami i mechanizmami, które będą się koncentrować na tych operacjach przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przeprowadzanie oceny skutków dla ochrony danych jest jednym z elementów zarządzania ryzykiem związanym z przetwarzaniem danych.

Ocenę skutków należy podzielić na dwa etapy. W pierwszym etapie administrator dokonuje oceny, czy dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój zakres kontekst lub cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 RODO). Jeżeli odpowiedź jest twierdząca, administrator powinien przystąpić do drugiego etapu oceny skutków. Dokonując oceny skutków, administrator jest zobowiązany do podjęcia konsultacji z inspektorem ochrony danych, jeżeli został powołany. Zasady powoływania inspektora ochrony danych omówiono szerzej w podrozdziale 5.10.

Zakres czynności, które powinny się znaleźć w ocenie skutków, został określony w art. 35 ust. 7 RODO:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym – gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Artykuł 35 ust. 3 RODO zawiera przykładowe wyliczenie sytuacji, w których przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe. Ocena taka jest wymagana w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Ponadto na podstawie art. 35 ust. 1, art. 35 ust. 3 lit. a)–c), motywów 71, 75 oraz 91 preambuły RODO Grupa Robocza Artykułu 29 wskazała kryteria, które należy brać pod uwagę przy ocenie ryzyka dla naruszenia praw lub wolności osób fizycznych:

- ocena lub punktacja, w tym profilowanie i przewidywanie, w szczególności dotyczące takich aspektów podmiotu danych jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się;
- zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub wpływające na podmiot danych w podobny sposób;
- systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie podmiotu danych, w tym systematyczne monitorowanie miejsc dostępnie publicznych;
- przetwarzanie tzw. danych wrażliwych lub przetwarzanie danych o charakterze wysoce osobistym;
- przetwarzanie danych na dużą skalę;
- przetwarzanie danych osobowych podlegające łączeniu lub dopasowywaniu;
- przetwarzanie danych dotyczących osób wymagających szczególnej opieki, których dane dotyczą;
- wykorzystanie do przetwarzania danych innowacyjnych rozwiązań technicznych lub organizacyjnych;
- przetwarzanie danych w sposób utrudniający podmiotom danych wykonywanie przysługujących im praw lub korzystanie z usługi lub z umowy.

Im więcej kryteriów zostanie spełnionych, tym większe jest prawdopodobieństwo, że przetwarzanie danych przez administratora może powodować wysokie ryzyko naruszenia praw lub wolności podmiotu danych. W większości przypadków administrator powinien uznać, że przetwarzanie spełniające dwa kryteria będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Natomiast jeżeli administrator danych uważa, że przetwarzanie danych nie narusza praw i wolności, mimo że zostały spełnione określone kryteria, to powinien tę okoliczność dokładnie udokumentować i załączyć stanowisko inspektora ochrony danych, jeżeli został on powołany.

Należy również dodać, że zgodnie z art. 35 ust. 4 RODO organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz operacji przetwarzania danych podlegających wymogowi oceny skutków dla ochrony danych. W dniu 27 marca 2018 r. GIODO zamieścił na swojej stronie internetowej propozycję wykazu rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych (https://giodo.gov.pl/pl/1520281/10430). Ze względu na trwające jeszcze konsultacje nie jest to wersja ostateczna dokumentu.

Odniesienie do działalności radcy prawnego lub adwokata

Radca prawny lub adwokat powinien dokonywać stałej i systematycznej oceny, czy dany rodzaj przetwarzania ze względu na swój zakres kontekst lub cele podlega obowiązkowi oceny skutków dla ochrony danych osobowych. Przegląd ten winien obejmować wszystkie czynności przetwarzania danych, w szczególności w kontekście planowanych działań.

Tylko przykładowo podajemy, że w działalności radcy prawnego lub adwokata konieczność przeprowadzenia oceny skutków dla ochrony danych może zachodzić w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10. Kluczowe dla rozstrzygnięcia, czy należy przeprowadzić ocenę skutków, jest pojęcie „duża skala". Oceniając, czy przetwarzanie odbywa się na „dużą skalę", należy brać pod uwagę takie czynniki jak ilość osób, których przetwarzanie dotyczy, wielkość oraz różnorodność przetwarzanych danych, czas przetwarzania danych osobowych oraz zasięg terytorialny przetwarzania danych.

Wydaje się, że o dużej skali przetwarzania danych z art. 9 i 10 RODO można mówić przykładowo w przypadku dużych kancelarii specjalizujących się w sprawach karnych lub zajmujących się sprawami medycznymi i ubezpieczeniowymi. Przetwarzanie danych osobowych na dużą skalę nie wystąpi natomiast w przypadku prowadzenia przez radcę prawnego lub adwokata jednoosobowej kancelarii. Wskazuje na to motyw 91 RODO, zgodnie z którym: *Przetwarzanie danych osobowych nie powinno zostać uznane za przetwarzanie danych osobowych na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa*. W przypadku gdy nie jest jasne, czy ocena skutków jest konieczna, zaleca się jej przeprowadzenie.

Jeżeli w ramach organizacji dochodzi do przetwarzania danych, które wymaga przeprowadzania oceny skutków dla ochrony danych, to dobrą praktyką jest stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny. Ocena skutków dla ochrony danych to proces ciągły, wymagający określenia cykliczności wykonywania go u administratora przez cały czas trwania danego procesu przetwarzania danych.

Norma ISO/EIC 29134

W czerwcu 2017 r. została ponadto opublikowana norma ISO/IEC 29134, w której sformułowano wytyczne dla szacowania ryzyka w odniesieniu do oceny skutków. Standard ten zawiera wskazówki do przeprowadzenia procesu szacowania ryzyka dla prywatności osoby, której dane dotyczą. Ponadto w normie tej określono strukturę i zawartość raportu z przeprowadzenia oceny skutków. Norma ta może być stosowana w szczególności w następujących sytuacjach dotyczących przetwarzania danych osobowych:

- identyfikacja skutków, ryzyk i odpowiedzialności dotyczących prywatności;
- dostarczanie wskazówek dla zapewnienia ochrony danych osobowych w fazie projektowania;
- ograniczanie ryzyka związane z przetwarzaniem danych osobowych w odniesieniu do podstawowych zadań ochrony danych osobowych.

Omówienie regulacji dotyczącej uprzednich konsultacji

Gdy ocena skutków przeprowadzona przez radcę prawnego lub adwokata zgodnie z art. 35 RODO wykaże, iż przetwarzanie danych spowodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to następuje aktualizacja obowiązku przeprowadzenia uprzednich konsultacji z organem nadzorczym (art. 36 RODO).

Uprzednie konsultacje rozpoczynają się na wniosek administratora. Wniosek skierowany do organu nadzorczego powinien zawierać (art. 36 ust. 3 RODO):

a) odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw, jeżeli ma to zastosowanie;
b) cele i sposoby zamierzonego przetwarzania;
c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO;
d) dane kontaktowe inspektora ochrony danych, jeżeli ma to zastosowanie;
e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz
f) wszelkie inne informacje, których żąda organ nadzorczy.

Zgodnie z art. 36 ust. 2 RODO, jeżeli organ nadzorczy uzna, że zamierzone przetwarzanie jest niezgodne z RODO, udziela administratorowi (a gdy ma to zastosowanie – także podmiotowi przetwarzającemu) pisemnego zalecenia i może skorzystać z uprawnień określonych w art. 58 RODO, czyli uprawnień dotyczących prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń i uprawnień doradczych.

5.11 Inspektor ochrony danych

Ogólne omówienie obowiązku

W RODO przewiduje się funkcję inspektora ochrony danych (IOD), która służy wspieraniu administratora (podmiotu przetwarzającego) w wykonywaniu jego obowiązków określonych w RODO. Powyższą funkcję (zakres obowiązków) może wykonywać pracownik lub osoba świadcząca usługę na podstawie umowy cywilnoprawnej.

W RODO wskazuje się trzy sytuacje, w których wyznaczenie IOD jest obowiązkowe. W pozostałych sytuacjach wyznaczenie IOD pozostawiono uznaniu administratora lub podmiotu przetwarzającego . W szczególności administrator lub podmiot przetwarzający musi to uczynić, gdy:

- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
- gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (określonych w art. 9 lub 10 RODO).

Zaistnienie dużej skali przetwarzania danych ustala się w oparciu o następujące kryteria:

- liczby osób, których dane dotyczą (jako konkretnej liczby, bądź jako proporcji odpowiedniej populacji);
- ilości danych lub zakresu różnych kategorii danych, jakie poddawane są przetwarzaniu;
- okresu czy trwałości czynności przetwarzania danych;
- geograficznego zakresu czynności przetwarzania.

Dalsze wyjaśnienie tych kryteriów znajduje się w wytycznych Grupy Roboczej Artykułu 29 dotyczących inspektorów ochrony danych (WP 243), przyjętych ostatecznie w dniu 5 kwietnia 2017 r.

Do zadań IOD należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie (art. 39 ust. 1 lit. a) RODO);
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty (art. 39 ust. 1 lit. b) RODO);
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO (art. 39 ust. 1 lit. c) RODO);
d) współpraca z organem nadzorczym (art. 39 ust. 1 lit. d) RODO);
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach (art. 39 ust. 1 lit. e) RODO);
f) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą (art. 38 ust. 4 RODO).

IOD może wykonywać również inne zadania i obowiązki, jednak administrator musi przestrzegać zasady, aby takie zadania i obowiązki nie powodowały konfliktu interesów. IOD wykonuje swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania danych.

Przepisy RODO określają organizacyjne warunki pełnienia funkcji oraz wymogi kwalifikacyjne stawiane osobie wykonującej funkcję, o czym piszemy poniżej w części „Wykonanie obowiązku".

Odniesienie obowiązku do działalności radcy prawnego lub adwokata

W RODO wprost nie zobowiązuje się radcy prawnego lub adwokata do wyznaczenia IOD. Jednak przy określonej specjalizacji kancelarii, której konsekwencją jest przetwarzanie szczególnych kategorii danych osobowych (wymienionych w art. 9 lub 10 RODO) oraz dużej skali przetwarzania danych osobowych może zachodzić ten obowiązek. W przypadku pozostałych kancelarii wyznaczenie IOD nie jest obowiązkowe, ale jeżeli to nastąpi, IOD również musi wykonywać swoją funkcję zgodnie z przepisami RODO.

Wyznaczana osoba powinna spełniać wymogi kwalifikacyjne określone w RODO. Po wyznaczeniu IOD wykonuje swoje zadania w sposób niezależny.

Wykonanie obowiązku

Administracyjne wyznaczenie konkretnej osoby do pełnienia funkcji IOD dokonywane jest oświadczeniem administratora przyjmowanym przez wyznaczonego, przy czym należy ustalić podstawę świadczeń ze strony tej osoby (pracowniczą lub cywilnoprawną) oraz odpowiednio określić obowiązki IOD w treści umowy z nim.

Wobec osoby mającej pełnić funkcję IOD ogólne rozporządzenie stawia wymogi posiadania stosownych kwalifikacji. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, które nakłada na niego RODO.

W RODO określono także warunki organizacyjne wykonywania funkcji IOD. Administrator powinien jednocześnie zapewnić, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, i wspierać go w wypełnianiu zadań określonych w RODO, zapewniając mu zasoby niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. RODO wymaga również, aby IOD miał zapewnioną niezależność wewnątrz jednostki organizacyjnej (kancelarii): nie może otrzymywać instrukcji dotyczących wykonywania zadań określonych w RODO, nie może być także odwoływany ani karany przez administratora za wypełnianie swoich zadań, a podlegać ma bezpośrednio kierownikowi jednostki organizacyjnej.

Równocześnie z wyznaczeniem IOD administrator może uszczegółowić jego zadania w kancelarii, a to ze względu na użycie w RODO pojęć nieostrych w tym zakresie (np. „monitorowanie przestrzegania"), jak również nałożyć inne, dodatkowe zadania, nieprzewidziane wprost w art. 39 ust. 1 RODO (np. prowadzenie rejestru czynności przetwarzania). Jednym z zadań IOD jest pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą. W ramach tego zadania osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw. W tym zakresie administrator zobowiązany jest do opublikowania danych kontaktowych IOD (np. adres korespondencyjny, dedykowany numer telefonu lub adres email przeznaczony tylko do kontaktu z IOD) i przekazania ich organowi nadzorczemu. Wskazuje się, że do celów kontaktu podmiotów danych z IOD można także stworzyć specjalny formularz kontaktowy na stronie internetowej kancelarii administratora.

Załącznik

Załącznikiem jest dokument wyznaczający IOD oraz określający jego zakres zadań.

6. Kodeksy postępowania oraz mechanizmy certyfikacji jako mechanizmy *compliance* określone w RODO

6.1 Znaczenie prawne stosowania zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji

Stosowanie zatwierdzonych kodeksów postępowania oraz mechanizmów certyfikacji przez administratora lub podmiot przetwarzający wiąże się z szeregiem korzyści prawnych po stronie tych podmiotów.

Zgodnie z ogólną regułą określoną w art. 24 ust. 3 RODO stosowanie zatwierdzonych kodeksów postępowania oraz mechanizmów certyfikacji może być wykorzystane jako element umożliwiający wykazanie wywiązania się przez administratora lub podmiot przetwarzający z ciążących na nich obowiązków.

Niezależnie od powyższej ogólnej reguły, również inne przepisy RODO przy określeniu szczegółowych obowiązków administratora lub podmiotu przetwarzającego wprost wskazują na możliwość stosowania mechanizmów *compliance* jako sposobu wykazania spełnienia zgodności z przepisami rozporządzenia.

Artykuł 25 ust. 3 RODO stanowi, że wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42 RODO można wykorzystać w celu wykazania spełnienia obowiązków, o których mowa w art. 25 ust. 1 i 2 RODO, tj. realizacji zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (*privacy by design* i *privacy by default*).

Z kolei zgodnie z art. 28 ust. 5 RODO podmiot przetwarzający może wykazać wystarczające gwarancje, o których mowa w art. 28 ust. 1 i 4 RODO, m.in. poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

Poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji będzie można również wykazać spełnienie obowiązku z art. 32 ust. 1 RODO, tj. obowiązku wdrożenia odpowiednich środków organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa przetwarzanych danych osobowych.

W uzupełnieniu określenia korzyści prawnych wynikających ze stosowania mechanizmów *compliance* warto również wskazać na treść art. 83 ust. 2 lit. j) RODO, zgodnie z którym organ nadzorczy, decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca uwagę na stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji. W przypadku podejmowania decyzji o ewentualnym nałożeniu kary (i jej wysokości), organ nadzorczy (PUODO) powinien zatem uwzględnić stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji jako działań podjętych przez administratora lub podmiot przetwarzający w celu zmniejszenia ryzyka naruszeń.

6.2 Regulacje prawne dotyczące zatwierdzonych kodeksów postępowania oraz zatwierdzonych mechanizmów certyfikacji

Przepisami RODO dotyczącymi kodeksów postępowań oraz mechanizmów certyfikacji są art. 40–43 rozporządzenia ogólnego.

Powyższe przepisy nie regulują jednak w sposób wyczerpujący funkcjonowania i organizacji obu mechanizmów *compliance*. Do 25 maja 2018 r. państwa członkowskie zobowiązane są bowiem przyjąć odpowiednie przepisy prawne, które zapewnią skuteczne funkcjonowanie obu tych instrumentów w krajowym porządku prawnym. W przypadku Polski tego rodzaju przepisy zawarte są w projekcie ustawy o ochronie danych. Przepisy PrUODO doprecyzowują w szczególności takie zagadnienia jak: warunki i tryb udzielania akredytacji podmiotowi certyfikującemu, warunki i tryb udzielania certyfikacji, zasady opracowywania oraz zatwierdzania kodeksu postępowania oraz warunki i tryb akredytacji podmiotu monitorującego jego przestrzeganie.

Ostateczne ukształtowanie procesu zatwierdzania kodeksów postępowania, procesu certyfikacji oraz akredytacji będzie zależeć również od praktyki działania organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych). RODO pozostawia bowiem krajowym organom nadzorczym dookreślenie pewnych kwestii związanych ze stosowaniem tych mechanizmów.

6.3 Akredytacja

Dla stosowania mechanizmów *compliance* określonych w RODO istotne znaczenie ma akredytacja podmiotów świadczących usługi certyfikacyjne, jak również podmiotów monitorujących przestrzeganie zatwierdzonego kodeksu postępowania.

Pojęcie „akredytacja" nie jest zdefiniowana na gruncie RODO. Definicja zawarta jest natomiast w rozporządzeniu 765/2008, które reguluje wymogi akredytacji związanej z marketingiem produktów na poziomie unijnym. Zgodnie z art. 2 pkt 10 rozporządzenia 765/2008 „akredytacja" to poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych, konieczne do realizacji określonych czynności związanych z oceną zgodności. „Krajowa jednostka akredytująca" oznacza natomiast jedyną autorytatywną jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo (art. 2 pkt 11 rozporządzenia 765/2008).

Zgodnie z rozwiązaniem przyjętym w PrUODO akredytacji podmiotów świadczących usługi certyfikacyjne dokonuje Polskie Centrum Akredytacji (art. 12), a podmiotów monitorujących przestrzeganie zatwierdzonych kodeksów postępowania – Prezes Urzędu Ochrony Danych Osobowych (art. 29).

6.4 Kodeksy postępowania

Natura i cel kodeksów postępowania

Zgodnie z art. 40 ust. 1 RODO państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja Europejska zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO, z uwzględnieniem szczególnych cech przetwarzania prowadzonego

w niektórych sektorach oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Istotą funkcjonowania kodeksów jest to, że podmioty, które je przyjmują (sygnatariusze), zobowiązują się do jego stosowania i podlegają określonym w RODO konsekwencjom w przypadku naruszenia jego postanowień (art. 41 ust. 4).

Podmiot odpowiedzialny za sporządzenie kodeksu postępowania

Podmiotami uprawnionymi do sporządzania kodeksów postępowania są zrzeszenia oraz inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Uprawnienie do tworzenia kodeksów nie przysługuje jednak indywidualnemu administratorowi.

W polskim prawie przez „zrzeszenia" rozumie się organizacje czy też grupy podmiotów, do których przyłączenie się następuje w sposób sformalizowany, na podstawie powszechnie obowiązujących przepisów lub zgodnie z ich prawem wewnętrznym. W przypadku polskiego systemu prawnego przykładami takich przepisów mogą być przepisy ustawy – prawo o stowarzyszeniach, ustawy o izbach gospodarczych, czy ustawy o organizacji pracodawców.

Motyw 99 RODO wskazuje, że sporządzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym, jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz uwzględniać uwagi i opinie otrzymane w ramach takich konsultacji.

Przedmiot kodeksów postępowania

W założeniu kodeksy postępowania powinny doprecyzowywać stosowanie RODO i dotyczyć:

a) rzetelnego i przejrzystego przetwarzania;

b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach;

c) zbierania danych osobowych;

d) pseudonimizacji danych osobowych;

e) informowania opinii publicznej i osób, których dane dotyczą;

f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw;

g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem;

h) środków i procedur, o których mowa w art. 24 i 25 RODO, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO;

i) zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;

j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; lub

k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79 RODO.

Kodeksy postępowania mogą obejmować wszelkie aspekty stosowania RODO. Można założyć, że np. kodeksy postępowania danego sektora lub branży będą uwzględniać specyfikę stosowania przepisów RODO właśnie przez przedsiębiorstwa z danego sektora lub branży. RODO wskazuje, że w kodeksach można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do zagrożeń naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie danych przez podmioty z konkretnego sektora.

Grupa Robocza Artykułu 29 wskazuje, że kodeksy powinny tworzyć wartość dodaną w stosunku do tego, co uregulowane zostało w RODO, tj. nie powinny stanowić wyłącznie powtórzenia przepisów RODO (np. mogą uwzględniać specyfikę stosowania RODO w danym sektorze lub branży).

Proces zatwierdzania kodeksu

Chcąc zatwierdzić lub zmienić już zatwierdzony kodeks postępowania, zrzeszenie podmiotów lub inne uprawnione podmioty muszą przedłożyć projekt kodeksu lub zmiany właściwemu organowi nadzorczemu (art. 40 ust. 5 RODO). Organ nadzorczy wydaje opinię o zgodności projektu kodeksu i zatwierdza taki projekt, jeżeli kodeks stanowi odpowiednie zabezpieczenie dla praw i wolności osób, których dane dotyczą. Ewentualne zmiany w kodeksie lub rozszerzenia postępowania również muszą być każdorazowo przedłożone organowi nadzorczemu.

W przypadku gdy kodeks dotyczy czynności przetwarzania w jednym z państw członkowskich i nie rozciąga się na działania w innych państwach, organ nadzorczy dokonuje rejestracji tego kodeksu i publikuje jego treść (art. 40 ust. 6 RODO).

W przypadku projektu kodeksu postępowania dotyczącego czynności przetwarzania prowadzonych w kliku państwach członkowskich organ nadzorczy przed zatwierdzeniem kodeksu – zgodnie z mechanizmem spójności – przedkłada go Europejskiej Radzie Ochrony Danych. Jeżeli Europejska Rada Ochrony Danych wyda pozytywną opinię, przekazuje takowy kodeks Komisji Europejskiej, która w drodze aktu wykonawczego stwierdza z zachowaniem procedury sprawdzającej (art. 93 ust. 2 RODO), że jest on powszechnie obowiązujący w Unii Europejskiej (art. 40 ust. 9 RODO).

Na mocy art. 40 ust. 11 RODO Europejska Rada Ochrony Danych prowadzi rejestr zatwierdzonych kodeksów postępowania. Gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania, zmiany i rozszerzenia i udostępnia je opinii publicznej za pomocą odpowiednich środków.

Zgodnie z art. 27 ust. 2 PrUODO zatwierdzenia kodeksów postępowania będzie dokonywał Prezes Urzędu Ochrony Danych Osobowych.

Obowiązek monitorowania przestrzegania kodeksu postępowania

Zgodnie z art. 40 ust. 4 RODO kodeks postępowania musi przewidywać również mechanizmy pozwalające podmiotowi monitorującemu (akredytowanemu przez właściwy organ nadzorczy) prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania.

W przypadku stwierdzenia przez podmiot wykonujący proces monitorowania, że nastąpiło naruszenie przez konkretnego administratora lub podmiot przetwarzający zasad określonych w tym dobrowolnie przyjętym kodeksie, podmiot monitorujący może zawiesić lub wykluczyć tego administratora spośród podmiotów stosujących ten kodeks i podjąć inne stosowne działania, o czym zobowiązany jest poinformować organ nadzorczy (art. 41 ust. 4 RODO).

Należy przy tym wskazać, że czynności te stosuje się bez uszczerbku dla zadań i uprawnień organu nadzorczego do kontrolowania zgodności przetwarzania danych przez administratorów lub podmioty przetwarzające.

Kodeksy postępowania a przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

RODO w art. 40 ust. 3 umożliwia zastosowanie kodeksów postępowania jako instrumentów zapewniających odpowiednie gwarancje przy przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej (na warunkach określonych w art. 46 ust. 2 lit. e) RODO).

Administratorzy lub podmioty przetwarzające, którzy nie podlegają RODO (tj. podmioty spoza EOG), mogą przystąpić tylko do kodeksu, który został uprzednio zatwierdzony przez organ nadzorczy zgodnie z art. 40 ust. 5 RODO, lub takiego, któremu nadano przymiot powszechnego obowiązywania zgodnie z art. 40 ust. 9 RODO.

Przystąpienie do kodeksu przez administratorów lub podmioty przetwarzające spoza EOG będzie jednak możliwe jedynie wówczas, jeżeli podmioty te w sposób wiążący i możliwy do wyegzekwowania zobowiążą się do jego stosowania w drodze umowy lub innego prawnie wiążącego instrumentu.

Przystąpienie do takiego kodeksu po spełnieniu ww. wymogów pozwoli administratorom i podmiotom przetwarzającym niepodlegającym RODO na wykazanie, że zapewniają odpowiednie zabezpieczenia w rozumieniu RODO.

6.5 Certyfikacja

Natura i cel mechanizmów certyfikacji

Zgodnie z art. 42 ust. 1 RODO państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty

przetwarzające, uwzględniając przy tym szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Przepisy RODO nie definiują pojęcia „certyfikacja". Uniwersalną definicję wprowadzają normy Międzynarodowej Organizacji Normalizacyjnej w Genewie (ISO), zgodnie z którymi „certyfikacja" oznacza poświadczenie przez niezależny podmiot, wydane w formie pisemnego zapewnienia (certyfikatu), że dany produkt, usługa lub system spełniają określone wymagania, np. odpowiednie normy prawne lub techniczne.

W przepisach nie definiuje się również znaków jakości i oznaczeń, jednak wydaje się, że posługiwanie się nimi będzie oznaczać, że z powodzeniem zakończono procedurę certyfikacji. Nadanie znaków jakości i oznaczeń wskazuje, że produkt, proces lub usługa zostały poddane niezależnej ocenie w ramach certyfikacji i spełniają określone wymagania.

Motyw 100 RODO doprecyzowuje, że celem mechanizmu certyfikacji jest stworzenie możliwości łatwej oceny poziomu ochrony danych oferowanych produktów i usług przez osoby, których dane dotyczą.

Należy również podkreślić, że certyfikacja jest dobrowolna i organ nadzorczy nie może uzależnić możliwości przetwarzania danych przez administratora lub podmiot przetwarzający od posiadania certyfikatu. Nic nie stoi jednak na przeszkodzie, aby w relacjach umownych wymagać posiadania certyfikatu, np. administrator może zobowiązać podmiot przetwarzający do uzyskania i utrzymania konkretnego certyfikatu.

Przedmiot certyfikacji

Przepisy RODO nie precyzują, jakie kwestie mogą być przedmiotem certyfikacji. Opierając się na samym brzmieniu art. 42 ust. 1 RODO, należy uznać, że przedmiotem certyfikacji mogą być wszelkie operacje przetwarzania dokonywane przez administratora lub podmiot przetwarzający. Dla przykładu certyfikacja może obejmować:

- standardy bezpieczeństwa dla różnych kategorii danych;
- mechanizmy pozyskiwania zgód dla różnych sytuacji;
- proces wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (*privacy by design* i *privacy by default*);
- procedury przeprowadzania oceny skutków dla ochrony danych (DPIA);
- procedury postępowania z wykonywaniem przez osoby, których dane dotyczą, przysługujących im praw (np. prawa do przenoszenia danych).

Z treści PrUODO wynika również, że przedmiotem certyfikacji może być usługa lub produkt wprowadzany na rynek, a z którą to usługą lub produktem związane jest przetwarzanie danych osobowych.

Podmiot udzielający certyfikacji

RODO wskazuje, że w każdym państwie członkowskim certyfikacji mogą dokonywać podmioty certyfikujące akredytowane zgodnie z art. 43 RODO lub właściwy organ nadzorczy. Dokładne wskazanie podmiotu, który dokonywać będzie certyfikacji, musi nastąpić w przepisach krajowych.

Na gruncie art. 42 ust. 5 RODO można zidentyfikować trzy potencjalne modele w zakresie certyfikacji:

1) certyfikacji dokonuje wyłącznie organ nadzorczy;

2) certyfikacji dokonują wyłącznie podmioty certyfikujące;

3) uprawnienie do wydawania certyfikacji posiadają zarówno organ nadzorczy, jak i podmioty certyfikujące.

W PrUODO przyjęto ostatni z tych modeli (model mieszany), certyfikacji dokonywać ma bowiem zarówno Prezes Urzędu Ochrony Danych Osobowych, jak również podmioty certyfikujące akredytowane przez Polskie Centrum Akredytacji (art. 15).

Kryteria certyfikacji

RODO nie określa kryteriów, jakie administratorzy lub podmioty przetwarzające muszą spełnić, aby uzyskać certyfikat. Z art. 42 ust. 5 RODO wynika jedynie, że kryteria takie mogą zostać zatwierdzone przez:

- właściwy organ nadzorczy zgodnie z art. 58 ust. 3 RODO lub
- Europejską Radę Ochrony Danych zgodnie z art. 63 RODO.

Stosownie do art. 57 ust. 1 lit. n) RODO, organ nadzorczy zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5 RODO. Organ nadzorczy nie ma obowiązku opracowywać tych kryteriów. Jednocześnie wydaje się, że nie ma przeszkód, aby to właśnie on ustalał kryteria certyfikacji.

Zgodnie z art. 42 ust. 5 RODO w przypadku gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją – europejskim znakiem jakości ochrony danych. Przepisy RODO nie określają jednak, w jaki sposób kryteria certyfikacji trafiają do Rady, ani nie przydzielają jej żadnych konkretnych zadań w tym zakresie. W szczególności Europejska Rada Ochrony Danych nie została upoważniona do opracowania kryteriów certyfikacji, a jej funkcja została ograniczona jedynie do zatwierdzania przedłożonych jej kryteriów.

Artykuł 43 ust. 8 RODO przewiduje jednocześnie, że Komisja Europejska również jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 92 RODO w celu doprecyzowania wymogów, które uwzględnia się w przypadku mechanizmów certyfikacji w dziedzinie ochrony danych.

Proces udzielania certyfikatów

Po zatwierdzeniu przez Europejską Radę Ochrony Danych lub organ nadzorczy kryteriów certyfikacji dla określonej formy przetwarzania, administrator lub podmiot przetwarzający może złożyć wniosek odpowiednio albo do właściwego organu nadzorczego (PUODO), albo do akredytowanego podmiotu certyfikującego.

Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, udzielają akredytowanemu podmiotowi certyfikującemu lub właściwemu organowi nadzorczemu wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji (art. 42 ust. 6 RODO).

Jeżeli certyfikacji dokonuje podmiot certyfikujący, musi on poinformować organ nadzorczy o złożonym wniosku. Organ nadzorczy może w takiej sytuacji wykonać swoje uprawnienia zgodnie z art. 58 ust. 2 lit. h) RODO, tj. nakazać podmiotowi certyfikującemu nieudzielanie certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.

Analogicznie jak w przypadku zatwierdzonych kodeksów postępowania (art. 40 ust. 11 RODO), zgodnie z art. 42 ust. 8 RODO Europejska Rada Ochrony Danych zobowiązana jest do gromadzenia w rejestrze wszystkich mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych oraz udostępniania tego rejestru opinii publicznej za pomocą odpowiednich środków.

Ograniczony okres obowiązywania certyfikatu

Certyfikacja mająca na celu wykazanie przestrzegania przepisów RODO udzielana będzie maksymalnie na 3 lata (art. 42 ust. 7). Może być ona przedłużona na tych samych warunkach, o ile nadal spełnione są przez dany podmiot wymogi obowiązujące dla przedmiotowej certyfikacji.

Podmioty certyfikujące, o których mowa w ust. 1, przedstawiają właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji (art. 42 ust. 5 RODO). Organ nadzorczy lub podmiot certyfikujący mogą cofnąć certyfikat, jeżeli nie są spełnione lub przestały być spełniane wymogi (art. 42 ust. 7 RODO).

Podobnie, stosownie do art. 53 ust. 2 lit. h) RODO, organ nadzorczy może cofnąć certyfikat lub nakazać podmiotowi certyfikującemu cofnięcie certyfikacji udzielonej na mocy art. 42 lub 43 RODO.

Ponieważ RODO nie przewiduje szczegółowych warunków cofnięcia certyfikatu, będą one musiały zostać określone w przepisach prawa krajowego.

Koszty certyfikacji

RODO nie przewiduje pobierania opłat związanych z certyfikacją. Zgodnie jednak z PrUODO za czynności związane z certyfikacją Prezes Urzędu Ochrony Danych Osobowych pobiera opłatę w wysokości czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o certyfikację, ogłaszanego przez Prezesa

Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a) Ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (t.j. Dz. U. z 2017 r. poz. 1383 ze zm.).

Mechanizmy certyfikacji a przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Podobnie jak w przypadku kodeksów postępowania RODO umożliwia również wykorzystywanie zatwierdzonych mechanizmów certyfikacji przy przekazywaniu danych osobowych do państw trzecich lub organizacji międzynarodowych bez konieczności uzyskiwania zgody organu nadzorczego (art. 46 ust. 2 lit. f) RODO). Zgodnie z art. 42 ust. 2 administratorzy lub podmioty przetwarzające, którzy zgodnie z art. 3 RODO nie podlegają rozporządzeniu, mogą wykazać odpowiednie zabezpieczenia poprzez mechanizm certyfikacji w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. f) RODO.

Należy jednak podkreślić, że zastosowane w takich sytuacjach mechanizmy certyfikacji muszą być uzupełnione o przyjęte przez takich administratorów lub podmioty przetwarzające w drodze umowy lub innego prawnie wiążącego instrumentu wiążące prawnie i możliwe do wyegzekwowania zobowiązania.

7. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

Przez naruszenie przepisów o ochronie danych osobowych należy rozumieć naruszenie przepisów RODO, jak również aktów delegowanych i wykonawczych przyjętych na mocy rozporządzenia ogólnego oraz prawa państwa członkowskiego UE doprecyzowującego RODO.

7.1 Rodzaje odpowiedzialności za naruszenie przepisów o ochronie danych osobowych

W przepisach RODO prawodawca unijny przewiduje dwa rodzaje odpowiedzialności za naruszenie przepisów o ochronie danych osobowych:

- reżim odpowiedzialności administracyjnej (art. 77, 78 i 83) oraz
- reżim odpowiedzialności cywilnoprawnej (art. 79 i 82).

Niezależnie od powyższych zasad odpowiedzialności w RODO dopuszczono również wprowadzenie w porządkach krajowych państw członkowskich sankcji karnych (art. 84 RODO). Z możliwości tej skorzystał polski ustawodawca w PrUODO.

Przepisy RODO nie określają zasad proceduralnych w postępowaniach dotyczących poszczególnych rodzajów odpowiedzialności, pozostawiając w tym zakresie swobodę ustawodawcy krajowemu.

Wszystkie potencjalne możliwości dochodzenia odpowiedzialności za naruszenie przepisów o ochronie danych osobowych, w tym ich podstawy materialnoprawne oraz proceduralne możliwości, przedstawiono w formie graficznej w podsumowaniu (punkt VI poniżej).

7.2 Odpowiedzialność administracyjna

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez PUODO (art. 60 PrUODO). W postępowaniu tym stosują się – subsydiarnie – przepisy kodeksu postępowania administracyjnego, które znajdują zastosowanie w sprawach nieuregulowanych w PrUODO (art. 7 ust. 1 PrUODO).

Postępowanie przed PUODO może zostać wszczęte z urzędu lub w wyniku skargi podmiotu danych (osoby, której dane dotyczą). Szczególne uprawnienia przyznano organizacji społecznej, o której mowa w art. 31 § l KPA i która może występować w postępowaniu za zgodą osoby, której dane dotyczą, działając w jej imieniu i na jej rzecz (art. 61 PrUODO).

Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, PUODO, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych, wskazując dopuszczalny zakres tego przetwarzania (art. 70 ust. 1 PrUODO). W postanowieniu Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej

postępowanie w sprawie, a na orzeczenie to przysługuje skarga do sądu administracyjnego (art. 70 ust. 2 PrUODO).

W art. 7 ust. 2 PrUODO przesądzono, że postępowanie przed PUODO jest postępowaniem jednoinstancyjnym. a wydane w jego toku rozstrzygnięcia mają podlegać zaskarżeniu w toku dwuinstancyjnego postępowania sądowoadministracyjnego. W przypadku decyzji o nałożeniu administracyjnej kary pieniężnej wniesienie skargi do sądu administracyjnego skutkować ma wstrzymaniem jej wykonania (art. 74 PrUODO), natomiast w stosunku do decyzji przewidujących inne środki prawne konieczne jest złożenie – do PUODO lub sądu administracyjnego – wniosku o wstrzymanie decyzji.

Środki administracyjnoprawne za naruszenie przepisów o ochronie danych osobowych

Z odpowiedzialnością administracyjną administratora lub podmiotu przetwarzającego wiążą się następujące środki prawne przewidziane w RODO:

a) prawo wniesienia skargi do organu nadzorczego (art. 77 RODO),

b) uprawnienia naprawcze organu nadzorczego (art. 58 ust. 2 RODO),

c) administracyjne kary pieniężne (art. 83 RODO).

Prawo wniesienia skargi do organu nadzorczego (art. 77 RODO)

Zgodnie z RODO, bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej, w przypadku naruszenia ochrony danych osobowych osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia (art. 77 ust. 1).

Rozpatrywanie skarg złożonych przez podmioty uprawnione należy do kompetencji, a jednocześnie do obowiązków organu nadzorczego (art. 57 ust. 1 lit. f) RODO).

Rozpatrując skargę, organ nadzorczy może podjąć działania naprawcze, określone w art. 58 ust. 2 lit. a)–h) oraz j), jak również nałożyć kary pieniężne (art. 83). Warto wskazać, że zgodnie z art. 83 ust. 2 zdanie pierwsze RODO administracyjne kary pieniężne mogą być stosowane oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j). Organ nadzorczy może więc zastosować kary pieniężne oprócz lub zamiast środków prawnych, które stanowią odzwierciedlenie tzw. uprawnień naprawczych organów nadzorczych (art. 58 ust. 2 lit. a)–h) i lit. j) RODO). Wynika to m.in. z motywu nr 150 RODO, zgodnie z którym nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani innych sankcji na mocy RODO.

Uprawnienia naprawcze organów nadzorczych (art. 58 ust. 2 lit. a)–h) i lit. j) RODO).

Przepisy RODO przewidują możliwość korzystania przez organy kontrolne z uprawnień naprawczych, które stanowią rodzaj sankcji administracyjnych. Warto w związku z tym podkreślić, że RODO rozszerza

zakres uprawnień naprawczych organu nadzorczego w porównaniu do tych, które obecnie przysługujących GIODO na gruncie ustawy o ochronie danych osobowych (art. 18 UODO).

Zgodnie art. 58 ust. 2 RODO organowi nadzorczemu przysługiwać będą następujące uprawnienia naprawcze:

a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;

b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania;

c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;

d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;

f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

g) nakazanie na mocy art. 16, 17 i 18 RODO sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 RODO powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43 RODO, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;

i) zastosowanie, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 RODO, administracyjnej kary pieniężnej na mocy art. 83 RODO, zależnie od okoliczności konkretnej sprawy;

j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 RODO podlega, zgodnie z art. 83 ust. 6 RODO, administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Jest to tzw. niesamoistna kara pieniężna, którą odróżnić należy od kar pieniężnych niesamoistnych.

Administracyjne kary pieniężne (art. 83 RODO)

Jedną z najistotniejszych zmian, jakie przyniosła europejska reforma prawa ochrony danych, jest wprowadzenie do katalogu sankcji z tytułu naruszenia przepisów o ochronie danych osobowych administracyjnej kary pieniężnej nakładanej w każdym państwie członkowskim przez organy nadzorcze zgodnie z art. 83 RODO. Przepis art. 83 RODO określa przesłanki zastosowania administracyjnej kary pieniężnej, wyznacza jej wysokość oraz wskazuje wpływające na nią okoliczności.

Warto wskazać, że do elementów, które pośrednio będą oddziaływać na proces miarkowania wysokości administracyjnej kary pieniężnej, należą wytyczne, które w tym przedmiocie wydawać będzie Europejska Rada Ochrony Danych (art. 70 ust. 1 lit. k) RODO).

Okoliczności uwzględniane przy nakładaniu kar pieniężnych i określaniu ich wysokości

W artykule 83 ust. 2 RODO zawarty jest katalog okoliczności, które organ nadzorczy musi uwzględnić, rozstrzygając o nałożeniu sankcji administracyjnej, a także określając jej wysokość. Okoliczności wskazane w tym przepisie można podzielić na te dotyczące:

1) działań lub zaniechań podmiotu w ramach konkretnej sprawy i ich skutków dla osób poszkodowanych (lit. a)–d) i k)), czyli:

    a) charakteru, wagi i czasu trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;

    b) umyślnego lub nieumyślnego charakteru naruszenia;

    c) działań podjętych przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

    d) stopnia odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO;

    e) wszelkich innych obciążających lub łagodzących czynników mających zastosowanie do okoliczności sprawy, takich jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty;

2) kategorii naruszonych danych osobowych (lit. g));

3) współpracy z organem nadzorczym w ramach sprawy (lit. f) i i)), tj.:

    a) stopnia współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

    b) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 RODO – przestrzegania tych środków;

4) uprzedniej działalności podmiotu (lit. e), h) i j)), czyli:

   a) wszelkich stosownych wcześniejszych naruszeń ze strony administratora lub podmiotu przetwarzającego;

   b) sposobu, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;

   c) stosowania zatwierdzonych kodeksów postępowania na mocy art. 40 RODO lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 RODO.

Należy podkreślić, że wskazany powyżej katalog nie ma charakteru zamkniętego, gdyż art. 83 ust. 2 lit. k) RODO nakazuje w analizowanym procesie uwzględnić wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, wskazując dla przykładu korzyści finansowe osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem lub uniknięte straty.

Odnosząc się do okoliczności decydujących o wysokości administracyjnej kary pieniężnej, odwołać się także należy do dyrektywy skuteczności, proporcjonalności i odstraszającego charakteru sankcji, której adresatem jest organ nadzorczy. Zgodnie z art. 83 ust. 1 RODO organ nadzorczy zapewnia bowiem, aby administracyjne kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

Odnośnie do okoliczności wskazanych w pkt 1 lit. b) powyżej Grupa Robocza Artykułu 29 w wytycznych z dnia 3 października 2017 r. (WP 253) wskazała, że umyślne naruszenia, wskazujące na lekceważenie przepisów prawa, są cięższe niż te nieumyślne, przez co jest bardziej prawdopodobne, że będą skutkować nałożeniem administracyjnej kary pieniężnej. Okoliczności, które mogą wskazywać na umyślne naruszenie, to np. niezgodne z prawem przetwarzanie dopuszczone w sposób wyraźny przez kierownictwo administratora lub dokonane z pominięciem wytycznych udzielonych przez inspektora ochrony danych lub realizowane z naruszeniem istniejących polityk.

Rodzaje i wysokość administracyjnych kar pieniężnych.

W art. 83 RODO przewidziano trzy rodzaje kar pieniężnych i dwa pułapy ich wysokości, z czego dwa rodzaje (wyższa i niższa) mają charakter samoistny, a ich maksymalna wysokość jest zależna od rodzaju stwierdzonego przez organ naruszenia oraz charakteru podmiotu, wobec którego ma być ona zastosowana, a trzeci rodzaj jest następczy w stosunku do uprzednio już zastosowanego przez organ środka prawnego z art. 58 ust. 2 RODO (charakterem jest więc zbliżony do obowiązującej na gruncie UODO grzywny w celu przymuszenia, gdyż dotyczy egzekwowania obowiązków o charakterze niepieniężnym).

Na gruncie RODO możemy zatem wyróżnić:

1) karę samoistną niższą (art. 83 ust. 4 RODO),

2) karę samoistną wyższą (art. 83 ust. 5 RODO).

3) karę niesamoistną (art. 83 ust. 6 RODO).

- *Kara samoistna niższa (art. 83 ust. 4 RODO)*

Administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, podlegają naruszenia przepisów, o których mowa w art. 83 ust. 4 RODO, tj.:

a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25–39 oraz 42 i 43 RODO;

b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43 RODO;

c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4 RODO;

Z treści tego przepisu wynika, że kara niższa może zostać nałożona na: (1) administratora, (2) podmiot przetwarzający, (3) podmiot certyfikujący, (4) podmiot monitorujący.

- *Kara samoistna wyższa (art. 83 ust. 5 RODO).*

Administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, podlegają naruszenia przepisów, o których mowa w art. 83 ust. 5 RODO, tj.:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5–7 oraz 9 RODO;

b) praw osób, których dane dotyczą, o których mowa w art. 12–22 RODO;

c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49 RODO;

d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX RODO;

e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1 RODO.

Administracyjna kara pieniężna w większej wysokości może zostać nałożona na: (1) administratora, (2) podmiot przetwarzający, (3) współadministratora, (4) przedstawicieli.

- *Kara niesamoistna (art. 83 ust. 6 RODO).*

Kara ta może być nałożona przez organ nadzorczy w przypadku stwierdzenia, że administrator lub podmiot przetwarzający nie wykonał nakazów z art. 58 ust. 2 RODO. W takim przypadku organ nadzorczy może nałożyć administracyjną karę pieniężną w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 6 RODO).

Mimo że nie wynika to wprost z treści przepisu, wydaje się, że przepis ten powinien być stosowany łącznie z art. 83 ust. 1 i 2 RODO, a więc organ nadzorczy powinien stosować przy jej nakładaniu ogólne kryteria nakładania kar (art. 83 ust. 1 RODO), jak i okoliczności wskazane w art. 83 ust. 2 oraz określony w tym przepisie zakres zastosowania kar.

- *Administracyjne kary pieniężne nakładane na organy i podmioty publiczne (art. 83 ust. 7 RODO)*

Zgodnie z art. 83 ust. 7 RODO każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

Na gruncie RODO prawodawca unijny pozostawił zatem każdemu z państw członkowskich do rozstrzygnięcia, czy kary pieniężne znajdą zastosowanie wobec administratorów lub podmiotów przetwarzających, którymi są organy i podmioty publiczne ustanowione w tym państwie.

PrUODO, uwzględniając możliwość stworzoną przez art. 83 ust. 7 RODO, zakłada ograniczenie górnej granicy, do której może zostać nałożona kara pieniężna na jednostki sektora finansów publicznych, instytuty badawcze oraz Narodowy Bank Polski. Kwota ta, w zależności od rodzaju podmiotu publicznego, wynosi 100 tys. zł lub 10 tys. zł (art. 102 ust. 1–2 PrUODO).

- *Zbieg naruszeń a wysokość administracyjnej kary pieniężnej (art. 83 ust. 3 RODO)*

W przypadku zbiegu naruszeń, zgodnie z art. 83 ust. 3 RODO całkowita wysokość kary pieniężnej nie może przekroczyć wysokości kary za najpoważniejsze naruszenie. Do wyżej wymienionego zbiegu naruszeń dochodzić może w sytuacji, gdy w ramach tych samych lub powiązanych operacji przetwarzania danych administrator danych lub podmiot przetwarzający dopuszcza się naruszeń umyślnie lub nieumyślnie.

Należy wskazać, że podstawowym warunkiem zastosowania art. 83 ust. 3 RODO jest to, by do naruszeń doszło w ramach tych samych lub powiązanych operacji przetwarzania danych. Nie dojdzie więc do jego zastosowania w przypadku popełnienia przez ten sam podmiot (administratora lub podmiot przetwarzający) wielu naruszeń, ale w ramach różnych, niepowiązanych ze sobą procesów przetwarzania danych.

7.3 Odpowiedzialność cywilnoprawna

Na odpowiedzialność cywilnoprawną administratora lub podmiotu przetwarzającego składają się:

a) prawo do dochodzenia przed sądem swoich praw, z pominięciem postępowania skargowego przed organem nadzorczym (art. 79 RODO);

b) prawo do dochodzenia odszkodowania lub zadośćuczynienia (art. 82 RODO).

Wystąpienie z roszczeniami określonymi w art. 79 nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych (np. roszczeń określonych w art. 82 RODO).

Dochodzenie roszczeń cywilnoprawnych dotyczących naruszenia przepisów o ochronie danych osobowych

Zgodnie z art. 92 PrUODO w zakresie nieuregulowanym w RODO do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 rozporządzenia ogólnego, stosuje się przepisy KC.

Bez względu na wartość przedmiotu sporu sądem właściwym do orzekania w sprawach roszczeń określonych w art. 79 ust. 1 oraz art. 82 ma być w pierwszej instancji sąd okręgowy (art. 93 PrUODO). W zakresie nieuregulowanym przepisami przyszłej ustawy o ochronie danych osobowych subsydiarnie mają znaleźć zastosowanie przepisy KPC (art. 100 PrUODO).

Związek między postępowaniami administracyjnymi i cywilnymi w sprawach o naruszenie przepisów o ochronie danych osobowych

W PrUODO zawarto przepisy regulujące wzajemny związek spraw administracyjnych i cywilnoprawnych o naruszenie przepisów o ochronie danych osobowych.

Po pierwsze, sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed PUODO (art. 95 PrUODO).

Po drugie, sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja PUODO lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a PPSA, uwzględnia roszczenie dochodzone przed sądem (art. 96 PrUODO).

Po trzecie, ustalenia prawomocnej decyzji PUODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 PPSA, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów (art. 97 PrUODO).

Roszczenia przysługujące na podstawie art. 79 RODO

W przypadku roszczenia cywilnoprawnego z art. 79 RODO na podkreślenie zasługuje jego oderwanie od materialnoprawnych podstaw roszczeń o naruszenie dóbr osobistych (art. 23 i n. KC). Dla występowania na drogę sądową z tymi roszczeniami nie jest również konieczne wyczerpanie drogi w

postaci przeprowadzenia postępowania skargowego przed organem nadzorczym określonego w art. 78 RODO.

Realizację uprawnień określonych w art. 79 RODO urzeczywistniają przepisy art. 82 i n. PrUODO. Zgodnie z nimi w przypadku naruszenia praw przysługujących podmiotowi danych na podstawie przepisów o ochronie danych osobowych, może on może żądać zaniechania tego działania, a także dopełnienia przez tego, kto dopuścił się naruszenia, czynności potrzebnych do usunięcia jego skutków. Zgodnie z art. 80 RODO podmiot danych – niezależnie od możliwości samodzielnego działania – może również ustanowić swoim pełnomocnikiem organizację społeczną wyspecjalizowaną w ochronie danych osobowych. Uprawnienie to nie wyłącza możliwości powoływania profesjonalnych pełnomocników.

Roszczenia przysługujące na podstawie art. 82 RODO

W przepisie art. 82 określono zasady odpowiedzialności odszkodowawczej administratora i podmiotu przetwarzającego. Podobnie jak w przypadku art. 79 RODO, chodzi tutaj o roszczenia kierowane do tych podmiotów przez osobę, której dane dotyczą.

Artykuł 82 RODO dotyczy zarówno szkody majątkowej, jak i zadośćuczynienia (szkody niemajątkowej).

Warunkiem odpowiedzialności jest łączne spełnienie następujących przesłanek:

a) poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej,

b) naruszenia przez administratora lub podmiot przetwarzający przepisów RODO (tj. wystąpienia zdarzenia, w wyniku którego doszło do powstania szkody),

c) zaistnienia związku między szkodą a naruszeniem oraz

d) wystąpienia winy w naruszeniu przepisów RODO (przepisów o ochronie danych osobowych).

Ciężar dowodu wystąpienia naruszenia, poniesienia szkody oraz związku przyczynowego spoczywa na podmiocie danych.

Z art. 82 ust. 3 wynika domniemanie winy sprawy naruszenia. Ciężar dowodu, że do naruszenia nie doszło z winy administratora lub podmiotu przetwarzającego, spoczywa więc na tych podmiotach. Sposób sformułowania tego przepisu przypomina więc przepisy kodeksu cywilnego, wprowadzające tzw. odwrócony ciężar dowodu w sprawach o naruszenie dóbr osobistych.

Zgodnie z art. 82 ust. 4 RODO w przypadku gdy w przetwarzaniu bierze udział więcej niż jeden administrator, więcej niż jeden podmiot przetwarzający lub razem uczestniczą administrator i podmiot przetwarzający, odpowiedzialność wszystkich tych podmiotów jest solidarna.

7.4 Odpowiedzialność karna

W przepisach RODO nie określono zasad odpowiedzialności karnej, pozostawiając jedynie taką możliwość ustawodawcy krajowemu. Z możliwości tej skorzystał polski projektodawca, który w

rozdziale 11 PrUODO wprowadził trzy przestępstwa karne za naruszenie przepisów o ochronie danych osobowych. W porównaniu do przepisów aktualnie obowiązującej ustawy stanowi to istotne ograniczenie katalogu środków karnych.

Dochodzenie odpowiedzialności karnej dotyczącej naruszenia przepisów o ochronie danych osobowych

Postępowanie w sprawach o czyny określone w art. 107–108 PrUODO wszczyna się na podstawie przepisów kodeksu postępowania karnego.

Przestępstwa naruszenia przepisów o ochronie danych osobowych

W art. 107 PrUODO spenalizowano sytuację przetwarzania danych osobowych bez podstawy prawnej. Ustęp 2 tego przepisu zawiera kwalifikowaną postać przestępstwa – elementem różnicującym i kwalifikującym jest tutaj rodzaj danych (dane wrażliwe, których katalog określony został w art. 9 RODO). Z uwagi na zagrożenie (grzywną, karą ograniczenia wolności albo pozbawienia wolności do roku) przestępstwo określone w art. 108 zaliczyć należy do występków.

Przestępstwo to ma charakter powszechny, dopuścić się go może każda osoba, a nie tylko administrator danych czy podmiot przetwarzający. Sposób sformułowania art. 108 pozwala również na stwierdzenie, że opisany w nim czyn zabroniony może być popełnione jedynie z winy umyślnej.

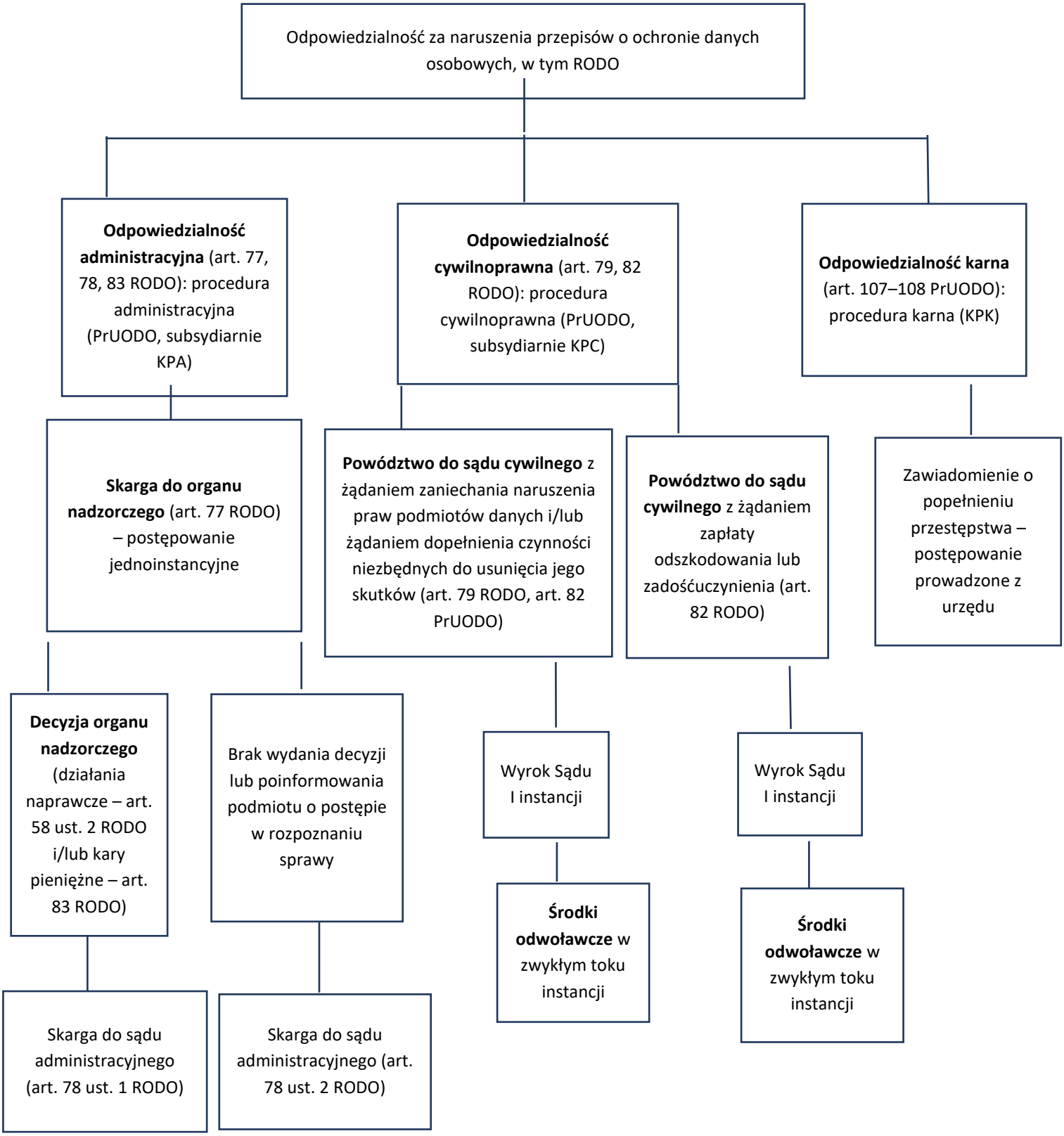
Z kolei w art. 108 PrUODO wprowadzono inny występek, który zgodnie z tym przepisem polegać ma na udaremnieniu lub utrudnieniu kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych.

7.5 Znaczenie przepisów o odpowiedzialności prawnej za naruszenie przepisów o ochronie danych osobowych dla radcy prawnego lub adwokata

Przepisy RODO oraz PrUODO statuujące odpowiedzialność za naruszenie przepisów o ochronie danych osobowych mogą mieć dwojakiego rodzaju znaczenie dla radcy prawnego lub adwokata. Po pierwsze, mogą oni – jak administratorzy lub podmioty przetwarzające – ponosić odpowiedzialność administracyjną, cywilną lub karną. Po drugie, mogą występować w tych postępowaniach jako pełnomocnicy, a w przypadku adwokatów – również jako obrońcy w sprawach karnych.

7.6 Podsumowanie

Z punktu widzenia roszczeń przysługujących podmiotowi danych w przypadku naruszenia przepisów RODO proceduralne możliwości ich dochodzenia przedstawiają się następująco:


Odpowiedzialność za naruszenia przepisów o ochronie danych osobowych, w tym RODO
Odpowiedzialność administracyjna (art. 77, 78, 83 RODO): procedura administracyjna (PrUODO, subsydiarnie KPA)
Odpowiedzialność cywilnoprawna (art. 79, 82 RODO): procedura cywilnoprawna (PrUODO, subsydiarnie KPC)
Odpowiedzialność karna (art. 107–108 PrUODO): procedura karna (KPK)
Skarga do organu nadzorczego (art. 77 RODO) – postępowanie jednoinstancyjne
Powództwo do sądu cywilnego z żądaniem zaniechania naruszenia praw podmiotów danych i/lub żądaniem dopełnienia czynności niezbędnych do usunięcia jego skutków (art. 79 RODO, art. 82 PrUODO)
Powództwo do sądu cywilnego z żądaniem zapłaty odszkodowania lub zadośćuczynienia (art. 82 RODO)
Zawiadomienie o popełnieniu przestępstwa – postępowanie prowadzone z urzędu
Decyzja organu nadzorczego (działania naprawcze – art. 58 ust. 2 RODO i/lub kary pieniężne – art. 83 RODO)
Brak wydania decyzji lub poinformowania podmiotu o postępie w rozpoznaniu sprawy
Wyrok Sądu I instancji
Wyrok Sądu I instancji
Skarga do sądu administracyjnego (art. 78 ust. 1 RODO)
Skarga do sądu administracyjnego (art. 78 ust. 2 RODO)
Środki odwoławcze w zwykłym toku instancji
Środki odwoławcze w zwykłym toku instancji

8. Załączniki do poradnika dla radców prawnych i adwokatów dotyczącego RODO

Załącznikami do poradnika są wzory następujących dokumentów mających na celu wdrożenie RODO:

- Wzór klauzuli informacyjnej zgodnej z RODO (przykład: klauzula dla kandydata do pracy)
- Wzór umowy powierzenia przetwarzania danych osobowych
- Wzór dokumentu upoważnienia do przetwarzania danych osobowych
- Wzór rejestru czynności przetwarzania danych osobowych prowadzonego przez administratora (dla dwóch przykładowych czynności przetwarzania)
- Wzór ewidencji naruszeń ochrony danych
- Wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu jej danych osobowych
- Wzór dokumentu wyznaczenia inspektora ochrony danych

8.1 Wzór klauzuli informacyjnej (przykład: klauzula dla kandydata do pracy)

Wyjaśnienie

Poniższe klauzule informacyjne przygotowane są w sposób „warstwowy", tj. w pierwszej kolejności wskazane są podstawowe informacje dotyczące przetwarzania (w tabeli), a następnie wyliczone są szczegółowe informacje dotyczące przetwarzania. Warstwa podstawowa powinna być przedstawiana w momencie i w miejscu zbierania danych (np. na formularzu), natomiast warstwa szczegółowa może być umieszczona w innym miejscu (np. na dedykowanej stronie internetowej, na odrębnej kartce), pod warunkiem że osoba, której dane dotyczą, ma do niej dostęp podczas podawania danych.

Podział klauzuli informacyjnej na warstwy rekomendowany jest przez hiszpański organ nadzorczy, a także przez Grupę Roboczą Artykułu 29.

Informacje podstawowe dotyczące przetwarzania danych osobowych kandydatów do pracy	
Administrator danych	Kancelaria Prawna
Cele przetwarzania	• ocena kwalifikacji kandydata do pracy w Kancelarii na określonym stanowisku • ocena zdolności i umiejętności kandydata potrzebnych do pracy w Kancelarii na określonym stanowisku • wybór odpowiedniej osoby lub odpowiednich osób do zatrudnienia w Kancelarii
Podstawy prawne przetwarzania	• obowiązek prawny • umowa o pracę • Twoja zgoda • nasz uzasadniony interes
Odbiorcy danych	Podmioty przetwarzające dane w imieniu Kancelarii
Prawa związane z przetwarzaniem danych	• prawo wycofania zgody na przetwarzanie danych • prawo dostępu do danych osobowych oraz prawo żądania ich sprostowania, ich usunięcia lub ograniczenia ich przetwarzania • inne prawa określone w informacji szczegółowej
Szczegółowe informacje	***link do szczegółowej warstwy informacji***

Szczegółowe informacje dotyczące przetwarzania danych kandydatów do pracy

1. Administrator danych osobowych

Administratorem Twoich danych osobowych będzie Kancelaria Prawna z siedzibą w Warszawie (dalej: my). Możesz się z nami skontaktować w następujący sposób:

- listownie na adres: ul. Kancelaryjna 1, 00-001 Warszawa
- przez e-mail: biuro@kancelaria

- telefonicznie: 22 101 00 00
- [*ewentualnie inne kanały kontaktu do uzupełnienia*].

2. Inspektor ochrony danych

Wyznaczyliśmy inspektora ochrony danych. Jest to osoba, z którą możesz się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych. Z inspektorem możesz się kontaktować w następujący sposób:

- listownie na adres: ul. Kancelaryjna 1, 00-001 Warszawa
- przez e-mail: iod@kancelaria
- telefonicznie: 22 101 00 00

3. Cele przetwarzania oraz podstawa prawna przetwarzania

Będziemy przetwarzać Twoje dane osobowe, aby:

- ocenić Twoje kwalifikacje do pracy na stanowisku, na które aplikujesz;
- ocenić Twoje zdolności i umiejętności potrzebne do pracy na stanowisku, na które aplikujesz;
- wybrać odpowiednią osobę do pracy u nas.

Podstawą prawną przetwarzania Twoich danych osobowych jest:

- Przepis prawa (art. 22^1 § 1 kodeksu pracy) i przetwarzanie potrzebne do zawarcia umowy o pracę – w zakresie następujących danych: imię i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia.
- Twoja zgoda na przetwarzanie danych przekazanych w CV i w liście motywacyjnym, jeżeli przekazujesz nam dane inne niż: imię i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia.
- Nasz uzasadniony interes – w zakresie danych zebranych podczas rozmowy kwalifikacyjnej oraz wyników testów kwalifikacyjnych. Mamy uzasadniony interes w tym, aby sprawdzić Twoje umiejętności i zdolności – jest to nam potrzebne do oceny, czy jesteś odpowiednią osobą na stanowisko, na które rekrutujemy.

4. Wykorzystywanie testów kwalifikacyjnych

W ramach rekrutacji przeprowadzamy następujące testy dotyczące znajomości przepisów prawa oraz umiejętności rozwiązywania kazusów prawniczych. Takie testy mają na celu sprawdzenie, czy masz umiejętności potrzebne do pracy na stanowisku, na które aplikujesz.

5. Okres przechowywania danych osobowych

Będziemy przechowywać Twoje dane osobowe do momentu zakończenia rekrutacji na stanowisko, na które aplikujesz.

6. Odbiorcy danych

Będziemy przekazywać Twoje dane osobowe:

- naszym dostawcom, którym zlecimy usługi związane z przetwarzaniem danych osobowych, np. dostawcom usług IT. Takie podmioty przetwarzają dane na podstawie umowy z nami i tylko zgodnie z naszymi poleceniami.

7. Twoje prawa związane z przetwarzaniem danych osobowych i podejmowaniem zautomatyzowanych decyzji

Przysługują Ci następujące prawa związane z przetwarzaniem danych osobowych:

a. prawo wycofania zgody na przetwarzanie danych;
b. prawo dostępu do Twoich danych osobowych;
c. prawo żądania sprostowania Twoich danych osobowych;
d. prawo żądania usunięcia Twoich danych osobowych;
e. prawo żądania ograniczenia przetwarzania Twoich danych osobowych;
f. prawo wyrażenia sprzeciwu wobec przetwarzania Twoich danych ze względu na Twoją szczególną sytuację – w przypadkach kiedy przetwarzamy Twoje dane na podstawie naszego prawnie uzasadnionego interesu;
g. prawo do przenoszenia Twoich danych osobowych, tj. prawo otrzymania od nas Twoich danych osobowych w ustrukturyzowanym, powszechnie używanym formacie informatycznym nadającym się do odczytu maszynowego. Możesz przesłać te dane innemu administratorowi danych lub zażądać, abyśmy przesłali Twoje dane do innego administratora. Jednakże zrobimy to tylko wówczas, jeśli takie przesłanie jest technicznie możliwe. Prawo do przenoszenia danych osobowych przysługuje Ci tylko co do tych danych, które przetwarzamy na podstawie umowy z Tobą lub na podstawie Twojej zgody,

Aby skorzystać z powyższych praw, skontaktuj się z nami lub z naszym inspektorem ochrony danych (dane kontaktowe w punktach 1 i 2 powyżej [*link*]).

<u>Prawo wycofania zgody</u>

W zakresie, w jakim Twoje dane są przetwarzane na podstawie zgody (czyli dane przekazane w CV i w liście motywacyjnym, inne niż: imię i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania, wykształcenie, przebieg dotychczasowego zatrudnienia), masz prawo wycofania zgody na przetwarzanie danych w dowolnym momencie. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem. Zgodę możesz wycofać poprzez wysłanie oświadczenia o wycofaniu zgody na nasz adres korespondencyjny, nasz adres emailowy, a także poprzez niniejszy link [*link*].

Prawo wniesienia skargi do organu

Przysługuje Ci także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych.

8.2 Wzór umowy powierzenia przetwarzania danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w _____

pomiędzy

_____, zwanym dalej „Administratorem"

a

_____, zwanym dalej „Przetwarzającym"

1. DEFINICJE

Dla potrzeb niniejszej umowy Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1) **Umowa Powierzenia** – niniejsza umowa;

2) **Umowa Główna** – [*umowa, w związku z którą zawierana jest umowa powierzenia – przetwarzanie danych jest konieczne do wykonania Umowy Głównej*]

3) **RODO** – rozporządzenie 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) (Dz. Urz. UE L z 2016 r. nr 119, str. 1).

2. OŚWIADCZENIA STRON

Strony oświadczają, że Umowa Powierzenia została zawarta w celu wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy Głównej.

3. PRZEDMIOT UMOWY

3.1. W trybie art. 28 ust. 3 RODO Administrator powierza Przetwarzającemu do przetwarzania dane osobowe wskazane w pkt 4.1.–4.2. poniżej, a Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem i Umową Powierzenia.

3.2. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie Powierzenia oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora drogą elektroniczną na adres _____ lub na piśmie.

4. CEL, ZAKRES I CHARAKTER PRZETWARZANIA

4.1. Przetwarzający zobowiązuje się do przetwarzania danych osobowych następujących kategorii osób, których dane dotyczą:

a) _____

b) _____

4.2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:

a) co do [*kategoria osób*]:

i. _____

b) co do [*kategoria osób*]:

i. _____

4.3. Celem przetwarzania danych osobowych wskazanych w pkt 4.1–4.2 powyżej jest wykonanie Umowy Głównej, w szczególności _____.

4.4. Przetwarzający zobowiązuje się do przetwarzania danych osobowych w sposób stały. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: _____. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych oraz w formie papierowej.

4.5. Przetwarzający będzie zbierał/otrzymywał dane osobowe od _____ [*sposób, źródła zbierania danych*].

5. ZASADY POWIERZENIA PRZETWARZANIA

5.1. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a w szczególności:

a) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z Administratorem;

b) zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora w celach i zakresie przewidzianym w Umowie Powierzenia;

c) prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO, i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

5.2. Przetwarzający zapewnia, aby osoby mające dostęp do przetwarzanych danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania

tajemnicy istnieje również po realizacji Umowy Powierzenia oraz ustaniu zatrudnienia u Przetwarzającego.

6. DALSZE OBOWIĄZKI PRZETWARZAJĄCEGO

6.1. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32–36 RODO.

6.2. W sytuacji podejrzenia naruszenia ochrony danych osobowych Przetwarzający zobowiązuje się do:

a) przekazania Administratorowi informacji dotyczących naruszenia ochrony danych osobowych w ciągu 24 godzin od jego wykrycia, w tym informacji, o których mowa w art. 33 ust. 3 RODO;

b) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych;

c) przekazania Administratorowi – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.

6.3. Przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15–22 RODO. W szczególności Przetwarzający zobowiązuje się – na żądanie Administratora – do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora.

6.4. Przetwarzający zobowiązuje się stosować do ewentualnych wskazówek lub zaleceń wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.

6.5. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych przez Przetwarzającego, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych skierowanym do Przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

7. PODPOWIERZENIE PRZETWARZANIA

[*Komentarz: Jeżeli nie przewiduje się możliwości podpowierzenia przetwarzania, należy usunąć postanowienia pkt 7.*]

7.1. Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych danych osobowych podwykonawcom Przetwarzającego (tzw. subprocesorom). Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych swoim podwykonawcom, musi uprzednio poinformować Administratora o zamiarze podpowierzenia oraz o tożsamości

(nazwie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie danych, a także o charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia. O ile Administrator nie wyrazi sprzeciwu wobec podpowierzenia w terminie 7 dni od daty zawiadomienia, Przetwarzający uprawniony będzie do dokonania podpowierzenia.

7.2. W przypadku podpowierzenia przetwarzania danych osobowych podpowierzenie przetwarzania będzie mieć za podstawę umowę, na podstawie której podwykonawca (subprocesor) zobowiąże się do wykonywania tych samych obowiązków, które na mocy Umowy Powierzenia nałożone są na Przetwarzającego. Umowa będzie zawarta w tej samej formie co Umowa Powierzenia.

7.3. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy (subprocesora). W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia Przetwarzający poinformuje o tym fakcie Administratora w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

7.4. Przetwarzający nie może przekazywać powierzonych mu przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego.

8. AUDYT PRZETWARZAJĄCEGO

8.1. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz Umowy Powierzenia przez Przetwarzającego, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych.

8.2. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub inspekcje, o których mowa w zdaniu poprzedzającym, mogą być przeprowadzane przez podmioty trzecie upoważnione przez Administratora.

8.3. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane jemu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

9. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA

9.1. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.

10. POSTANOWIENIA KOŃCOWE

_____

_____

8.3 Wzór dokumentu upoważnienia do przetwarzania danych osobowych

……., dnia ..... 20..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

Niniejszym, zgodnie z art. 5 ust. 1 lit. f) w zw. z art. 29 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 (ogólnego rozporządzenia o ochronie danych) (dalej jako „RODO"),

upoważniam

Panią/Pana: .....

Stanowisko: .....

do przetwarzania danych osobowych w *podać nazwę podmiotu* (dalej jako „Kancelaria") w następującym zakresie:

A. Okres upoważnienia:

- na okres zatrudnienia w Kancelarii */ do dnia …… włącznie*

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych:

  ……

- system informatyczny oraz urządzenia wchodzące w jego skład:

  …….

  (bez ograniczeń*, podgląd danych*, wprowadzanie danych*, opracowywanie danych*, zmienianie danych*, usuwanie danych*, na komputerach przenośnych*).

- dane osobowe przetwarzane w ramach udziału w następujących czynnościach przetwarzania danych:
  a) *podać nazwę czynności (procesu) zgodnie z rejestrem czynności*
  b) ……

c) ……

.....

Imię, nazwisko i podpis

/zgodnie z zasadami reprezentacji/

* niepotrzebne usunąć

8.4 Wzór rejestru czynności przetwarzania danych osobowych prowadzonego przez administratora

Rejestr czynności – odrębny plik Excel w wariantach dla dwóch czynności (procesów) przetwarzania danych.

8.5 Wzór ewidencji naruszeń ochrony danych

Wyjaśnienie

Zgodnie z art. 33 ust. 5 RODO administrator ma obowiązek dokumentowania wszystkich naruszeń ochrony danych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych. Grupa Robocza Artykułu 29 rekomenduje utworzenie wewnętrznego rejestru naruszeń ochrony danych. Poniżej w formie tabeli podany jest przykładowy zakres informacji, który powinien znaleźć się w rejestrze naruszeń.

1	2	3	4	5	6	7
Administrator (nazwa, adres siedziby)	Jeżeli do naruszenia doszło u podmiotu przetwarzającego – wskazanie nazwy i adresu podmiotu	Data i godzina wystąpienia incydentu prowadzącego do naruszenia	Data i godzina stwierdzenia naruszenia	Miejsce incydentu prowadzącego do naruszenia	Nośniki danych osobowych, których dotyczy naruszenie	Charakter naruszenia ochrony danych (opis incydentu/naruszenia ochrony danych)

8	9	10	11	12	13	14
Kategorie osób, których danych osobowych dotyczy naruszenie	Przybliżona liczba osób, których danych osobowych dotyczy naruszenie	Kategorie danych osobowych, których dotyczy naruszenie	Przybliżona liczba wpisów (rekordów) danych osobowych, których dotyczy naruszenie	Możliwe konsekwencje naruszenia ochrony danych osobowych dla osób fizycznych	Środki zastosowane w celu zaradzenia naruszeniu ochrony danych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków	Ocena ryzyka naruszenia praw i wolności osób fizycznych wynikającego z naruszenia ochrony danych

15	16	17	18	19	20
Czy naruszenie zostało zgłoszone do organu nadzorczego	Jeżeli tak: data i godzina zgłoszenia naruszenia do organu nadzorczego i link do treści zgłoszenia	Jeżeli nie: wyjaśnienie powodów braku zgłoszenia naruszenia do organu nadzorczego	Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu ochrony danych	Jeżeli tak: sposób i data wysłania zawiadomienia oraz link do jego treści	Jeżeli nie: wyjaśnienie powodów braku zawiadomienia osób, których dane dotyczą

8.6 Wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu jej danych osobowych

Kancelaria Prawna
ul. Kancelaryjna 1
00-001 Warszawa
biuro@kancelaria

Zawiadomienie o naruszeniu ochrony Pani danych osobowych

Szanowna Pani,

W ostatnich dniach doszło do incydentu, wskutek którego Pani dane osobowe mogły znaleźć się w posiadaniu osób nieupoważnionych. Poniżej przekazujemy informacje dotyczące tego incydentu, a także działań, jakie w związku z tym podejmujemy. Podajemy też informacje o krokach, które Pani może podjąć w związku z incydentem. Prosimy o uważną lekturę niniejszego zawiadomienia.

Co się stało?

Dnia ... omyłkowo wysłaliśmy wystawioną na Panią fakturę za nasze usługi do innego klienta. Chodzi tutaj o fakturę dotyczącą reprezentowania Pani w postępowaniu sądowym w sprawie o zapłatę przeciwko Budowanie Domów sp. z o.o.

Faktura zawierała następujące dane osobowe dotyczące Pani: imię i nazwisko, numer NIP, adres zamieszkania, informację na temat świadczonych przez nas usług (reprezentowanie w postępowaniu sądowym przeciwko Budowanie Domów sp. z o.o.) oraz kwotę do zapłaty.

Możliwe konsekwencje dla Pani

Wskutek wysłania faktury wystawionej na Pani może dojść do tego, że dostęp do tych danych uzyska osoba nieupoważniona. Osoba ta miałaby więc informacje o Pani imieniu i nazwisku, adresie zamieszkania, numerze NIP, a także informacje o tym, że między Panią a Budowanie Domów sp. z o.o. toczy się sprawa o zapłatę. Ponadto na fakturze widnieje kwota do zapłaty, co może pośrednio dotyczyć Pani zobowiązań finansowych.

Na chwilę obecną nie mamy żadnych sygnałów, że dokument z Pani danymi został gdzieś upubliczniony lub jest wykorzystywany przez osobę niepowołaną. Istnieje jednakże ryzyko, że ktoś będzie próbował wykorzystać Pani dane osobowe w celu podszycia się pod Panią (tzw. kradzież tożsamości). Rozumiemy także, że upublicznienie Pani danych osobowych mogłoby wywołać u Pani stres lub inne negatywne odczucia.

Działania podjęte przez nas

Wysłaliśmy zawiadomienie do naszego klienta, któremu omyłkowo wysłaliśmy fakturę przeznaczoną dla Pani. Wyjaśniliśmy klientowi, że faktura została do niego wysłana omyłkowo i poprosiliśmy o jej zniszczenie lub odesłanie do nas. Gdy tylko otrzymamy odpowiedź od naszego klienta z potwierdzeniem zniszczenia faktury lub jeśli klient odeśle nam fakturę, poinformujemy Panią o tym.

Na bieżąco monitorujemy, czy Pani dane zostały gdzieś upublicznione lub wykorzystane przez osobę nieuprawnioną. Na chwilę obecną nie mamy żadnych sygnałów o takim nieuprawnionym wykorzystaniu Pani danych lub o ich upublicznieniu.

Co może Pani zrobić?

W związku z ryzykiem kradzieży tożsamości prosimy o ostrożność przy podawaniu Pani danych osobowych innym osobom. Dotyczy to szczególnie podawania danych za pośrednictwem Internetu lub przez telefon.

Jeżeli dowie się Pani o upublicznieniu lub wykorzystaniu Pani danych przez osobę nieuprawnioną, bardzo prosimy o natychmiastowe przekazanie nam tej informacji.

Więcej informacji

Jeżeli ma Pani jakiekolwiek pytania lub chciałaby nam Pani przekazać dodatkowe informacje w związku z zagubieniem dokumentu z Pani danymi osobowymi, prosimy o kontakt z naszym inspektorem ochrony danych – p. Janem Nowakiem. Poniżej podajemy dane kontaktowe inspektora ochrony danych:
Adres email: iod@kancelaria
Numer telefonu: 22 101 00 00
Adres korespondencyjny: Kancelaria Prawna
DW: Inspektor ochrony danych
ul. Kancelaryjna 1, 00-001 Warszawa

8.7 Wzór dokumentu wyznaczenia inspektora ochrony danych

Wyznaczenie inspektora ochrony danych

w *podać nazwę podmiotu*

W imieniu *podać nazwę podmiotu* na podstawie art. 37 ust. 1 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 (ogólnego rozporządzenia o ochronie danych) (dalej jako „RODO"),

wyznacza Panią/Pana *imię i nazwisko* na inspektora ochrony danych (dalej jako „Inspektor") w *podać nazwę podmiotu*.

Inspektor będzie wykonywał zadania określone w RODO, w szczególności w art. 39 i art. 47 ust. 2 pkt h), oraz zadania określone na podstawie art. 38 ust. 6 RODO *wymienić zadania IOD inne niż wykonywane na podstawie art. 39 i art. 47 ust. 2 pkt h) RODO, jeżeli dotyczy.*

Inspektor pełni swoją funkcję do *data wygaśnięcia* lub aż do wyraźnego odwołania przez administratora danych z innych przyczyn niż wypełnianie zadań Inspektora, lub aż do wyraźnej rezygnacji Inspektora z tej funkcji.

Niniejsze wyznaczenie wchodzi w życie z dniem 25 maja 2018 r.

……..

Imię, nazwisko i podpis

/zgodnie z zasadami reprezentacji/

9. Przydatne materiały

9.1 Wytyczne i opinie Grupy Roboczej Artykułu 29

a) Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169), wersja po zmianach z dnia 16 lutego 2010 r.

b) Wytyczne dotyczące prawa do przenoszenia danych (WP 242), wersja po zmianach z dnia 5 kwietnia 2017 r.

c) Wytyczne dotyczące inspektorów ochrony danych (WP 243), wersja po zmianach z dnia 5 kwietnia 2017 r.

d) Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244), wersja po zmianach z dnia 5 kwietnia 2017 r.

e) Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 679/2016 (WP 248), wersja po zmianach z dnia 4 października 2017 r.

f) Opinia 2/2017 w sprawie przetwarzania danych w pracy (WP 249), wersja po zmianach z dnia 8 czerwca 2017 r.

g) Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania (WP 251), wersja po zmianach z dnia 6 lutego 2018 r.

h) Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 (WP 250), wersja po zmianach z dnia 6 lutego 2018 r.

i) Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 (WP 253), wersja po zmianach z dnia 3 października 2017 r.

j) Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP259), wstępna wersja z dnia 12 grudnia 2017 r.

k) Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 (WP260), wstępna wersja z dnia 12 grudnia 2017 r.

9.2 Materiały GIODO i Ministerstwa Cyfryzacji

1) GIODO, *Kiedy trzeba przeprowadzić ocenę skutków dla ochrony danych? Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków*, dostępne pod adresem: https://giodo.gov.pl/pl/1520281/10430.

2) GIODO, *Jak rozumieć i stosować podejście oparte na ryzyku?*, poradnik dostępny pod adresem: https://giodo.gov.pl/pl/1520282/10294

3) Stanowisko GIODO w sprawie w sprawie skuteczności zgód, dostępne pod adresem: https://giodo.gov.pl/en/1520281/10303.

4) GIODO, *Jak można prowadzić rejestr czynności przetwarzania danych oraz rejestr kategorii czynności?*, wyjaśnienia i wskazówki GIODO dotyczące sposobu realizacji określonego w art. 30 RODO obowiązku prowadzenia rejestru czynności oraz kategorii czynności wraz

szablonami obu typów rejestrów i przykładami ich uzupełnienia, dostępne pod adresem: https://giodo.gov.pl/pl/1520281/10449.

5) Ministerstwo Cyfryzacji, *Informator RODO*, dostępny pod adresem: https://www.gov.pl/documents/31305/436699/RODO.pdf/9b7e519b-0d5c-1ef8-4caf-02f8d247aa1d.

9.3 Komentarze i inne publikacje

a) E. Bielak-Jomaa, D. Lubasz (red.), *Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

b) P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017.

c) R. Jay, *Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice*, Sweet & Maxwell 2017.

d) G. Sibiga, K. Syska, *Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów oraz wzorów rejestru czynności przetwarzania*, Warszawa 2017.

e) G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016.