RODO- nowe regulacje w zakresie danych osobowych - cele, założenia implementacja w Polsce

I.Zasady i zakres zastosowania rozporządzenia Parlamentu Europejskiego i Rady Europejskiej 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.U.UE.L.2016.119.1 (zwanego dalej rozporządzeniem).

II. Podstawowe polityki celowościowe ochrony danych.

III. Cele ochronne: uprawnienia organów, skargi i sankcje.

I.Zasady i zakres zastosowania rozporządzenia Parlamentu Europejskiego i Rady Europejskiej 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.U.UE.L.2016.119.1 (zwanego dalej rozporządzeniem).

Parlament Europejski i Rada Europejska w dniu 27 kwietnia 2016 r. przyjęły rozporządzenie 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), opublikowane w Dz.U.UE.L.2016.119.1, z mocą obowiązywania od dnia 25 maja 2018r.

Celem rozporządzenia jest ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jako jednego z praw podstawowych chronionych prawnie.

Zakres podmiotowy reguluje przepis art. 1 i art. 2 rozporządzenia. Zgodnie z treścią art. 1 rozporządzenie ma ono zastosowanie do danych osobowych poddanych procesowi przetwarzania oraz podlegających swobodnemu przepływowi. Ochrona w zakresie podmiotowym przysługuje wyłącznie osobom fizycznym z pominięciem osób prawnych i ułomnych osób prawych.

Stosownie do treści rozporządzenia uprawnienia i instrumenty ochronne przewidziane w treści rozporządzenia przysługują osobom fizycznym.

Co do aspektu przedmiotowego i terytorialnego omówienie tego zagadnienia połączone jest z odniesieniem się do definicji legalnych rozporządzenia (art. 4 pkt. 1, 2 i 6). definicji danych osobowych, zbioru danych i procesu przetwarzania.

Definicje legalne w treści rozporządzenia dookreślają pojęcie dane osobowe, zbiór danych oraz pojęcie przetwarzania.

Pod pojęciem **danych osobowych** rozumie się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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.

Katalog faktorów identyfikujących jest otwarty i obejmuje obok wskazanych wyżej faktory takiej jak: „numer pesel, serię i numer dowodu tożsamości, fotografię (wizerunek twarzy to jedna z danych biometrycznych), imię i nazwisko małżonka, numer telefonu, adres e-mail, numer rejestracyjny samochodu, wzór podpisu, numer rachunku bankowego, numer karty kredytowej, dane o lokalizacji, identyfikatory internetowe (nick, IP komputera[1] – Internet Protocol Adress) oraz czynniki określające ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, data i miejsce urodzenia, obywatelstwo, stan cywilny i rodzinny, wykształcenie, stan majątkowy, formę zatrudnienia, dochody i wydatki, liczbę osób w gospodarstwie, ustrój majątkowy małżonków, miejsce pracy, zawód, skazanie za przestępstwo, zachowania konsumenta lub użytkownika strony internetowej, czynniki określające fizyczną, fizjologiczną, genetyczną lub psychiczną tożsamość osoby fizycznej[2]”.

Rozporządzenie zawiera w swej treści definicję: danych genetycznych, biometrycznych oraz danych dotyczących zdrowia (art. 4 pkt. 13, 14 i 15).

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.

Zbiór danych oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Natomiast proces **przetwarzania** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie,

---

1 wyrok Trybunału Sprawiedliwości EU z 19 października 2016 r. w sprawie Patrick Breyer przeciwko Niemcom (C-582/14), Dz.U.UE.C.2016.475.3/1.

2 Mariusz Krzysztofek, Ochrona danych osobowych w Unii Europejskiej po reformie, Wydawnictwo CH Beck, Warszawa 2016, str. 43.

porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Przetwarzanie może odbywać się w postaci papierowej, elektronicznej, automatycznie lub ręcznie. [3] Warunki wyrażania zgody na przetwarzanie danych zawarte są w rozporządzeniu wprost. Jeżeli przetwarzanie danych odbywa się na podstawie zgody (art. 7) administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych **i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia**. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. **Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.** Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Proces przetwarzania danych winien być realizowany w odwołaniu się do zasad:

-zasady przetwarzania danych zgodnie z prawem (art. 9 – rozporządzenie statuuje zasadę przetwarzanie danych osobowych w ściśle oznaczonych sytuacjach).
- zasady przetwarzania danych za zgodą. (art. 7).
-zasady rzetelności i prawidłowości. (zasada przetwarzania danych aktualnych, poprawnych, i w procesie niepodlegającym bez zakłóceń).

[3] Vademecum ABI. Część II – Przygotowanie do roli Inspektora Danych Osobowych, Wydawnictwo CH Beck, Warszawa 2017, str. 86.

-zasady ograniczenia celu (zasada przetwarzania danych w konkretnym, wyraźnie i prawnie uzasadnionym celu)[4].
-zasada minimalizacji danych (zasada kolekcjonowania danych w ograniczeniu do minimum niezbędnego dla realizacji założonego celu).
-zasada integralności i poufności (zasada przetwarzania danych z odniesieniu do ich nienaruszalności i spójności oraz ich udostępniania wyłącznie osobom uprawnionym).

Wobec wyjaśnienia definicyjnego wskazać należy materialny zakres przeznaczenia rozporządzenia. Jak wynika z art. 2 rozporządzenie ma ono 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.

„Należy podkreślić, że zgodnie z literalnym brzmieniem tego przepisu, który należy poddać dalszej interpretacji – dane przetwarzane w sposób inny niż zautomatyzowany, a więc poza systemami informatycznymi, podlegają RODO pod warunkiem, że stanowią lub mają stanowić część zbioru danych[5]".

Orzecznictwo Sądu Najwyższego stoi na straży szerokiej ochrony danych przyjmując, że: „dane osobowe korzystają z ochrony już wówczas, jeżeli tylko mogą znaleźć się w zbiorze danych osobowych, bez względu na to, czy się w nim ostatecznie znalazły, ... Rzecz, bowiem w tym, że każdy ma prawo do ochrony dotyczących go danych osobowych, a nie jedynie ten, czyje dane znalazły się już w zbiorze[6].

Regulacja unijna wyłącza jej zastosowanie między innymi do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa 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.

Terytorialnie rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Rozporządzenie ma zastosowanie także do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

---

[4] Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych, Deloitte 2017, str. 11 i n.

[5] Mariusz Krzysztofek, Ochrona danych osobowych w Unii Europejskiej po reformie, Wydawnictwo CH Beck, Warszawa 2016, str. 31.

[6] Postanowienie Sądu Najwyższego z dnia 11 grudnia 2000 r. II KKN 438/00, program prawniczy LEX Wolters Kluver.

„Przełomową zmianę, którą wprowadza RODO, jest ochrona danych osobowych niezależnie od miejsca ich przetwarzania (protection regardless of data location). Relewantną zmianą , które przyniosło RODO jest stosowanie go do danych osobowych osób przebywających w UE przez administratora lub processora, którzy nie mają na jej terytorium jednostek organizacyjnych, ale ich czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii - niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii”[7]. (art. 3 ust. 2).

Dodatkowo, jeżeli zastosowanie ma art. 3 ust. 2, administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii.

II. Podstawowe polityki celowościowe ochrony danych.

W katalogu pojęć rozporządzenia w podstawowej ich grupie zamieszczono pojęcia: profilowanie i pseudonimizacja. (art. 4 pkt. 4 i 5), pojęcia privacy by design, privacy by default (art. 25 ust. 1 i 2 rozporządzenia) oraz pojęcie privacy impact assessment (art. 35 jako pojęcia przedmiotowo istotne w zakresie realizacji polityki zabezpieczania.

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

„Nowa regulacja ułatwi osobom, których dane dotyczą wyłączenie swoich danych spod profilowania. Zmiana wpłynie, więc niekorzystnie na podmioty proponujące usługi marketingu online, śledzenia konsumenta oraz reklamy online. Zgodnie, bowiem z przepisami Rozporządzenia osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji, która ocenia jej czynniki osobowe, opierając się wyłącznie na przetwarzaniu zautomatyzowanym. Tego typu decyzje mogą wywoływać skutki prawne lub w podobny sposób znacząco wpływać na sytuację osoby, której dane dotyczą. Skutkiem zautomatyzowanego przetwarzania danych może być na przykład odrzucenie elektronicznego wniosku kredytowego. Może być ono również wykorzystywane podczas elektronicznych metod rekrutacji niewymagającej interwencji ludzkiej. Mechanizm podejmowania takich decyzji określa się jako profilowanie. Jako ograniczające uznaje się formy zautomatyzowanego przetwarzania danych osobowych, polegającego na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Zakazane będzie każde

[7] Mariusz Krzysztofek, Ochrona danych osobowych w Unii Europejskiej po reformie, Wydawnictwo CH Beck, Warszawa 2016, str. 35.

profilowanie które (i) wywołuje wobec osoby skutki prawne lub (ii) w podobny sposób istotnie na niego wpływa i które nie ma podstawy prawnej. Ta definicja jest znacznie szersza niż przewidziana w Dyrektywie. W rezultacie legalne obecnie czynności profilowania mogą stać się zakazane przez Rozporządzenie. Wydaje się, więc, iż w praktyce jedyną możliwością prowadzenia profilowania będzie uzyskanie wyraźnej zgody osoby na profilowanie, co oznacza że samo wyrażenie zgody na profilowanie za pomocą klauzuli zawartej w regulaminie nie będzie prawnie skuteczne". [8]

Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

„Pseudonimizacja danych i szyfrowanie powinno być przeprowadzone na podstawie analizy ryzyka. Realizacja tych elementów może być stosowana poprzez różne techniki, w tym m.in. tzw. scrambling, maskowanie danych (np. w środowiskach testowych wytwarzanych aplikacji), ich zaciemnianie (obfuscation), a także ich szyfrowanie podczas przechowywania i przekazywania w celu zapewnienia poufności, integralności i autentyczności. Dotyczy to w szczególności cyklu życia tworzenia aplikacji (środowiska testowe/produkcyjne), ale również przetwarzania w aplikacjach i bazach danych. Procesy zarządcze wspierające te elementy mogą uwzględniać m.in. sposoby zarządzania wykorzystywanym systemem kryptograficznym, w tym np. kluczami kryptograficznymi". [9]

Dookreślenie pojęcia **privacy by design** zamieszczone jest w art. 25 ust. 1 rozporządzenia. 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 wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania -wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Zgodnie z treścią dyspozycji art. 25 ust. 1 administrator danych jest zobowiązany na etapie projektowania rozwiązań lub ich zastosowania w zakresie przetwarzania danych zapewnić odpowiednie środki techniczne i organizacyjne, która mają na celu realizowanie polityki ochrony danych osobowych i ich zgodności z RODO. Wśród tych środków protekcyjnych wskazać należy między innymi: przeprowadzania testów bezpieczeństwa, wycofywania z użycia aplikacji lub ich udoskonalania, monitorowania stanu zabezpieczeń, zastosowanie mechanizmów certyfikacji.

---

[8] Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych, Deloitte 2017, str. 18.

[9] Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych, Deloitte 2017, str. 18.

Privacy by default (art. 25 ust. 1 i 2 rozporządzenia) reguluje art. 25 ust. 2 wprowadzając w swej treści dyspozycję zgodnie, z którą administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. „W tym kontekście istotne jest zapewnienie inwentaryzacji danych i wdrożenie środków bezpieczeństwa zgodnie z wykonaną oceną profilu ryzyka i krytyczności danych[10]". Możliwe jest wejście w procedurę certyfikacji (art. 42 rozporządzenia).

Procedura oceny skutków dla ochrony danych (art. 35) (privacy impact assessment) stanowi, że jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania **dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych**. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Ocena skutków dla ochrony danych jest wymagana w szczególności 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.

Ocena zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora, ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, ocenę ryzyka naruszenia praw lub wolności osób oraz 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.

„Z punktu widzenia bezpieczeństwa, ocena ryzyka prywatności powinna dotyczyć wszystkich wykorzystywanych aplikacji i wspomagającej je infrastruktury (w tym ich tworzenia, a także zmiany). Ocena ryzyka w tym zakresie powinna identyfikować potencjalne ryzyka dla

[10] Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych, Deloitte 2017, str. 20.

zasobów, a także definiować procesy (przydzielanie uprawnień, przegląd uprawnień, procesy monitorowania i reagowania na incydenty) i środki je ograniczające (np. zasady bezpiecznego tworzenia kodu, procesy bezpieczeństwa przy tworzeniu aplikacji, testy penetracyjne, bezpieczną konfigurację infrastruktury)[11].

III. Cele ochronne : uprawnienia organów, skargi i sankcje.

Uprawnionemu, którego dane osobowe przetwarzane zostały niezgodnie z zasadami statuowanymi w rozporządzeniu przysługuje:

- prawo do wniesienia skargi do organu nadzorczego (art. 77) - każda 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, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie.

-**prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu (art. 78)** - każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.

-prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu (art. 79) - każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

-p**rawo do odszkodowania (art. 82) -** każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę, wyłącznie, gdy przetwarzający nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom i gdy ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Naruszyciel poddany jest także administracyjnemu reżimowi kar pieniężnych: skutecznych, proporcjonalnych i odstraszających. (art. 83) ważących między innymi:

---

[11] Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych, Deloitte 2017, str. 20.

a). charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
b) umyślny lub nieumyślny charakter naruszenia;
c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
g) kategorie danych osobowych, których dotyczyło naruszenie;

Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 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:

a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 -39 oraz 42 i 43;
b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43;
c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4;

Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 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:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9;
b) praw osób, których dane dotyczą, o których mowa w art. 12-22;
c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44-49;
d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX;
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.

VI 2018r. Magdalena Padzik