Szanowni Państwo.
Oddaję w Państwa ręce skrypt z ochrony danych osobowych, który liczy 136 stron. Przedmiotem egzaminu będą zagadnienia od str. 1 do str. 70.
Pozostała część (od str. 70 do str. 136), zatytułowana DANE OSOBOWE W TYPOWYCH DZIAŁACH FIRMY stanowi materiał uzupełniający dla osób zainteresowanych konkretnym zagadnieniem.

OCHRONA DANYCH OSOBOWYCH

Historia prawa do ochrony danych osobowych

Rozważając tematykę ochrony danych osobowych warto znać i rozumieć przyczyny istnienia takiego prawa i powody, dla których ta problematyka w ostatnich czasach jest taka ważna. W tym celu przedstawię krótki rys historyczny rozwoju regulacji prawnych dotyczących ochrony danych osobowych, podstawowe zagadnienia związane z dobrami osobistymi i prawem do prywatności oraz najważniejsze założenia obowiązującego rozporządzenia RODO i ustawy o ochronie danych osobowych.

Regulacje prawne w tej materii zaczęły pojawiać się już względnie dawno. Analizując ich rozwój widać wyraźnie, że do ich tworzenia przyczyniał się przede wszystkim intensywny rozwój technologii informacyjnych (informatyki). Już kilkadziesiąt lat temu zaczęły powstawać duże zbiory informacji o osobach, które nazywano bankami danych. Możliwość ich przeszukiwania, kojarzenia i analizowania spowodowały, że zauważono w tym obszarze istnienie dużego zagrożenia dla prywatności. Uznano, że jeśliby nie wprowadzono żadnych ograniczeń, zarządzający takim bankiem danych mógłby o określonej osobie zgromadzić dowolną ilość informacji, a w konsekwencji wiedzieć o niej w zasadzie prawie wszystko. Zaistniała więc potrzeba wprowadzania regulacji nakładających pewne ograniczenia na zbieranie i przetwarzanie danych, w tym zasady odpowiedniej ich ochrony zapewniających równocześnie określone prawa osobom, których dane przetwarza się w sposób „zautomatyzowany". Na początku problem stanowiło automatyczne, komputerowe przetwarzanie danych, natomiast później cel ochrony uogólniono, skupiając się na danych dotyczących osób, bez względu na formę ich przetwarzania.

Wpływ uregulowań prawnych dotyczących ochrony danych osobowych na działalność podmiotów publicznych i prywatnych.

W dzisiejszych czasach ochrona danych osobowych staje się jednym z

ważniejszych obowiązków spoczywających na organizacjach, instytucjach i firmach. Przedsięwzięcia dotyczące ochrony danych osobowych należy realizować w oparciu o obowiązujące akty normatywno-prawne, w tym:

- 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).
- 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.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U., poz. 1000 ze zm. oraz akty wykonawcze do niej.

Podstawy prawne w zakresie ochrony danych osobowych

Podstaw do ochrony danych osobowych należy doszukiwać się w Konstytucji Rzeczypospolitej Polskiej uchwalonej dnia 2 kwietnia 1997 r. Na treść Konstytucji wpływ miały bez wątpienia akty europejskie, w tym także treść Dyrektywy 95/46/WE. Konstytucja stanowi swojego rodzaju wzorzec oceny wszystkich innych krajowych aktów prawnych, jest ona *najwyższym prawem Rzeczypospolitej Polskiej*. Rozdział II Konstytucji określa wolności, prawa i obowiązki obywateli względem Państwa, które stanowią podstawę dla regulacji chroniących dane osób (art. 47 Konstytucji RP):

> Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Dane osobowe są elementem życia prywatnego i mogą stanowić o dobrym imieniu osoby, a decydowanie o tym, czy chce się je ujawniać jest jednym z przejawów prawa do prywatności. Prawa te wyrażone są dalej w art. 51 Konstytucji:

> 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Kodeks cywilny w art. 23 wśród dóbr osobistych wymienia przykładowo nazwisko, pseudonim, tajemnicę korespondencji i wizerunek. Dane osobowe można w pewnym stopniu traktować jako dobra osobiste zakładając, że istnieje nierozerwalny, a w dodatku emocjonalny związek osoby z danymi, które jej dotyczą. W pewnym sensie osoba jest właścicielem danych jej dotyczących i powinna mieć możliwość o nich decydować. To prawo może być ograniczone jedynie ustawowo, co Konstytucja wyraźnie akcentuje: *nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby* podkreślając jednocześnie, że *zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.*

Wynika z tego, że przepisy o randze niższej niż ustawa - np. rozporządzenia - nie mogą regulować kwestii legalności przetwarzania danych osobowych.

Wraz z wprowadzeniem przepisów dotyczących ochrony danych osobowych wszyscy obywatele otrzymali potwierdzenie szerokiego katalogu praw:

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

Prawo osoby do kontroli nad tym, kto przetwarza dane jej dotyczące oraz jaki jest ich zakres, a więc z jej punktu widzenia najważniejsze prawo, wyraża się przez:

- obowiązek informowania jej o tym, kto te dane przetwarza,
- prawo informacji o tym, jakie jej dane są przetwarzane,
- możliwość sprostowania danych, ich aktualizacji, bądź usunięcia gdy są

niepełne lub nieprawdziwe,
- możliwość sprzeciwienia się przetwarzaniu danych.

RODO

25 maja 2018 roku weszło w życie tzw. „Rozporządzenie o ochronie danych osobowych" (RODO), które obowiązuje we wszystkich państwach członkowskich Unii Europejskiej, i którego wymogi muszą spełniać wszystkie organizacje przetwarzające dane osobowe.

Przedmiot i cele RODO (art. 1)

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

Materialny zakres stosowania RODO (art. 2)

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

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE (postanowienia dotyczące wspólnej polityki zagranicznej i bezpieczeństwa);

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

Co należy rozumieć przez czynności o czysto osobistym lub domowym charakterze? Chodzi tu o czynności, które pozostają bez związku z działalnością zawodową lub handlową. Tak więc może tu chodzić np. o przechowywanie adresów innych osób w celach prywatnych.

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub

wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.
3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.
4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12-15 tej dyrektywy.

Terytorialny zakres stosowania RODO (art. 3)
1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:
a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii - niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.
3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Rozumienie RODO

Aby móc zrozumieć rozporządzenie o ochronie danych osobowych, trzeba poznać pojęcia, które są w nim użyte. Nie wszystkie można łatwo zrozumieć bezpośrednio z jego treści, szczególnie nie posiadając wykształcenia prawniczego, dlatego warto zapoznać się z najważniejszymi terminami.

Do definicji RODO nie należy się bezwzględnie przywiązywać, są one tworzone na potrzeby konkretnej regulacji prawnej (w tym przypadku – rozporządzenia). Dlatego spotyka się często stwierdzenie: „na użytek niniejszego

rozporządzenia", które oznacza, że w tej konkretnej regulacji prawnej jest właśnie taka, a nie inna definicja. W innych może być odmienna.

Definicje RODO (art. 4)

Na użytek niniejszego rozporządzenia:

1) „dane osobowe" oznaczają 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;

2) „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) „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;

5) „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;

6) „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;

7) „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
8) „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, przetwarza dane osobowe w imieniu administratora;
9) „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10) „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
11) „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
12) „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13) „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;
14) „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;

15) „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;
16) „główna jednostka organizacyjna" oznacza:
a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim - miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;
b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim - miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii - jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia;
17) „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
18) „przedsiębiorca" oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
19) „grupa przedsiębiorstw" oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
20) „wiążące reguły korporacyjne" oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;
21) „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

22) „organ nadzorczy, którego sprawa dotyczy" oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;
b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub
c) wniesiono do niego skargę;
23) „transgraniczne przetwarzanie" oznacza:
a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
24) „mający znaczenie dla sprawy i uzasadniony sprzeciw" oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie - wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;
25) „usługa społeczeństwa informacyjnego" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);
26) „organizacja międzynarodowa" oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

Zgodność przetwarzania z prawem (art. 6 RODO)

Podstawowym założeniem RODO jest, że przetwarzanie jakichkolwiek danych osobowych jest możliwe tylko wtedy, gdy zostanie spełniona co najmniej jedna tzw. *przesłanka legalności przetwarzania danych.* Przesłanki te szczegółowo zostały określone w artykule 6 Rozporządzenia RODO.

Zgodnie z artykułem 6 RODO, dane osobowe mogą być przetwarzane, jeśli:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych,
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Wszystkie wymienione wyżej przesłanki są równoprawne i spełnienie się którejkolwiek z nich uprawnia do przetwarzania danych.

Przetwarzanie szczególnych kategorii danych osobowych (art. 9)

RODO wyróżnia szczególną kategorię danych o osobie, mających istotne znaczenie dla jej prywatności. Dane te określane potocznie jako *dane wrażliwe, sensytywne* lub *nieodporne* są szczególnie chronione.

Zgodnie z art. 9 ust 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie danych wrażliwych jest dopuszczalne tylko wtedy, gdy zostaną spełnione specjalne warunki np.:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie musi takiej zgody wyrazić;
b) 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 Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów

osoby, której dane dotyczą;

c) przetwarzanie danych 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 (np. ratowanie życia);

d) 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;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, 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;

h) 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 Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem odpowiednich warunków i zabezpieczeń. Dane o których mowa mogą być przetwarzane do wyżej wymienionych celów, jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe;

i) 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 Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, 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.

Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia (art. 9 ust. 4).

Zakres RODO

Przedmiotem ochrony RODO są wszystkie dane dotyczące osób fizycznych utrwalone w dowolnej postaci, ze szczególnym uwzględnieniem przetwarzania z użyciem systemów informatycznych. Będą to więc dane zapisane głównie tekstem (znaki językowe), ale mogą być także zdjęcia, nagrania wideo, dane biometryczne, zarejestrowane głosy.

RODO obejmuje wyłącznie dane osobowe osób fizycznych. Osoba fizyczna stanowi prawne określenie człowieka w prawie cywilnym; jest to człowiek od chwili urodzenia do śmierci. W konsekwencji rozporządzenie obejmuje dane osobowe osób żyjących i nie dotyczy osób zmarłych. RODO nie ogranicza się do przetwarzania danych osób obywatelstwa polskiego, dla stosowania rozporządzenia zupełnie nie ma znaczenia narodowość osób, których dane się przetwarza.

Rozporządzenie posługuje się pojęciem osoby fizycznej. Wyróżnia się ją z tej przyczyny, że wobec prawa istnieją dwa rodzaje osób: fizyczne i prawne (prawną osobą jest np. spółka akcyjna).

Podmiotami RODO, czyli tymi, którzy zobowiązani są stosować się do niej są podmioty publiczne i prywatne. Podmioty publiczne rozumie się jako organy państwowe, jednostki samorządu terytorialnego, jednostki organizacyjne państwowe i komunalne.

Podmioty prywatne to:

- osoby fizyczne,
- osoby prawne (m.in. spółki z ograniczoną odpowiedzialnością, spółki akcyjne, fundacje, partie polityczne, szkoły wyższe, jednostki samorządu terytorialnego),
- jednostki organizacyjne nieposiadające osobowości prawnej, którym odrębna ustawa przyznaje zdolność prawną - tzw. ułomne osoby prawne (spółka jawna, spółka partnerska, wspólnota mieszkaniowa, spółki komandytowe i komandytowo-akcyjne),
- podmioty niepubliczne realizujące zadania publiczne (np. szpitale niepubliczne).

RODO jednakowo dotyczy podmiotów prywatnych i publicznych, warto jednak zauważyć, że w jego stosowaniu jest pewna subtelna różnica. Otóż podkreśla się, że podmioty publiczne, w myśl zasady praworządności, wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień. W odniesieniu do podmiotów prywatnych obowiązuje odmienna zasada podmioty te mogą podejmować wszelkie działania, których prawo im nie zabrania.

W rezultacie podmioty publiczne nie powinny zbierać danych osobowych na podstawie zgody, musi natomiast istnieć przepis prawa, który zezwala im na zbieranie i przetwarzanie danych osobowych. A podmioty prywatne mogą zbierać w zasadzie dowolne dane, o ile będą mieć np. zgodę osób, których dane dotyczą i dane będą odpowiednie do celu ich przetwarzania.

Prasowa działalność dziennikarska, akademicka, literacka i artystyczna są częściowo wyłączone ze stosowania RODO, głównie w celu zachowania wolności wypowiedzi (art. 2 ust. 1 uodo w zw. z art. 85 RODO).

Jeśli inna ustawa odnosi się do przetwarzania danych o osobie i nakazuje je chronić bardziej restrykcyjnie, należy stosować te bardziej surowe wymogi:

Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Podmiot przetwarzający dane musi samodzielnie dokonać analizy, jakim regulacjom on podlega, czy przewidują one dalej idącą ochronę i w jakim stopniu jest ona dalej idąca. Może to mieć odniesienie szczególnie w stosunku do regulacji

branżowych określanych mianem sektorowych i zawartych w nich tzw. tajemnic prawnie chronionych: telekomunikacyjnej, bankowej, ubezpieczeniowej, itp.

Inspektor Ochrony Danych Osobowych (IODO)

Nad kontrolą zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych czuwa Inspektor Ochrony Danych Osobowych, w skrócie IODO.

Zgodnie z art. 8 uodo administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", w przypadkach i na zasadach określonych w art. 37 RODO.

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się: 1) jednostki sektora finansów publicznych; 2) instytuty badawcze; 3) Narodowy Bank Polski (art. 9 uodo).

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę (dotyczy to więc przykładowo profilowania i oceny osób w ramach szacowania ryzyka, w celu przyznania zniżek składek ubezpieczeniowych); lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 (np. danych ujawniających poglądy polityczne czy też danych dotyczących zdrowia przetwarzanych przez szpitale), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.

4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.
5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.
6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Zgodnie z art. 10 ust. 1 uodo podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

W zawiadomieniu tym oprócz danych, o których mowa powyżej, wskazuje się:
1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku, gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;
3) pełną nazwę oraz adres siedziby, w przypadku, gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2;
4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych (dotyczących inspektora), oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

Grupa przedsiębiorców, organów lub podmiotów publicznych może wyznaczyć jednego inspektora, wówczas każdy z tych podmiotów dokonuje zawiadomienia.

Zawiadomienia sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym

cPUAP.
Podmiot, który wyznaczył inspektora, udostępnia dane inspektora (imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu), niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.
Obowiązek powołania Inspektora Ochrony Danych spoczywa na administratorze (właścicielu firmy - co do zasady), który przetwarza regularnie i systematycznie dane z różnego typu monitorowania osób, badania preferencji, utrwalania wizerunku, badania rynku, prowadzenia baz danych klientów z akcji marketingowych, których dane te dotyczą. Pojęcie jest znacznie szersze niż zwykłe śledzenia internautów.

W wytycznych Grupy Roboczej art. 29 rozwinięto te obowiązki i wskazano następujące przykłady takiej działalności:

- obsługa sieci telekomunikacyjnej lub świadczenie usług telekomunikacyjnych,
- przekierowywanie poczty elektronicznej,
- działania marketingowe oparte na danych,
- profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy),
- śledzenie lokalizacji (na przykład przez aplikacje mobilne),
- programy lojalnościowe czy reklama behawioralna,
- monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych,
- monitoring wizyjny,
- urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, itd.

Jeżeli spełnia się już tylko jedną z wyżej wymienionych usług/przesłanek a przy tym wchodzi to w skład głównej działalności danej firmy i to na dużą skalę, wówczas ciąży na nas obowiązek powołania Inspektora Ochrony Danych.

Prezes Urzędu Ochrony Danych Osobowych (PUODO)

Prezes jest centralnym organem administracji publicznej, właściwym w sprawie ochrony danych osobowych. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej. Prezes w zakresie wykonywania swoich zadań podlega tylko ustawie.

Na stanowisko Prezesa Urzędu może być powołana osoba, która:

1) jest obywatelem polskim;
2) posiada wyższe wykształcenie;

3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych;
4) korzysta z pełni praw publicznych;
5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
6) posiada nieposzlakowaną opinię.
Kadencja Prezesa Urzędu trwa 4 lata, licząc od dnia złożenia ślubowania. Ta sama osoba nie może być Prezesem Urzędu więcej niż przez dwie kadencje. Prezes Urzędu po upływie kadencji wykonuje swoje obowiązki do czasu objęcia stanowiska przez nowego Prezesa Urzędu.
Kadencja Prezesa Urzędu wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.
Prezes Urzędu może zostać odwołany przed upływem kadencji, wyłącznie w przypadku, gdy:
1) zrzekł się stanowiska;
2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim;
3) sprzeniewierzył się ślubowaniu;
4) został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego;
5) został pozbawiony praw publicznych.
W przypadku wygaśnięcia kadencji Prezesa Urzędu jego obowiązki pełni zastępca Prezesa Urzędu wskazany przez Marszałka Sejmu.
Przed przystąpieniem do wykonywania obowiązków Prezes Urzędu składa przed Sejmem Rzeczypospolitej Polskiej ślubowanie o następującej treści: *„Obejmując stanowisko Prezesa Urzędu Ochrony Danych Osobowych, uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do ochrony danych osobowych, a powierzone mi obowiązki wypełniać sumiennie i bezstronnie"*. Ślubowanie może zostać złożone z dodaniem słów *„Tak mi dopomóż Bóg"*.
Prezes Urzędu może powołać do trzech zastępców. Na zastępcę Prezesa Urzędu może być powołana osoba, która spełnia takie same kryteria co osoba wybrana na Prezesa.
Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu, Zarówno Prezes

jak i jego zastępcy nie mogą należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.
Prezes Urzędu nie może być bez uprzedniej zgody Sejmu Rzeczypospolitej Polskiej pociągnięty do odpowiedzialności karnej ani pozbawiony wolności.
Prezes Urzędu może wyrazić zgodę na pociągnięcie go do odpowiedzialności karnej za wykroczenia (ukarania go mandatem karnym lub grzywną w myśl przepisów kodeksu wykroczeń), stanowi oświadczenie o wyrażeniu przez niego zgody na pociągnięcie go do odpowiedzialności w tej formie.
Prezes Urzędu nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.
Sejm Rzeczypospolitej Polskiej wyraża zgodę na pociągnięcie Prezesa Urzędu do odpowiedzialności karnej w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów. Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na pociągnięcie Prezesa Urzędu do odpowiedzialności karnej.
Sejm Rzeczypospolitej Polskiej wyraża zgodę na zatrzymanie lub aresztowanie Prezesa Urzędu w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów. Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na zatrzymanie lub aresztowanie Prezesa Urzędu. Wymóg uzyskania zgody Sejmu Rzeczypospolitej Polskiej nie dotyczy wykonania kary pozbawienia wolności orzeczonej prawomocnym wyrokiem sądu.
Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych, zwanego dalej „Urzędem". W przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie Prezes Urzędu może w ramach Urzędu tworzyć jednostki zamiejscowe Urzędu.
Prezes Urzędu, w drodze zarządzenia, nadaje statut Urzędowi, określając:
1) organizację wewnętrzną Urzędu,
2) zakres zadań swoich zastępców,
3) zakres zadań i tryb pracy komórek organizacyjnych Urzędu.
Prezes Urzędu, zastępcy Prezesa Urzędu, a także pracownicy Urzędu są obowiązani zachować w tajemnicy informacje, o których dowiedzieli się w związku z wykonywaniem czynności służbowych. Obowiązek zachowania w

tajemnicy informacji, trwa także po zakończeniu kadencji albo zatrudnienia.
Przy Prezesie Urzędu działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą", która jest organem opiniodawczo-doradczym Prezesa Urzędu.
Do zadań Rady należy:
1) opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych;
2) opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych;
3) opracowywanie propozycji kryteriów certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679;
4) opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;
5) inicjowanie działań w obszarze ochrony danych osobowych oraz przedstawianie Prezesowi Urzędu propozycji zmian prawa w tym obszarze;
6) wyrażanie opinii w sprawach przedstawionych Radzie przez Prezesa Urzędu;
7) wykonywanie innych zadań zleconych przez Prezesa Urzędu.
Rada wyraża opinię w terminie 21 dni od dnia otrzymania projektów lub dokumentów, o których mowa w pkt 2.
Opinie, protokoły posiedzeń oraz inne dokumenty Rady są udostępniane na stronie podmiotowej w Biuletynie Informacji Publicznej Prezesa Urzędu.
Rada przedstawia Prezesowi Urzędu sprawozdanie z działalności za każdy rok kalendarzowy w terminie do dnia 31 marca następnego roku.
Rada składa się z 8 członków.
Kandydatów na członków Rady zgłasza:
1) Rada Ministrów;
2) Rzecznik Praw Obywatelskich;
3) izby gospodarcze;
4) uczelnie, federacje podmiotów systemu szkolnictwa wyższego i nauki, instytuty naukowe PAN, instytuty badawcze, międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej (podmioty, o których mowa w art. 7 ust. 1 pkt 1, 2 i 4–6 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668 ze zm.);
5) fundacje i stowarzyszenia wpisane do KRS, których celem statutowym jest działalność na rzecz ochrony danych osobowych.
Członkiem Rady może być osoba, która:
1) posiada wykształcenie wyższe;

2) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
3) korzysta z pełni praw publicznych;
4) wyraziła zgodę na kandydowanie.
Członek Rady jest obowiązany do zachowania w tajemnicy informacji, o których dowiedział się w związku z wykonywaniem funkcji członka Rady. Prezes Urzędu może zwolnić z obowiązku zachowania tajemnicy w zakresie przez niego określonym.
Prezes Urzędu powołuje skład Rady, na dwuletnią kadencję, spośród kandydatów zgłoszonych przez w/w podmioty (w tym 5 członków spośród kandydatów zgłoszonych przez PRM i RPO, oraz 3 członków spośród kandydatów zgłoszonych przez podmioty, o których mowa w pkt 3–5).
Przed upływem kadencji członkostwo w Radzie wygasa z powodu:
1) rezygnacji złożonej na piśmie przewodniczącemu Rady;
2) śmierci;
3) niemożności sprawowania funkcji z powodu długotrwałej choroby stwierdzonej zaświadczeniem lekarskim;
4) skazania prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) pozbawienia praw publicznych.
W przypadku, o którym mowa powyżej, Prezes Urzędu powołuje nowego członka Rady na okres pozostały do końca kadencji, spośród pozostałych zgłoszonych kandydatów, po potwierdzeniu aktualności zgłoszenia.
Prezes Urzędu powołuje i odwołuje przewodniczącego Rady i wiceprzewodniczącego Rady spośród jej członków.
Przewodniczący Rady kieruje jej pracami i reprezentuje ją na zewnątrz. W przypadku nieobecności zastępuje go wiceprzewodniczący Rady.
Obsługę Rady zapewnia Urząd.
Na posiedzenie Rady mogą być zapraszane, przez Prezesa Urzędu oraz przewodniczącego Rady, inne osoby, o ile jest to uzasadnione zadaniami Rady.
Szczegółowy tryb działania Rady określa regulamin ustanawiany na wniosek Rady przez Prezesa Urzędu.
Za udział w pracach Rady członkowi Rady przysługuje wynagrodzenie. Wysokość wynagrodzenia uzależniona jest od zakresu obowiązków związanych z funkcją pełnioną w Radzie oraz liczby posiedzeń, w których uczestniczył. Wynagrodzenie członka Rady za udział w jednym posiedzeniu stanowi co najmniej 5% przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok powołania Rady, ogłaszanego przez Prezesa

GUS na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, i nie może przekroczyć 25% tego wynagrodzenia.

Rada Ministrów określi, w drodze rozporządzenia, wysokość wynagrodzenia członka Rady za udział w posiedzeniu oraz liczbę posiedzeń Rady w ciągu roku kalendarzowego, uwzględniając zakres obowiązków związanych z funkcją pełnioną w Radzie oraz prawidłową realizację zadań Rady.

Prezes Urzędu raz w roku do dnia 31 sierpnia przedstawia Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informację o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa Urzędu oraz wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych.

Prezes Urzędu udostępnia sprawozdanie na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

Założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.

Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

Podmiot, do którego zostało skierowane wystąpienie lub wniosek jest obowiązany ustosunkować się do niego na piśmie w terminie 30 dni od daty jego otrzymania.

Prezes Urzędu:

1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679;
2) może ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 5 rozporządzenia 2016/679.

Komunikaty, o których mowa są ogłasza się w Dzienniku Urzędowym

Rzeczypospolitej Polskiej „Monitor Polski".

„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" (art. 35 ust. 1 RODO).

Prezes Urzędu może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych.

Jeżeli Prezes Urzędu, na podstawie posiadanych informacji, uzna, że doszło do naruszenia przepisów dotyczących przetwarzania danych osobowych, może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom, które dopuściły się naruszeń, i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest prowadzone przez Prezesa Urzędu.

Organizacja społeczna, o której mowa w art. 31 § 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, może również występować w postępowaniu za zgodą osoby, której dane dotyczą, w jej imieniu i na jej rzecz.

W przypadku niezałatwienia sprawy w terminie Prezes Urzędu jest obowiązany zawiadomić strony, jest obowiązany również poinformować o stanie sprawy i przeprowadzonych w jej toku czynnościach.

Prezes Urzędu może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę. Tłumaczenie dokumentacji strona jest obowiązana wykonać na własny koszt.

W celu realizacji swoich zadań Prezes Urzędu ma prawo dostępu do informacji objętych tajemnicą prawnie chronioną, chyba że przepisy szczególne stanowią inaczej.

Strona może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa, przedstawiane Prezesowi Urzędu. W takim przypadku strona jest obowiązana przedstawić Prezesowi Urzędu również wersję

dokumentu niezawierającą informacji objętych zastrzeżeniem. W przypadku nieprzedstawienia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne. Prezes Urzędu może uchylić zastrzeżenie, w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa. W przypadku ustawowego obowiązku przekazania informacji lub dokumentów otrzymanych od przedsiębiorców innym krajowym lub zagranicznym organom lub instytucjom, informacje i dokumenty przekazuje się wraz z zastrzeżeniem i pod warunkiem jego przestrzegania.

Prezes Urzędu wydaje postanowienie, o którym mowa w art. 74 § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, na które służy zażalenie, również w przypadku, gdy udostępnienie informacji i dokumentów, o których mowa w art. 65 ust. 1 (przekazanie sprawy właściwemu organowi), grozi ujawnieniem tajemnic prawnie chronionych albo ujawnieniem tajemnicy przedsiębiorstwa, jeżeli o ograniczenie wglądu do akt dla stron postępowania wnosi przedsiębiorca, od którego informacja pochodzi.

Jeżeli w toku postępowania zajdzie konieczność uzupełnienia dowodów, Prezes Urzędu może przeprowadzić postępowanie kontrolne. Okresu postępowania kontrolnego nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

W przypadku, gdy obowiązany do osobistego stawienia się, mimo prawidłowego wezwania nie stawił się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadnie odmówił złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej może zostać ukarany.

Prezes Urzędu wymierza mu karę grzywny w wysokości od 500 złotych do 5000 złotych.

Wymierzając karę grzywny, Prezes Urzędu bierze pod uwagę:

1) w przypadku osoby fizycznej – sytuację osobistą wezwanego i stopień zrozumienia powagi ciążących na nim obowiązków wynikających z wezwania lub

2) potrzebę dostosowania wysokości kary grzywny do celu, jakim jest przymuszenie wezwanego do zadośćuczynienia wezwaniu.

Kara grzywny może być nałożona także w przypadku, gdy strona odmówiła przedstawienia tłumaczenia na język polski dokumentacji sporządzonej w języku obcym.

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, Prezes Urzędu, 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. W postanowieniu tym Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie. Na postanowienie służy skarga do sądu administracyjnego.

W uzasadnieniu decyzji kończącej postępowanie w sprawie wskazuje się dodatkowo przesłanki określone w art. 83 ust. 2 rozporządzenia 2016/679, na których Prezes Urzędu oparł się, nakładając administracyjną karę pieniężną oraz ustalając jej wysokość.

Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

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 (uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych; zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu);

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;

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

i) 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 - przestrzeganie tych środków;

j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz

k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, po zakończeniu postępowania informuje o wydaniu decyzji na swojej stronie podmiotowej w Biuletynie Informacji Publicznej. Jednostki sektora finansów publicznych, instytuty badawcze oraz Narodowy Bank Polski, w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej w Biuletynie Informacji Publicznej, informację o działaniach podjętych w celu wykonania decyzji.

Wniesienie przez stronę skargi do sądu administracyjnego wstrzymuje wykonanie decyzji w zakresie administracyjnej kary pieniężnej.

Kontrola przestrzegania przepisów o ochronie danych osobowych

Prezes Urzędu przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

Kontrolę przeprowadza upoważniony przez Prezesa Urzędu:

1) pracownik Urzędu,

2) członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 rozporządzenia 2016/679 (wspólne operacje organów nadzorczych państw członkowskich UE) – zwany dalej „kontrolującym".

Kontrolujący jest obowiązany do zachowania w tajemnicy informacji, o których dowiedział się w toku kontroli.

Kontrolujący podlega wyłączeniu z udziału w kontroli, na wniosek lub z urzędu, jeżeli:

1) wyniki kontroli mogłyby oddziaływać na prawa lub obowiązki jego, jego małżonka, osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnego i powinowatego do drugiego stopnia albo na osoby związanej z nim z tytułu przysposobienia, opieki albo kurateli;

2) zachodzą uzasadnione wątpliwości co do jego bezstronności.

Wskazane wyżej powody wyłączenia trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli.

O przyczynach powodujących wyłączenie kontrolujący lub podmiot objęty

kontrolą, zwany dalej „kontrolowanym", niezwłocznie zawiadamia Prezesa Urzędu. O wyłączeniu kontrolującego rozstrzyga Prezes Urzędu. Do czasu wydania postanowienia kontrolujący podejmuje czynności niecierpiące zwłoki.

Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2 (członka lub pracownika organu nadzorczego państwa członkowskiego UE), po okazaniu imiennego upoważnienia wraz z dokumentem potwierdzającym tożsamość.

Imienne upoważnienie do przeprowadzenia kontroli zawiera:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;
2) oznaczenie organu;
3) imię i nazwisko, stanowisko służbowe kontrolującego oraz numer legitymacji służbowej, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2, imię i nazwisko oraz numer dokumentu potwierdzającego tożsamość;
4) określenie zakresu przedmiotowego kontroli;
5) oznaczenie kontrolowanego;
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych;
7) podpis Prezesa Urzędu;
8) pouczenie kontrolowanego o jego prawach i obowiązkach;
9) datę i miejsce jego wystawienia.

Prezes Urzędu może upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy.

Zakres uprawnień kontrolującego osoby, Prezes Urzędu określa w upoważnieniu. Osoba ta jest obowiązana do zachowania w tajemnicy informacji, o których dowiedziała się w toku kontroli.

Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli.

Kontrolujący ma prawo:

1) wstępu w godzinach od 6:00 do 22:00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
2) wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
5) zlecać sporządzanie ekspertyz i opinii.

Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, o których mowa w pkt 3.

Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w pkt 2. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli.

W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000), na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.

Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do wykonywania czynności kontrolnych. Policja udziela pomocy przy wykonywaniu czynności kontrolnych, po otrzymaniu pisemnego wezwania na co najmniej 7 dni przed terminem tych czynności.

W pilnych przypadkach, w szczególności gdy kontrolujący trafi na opór uniemożliwiający lub utrudniający wykonywanie czynności kontrolnych, udzielenie pomocy następuje również na ustne wezwanie Prezesa Urzędu lub kontrolującego, po okazaniu imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej kontrolującego. W tym przypadku, Prezes Urzędu przekazuje potwierdzenie wezwania na piśmie, nie później niż w terminie 3 dni po zakończeniu czynności kontrolnych. Udzielenie pomocy Policji przy wykonywaniu czynności kontrolnych polega na zapewnieniu kontrolującemu bezpieczeństwa osobistego oraz dostępu do miejsca wykonywania kontroli i porządku w tym miejscu.

Policja, udzielając pomocy kontrolującemu przy wykonywaniu czynności kontrolnych, zapewnia bezpieczeństwo również innym osobom uczestniczącym przy wykonywaniu czynności kontrolnych, mając w szczególności na względzie

poszanowanie godności osób biorących udział w kontroli.

Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka. Za pracownika kontrolowanego uznaje się osobę zatrudnioną na podstawie stosunku pracy lub wykonującą pracę na podstawie umowy cywilnoprawnej. Do przesłuchania pracownika kontrolowanego stosuje się przepis art. 83 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Przebieg czynności kontrolnych kontrolujący przedstawia w protokole kontroli.

Protokół kontroli zawiera:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;
2) imię i nazwisko osoby reprezentującej kontrolowanego oraz nazwę organu reprezentującego kontrolowanego;
3) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer imiennego upoważnienia kontrolującego, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2, imię i nazwisko, numer dokumentu potwierdzającego tożsamość oraz numer imiennego upoważnienia;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie zakresu przedmiotowego kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) wyszczególnienie załączników;
8) omówienie dokonanych w protokole kontroli poprawek, skreśleń i uzupełnień;
9) pouczenie kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu kontroli oraz o prawie odmowy podpisania protokołu kontroli;
10) datę i miejsce podpisania protokołu kontroli przez kontrolującego i kontrolowanego.

Protokół kontroli podpisuje kontrolujący i przekazuje kontrolowanemu w celu podpisania. Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu podpisuje go albo składa pisemne zastrzeżenia do jego treści.

W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu kontroli.

W razie nieuwzględnienia zastrzeżeń w całości albo części, kontrolujący przekazuje kontrolowanemu informację o tym wraz z uzasadnieniem.

Brak doręczenia kontrolującemu podpisanego protokołu kontroli i niezgłoszenie zastrzeżeń do jego treści w terminie (7 dni), uznaje się za odmowę podpisania protokołu kontroli.

O odmowie podpisania protokołu kontroli kontrolujący czyni wzmiankę w tym protokole, zawierającą datę jej dokonania. W przypadku, o którym mowa powyżej, wzmianki dokonuje się po upływie 7 dniowego terminu.

Protokół kontroli sporządza się w postaci elektronicznej albo w postaci papierowej w dwóch egzemplarzach. Protokół kontroli kontrolujący doręcza kontrolowanemu.

Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego. Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 88 ust. 8 (odmowie podpisaniu protokołu).

Jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania w sprawie.

Odpowiedzialność cywilna i postępowanie przed sądem

W zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 (prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu) i art. 82 (prawo do odszkodowania i odpowiedzialność) tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.

W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, właściwy jest sąd okręgowy.

O wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, sąd zawiadamia niezwłocznie Prezesa Urzędu. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej

sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.

Sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu.

Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem.

Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych. W tych przypadkach do Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155, ze zm.) o prokuratorze. Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych.

Do postępowania w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, w zakresie nieuregulowanym niniejszą ustawą stosuje się przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego.

Przepisy o administracyjnych karach pieniężnych i przepisy karne

Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż:

1) jednostka sektora finansów publicznych,

2) instytut badawczy,

3) Narodowy Bank Polski – w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) instytut badawczy;

3) Narodowy Bank Polski.

Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Administracyjne kary pieniężne, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Naruszenia przepisów dotyczących ochrony danych osobowych podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % rocznego obrotu firmy, a w przypadku rażących naruszeń kwota ta może wzrosnąć do 20 000 000 EUR lub 4% rocznego obrotu (przy czym zastosowanie ma kwota wyższa). Wątpliwe jest, by największymi z wymienionych kwot zostały obciążone małe firmy czy jednoosobowe działalności gospodarcze. Najwyższe kary czekają korporacje i instytucje przetwarzające ogromne ilości danych, ponieważ to tam narażenie ich bezpieczeństwa wyrządzi najpoważniejsze szkody dotyczące wielu osób. Niemniej, trzeba pamiętać, że kary są dla wszystkich, a sposobem na ich uniknięcie jest dostosowanie się do obowiązujących przepisów.

Równowartość wyrażonych w euro kwot, o których mowa w art. 83 rozporządzenia 2016/679, oblicza się w złotych według średniego kursu euro ogłaszanego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego.

Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa.

Administracyjną karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego. Prezes Urzędu może, na wniosek podmiotu ukaranego, odroczyć termin uiszczenia administracyjnej kary pieniężnej albo rozłożyć ją na raty, ze względu na ważny interes wnioskodawcy.

W przypadku odroczenia terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty, Prezes Urzędu nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, przy zastosowaniu obniżonej stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56d ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2018 r. poz. 800 ze zm.), od dnia następującego po dniu złożenia wniosku.

W przypadku rozłożenia administracyjnej kary pieniężnej na raty, odsetki są naliczane odrębnie dla każdej raty.

Prezes Urzędu może uchylić odroczenie terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenie jej na raty, jeżeli ujawniły się nowe lub uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli rata nie została uiszczona w terminie.

Rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia.

Prezes Urzędu, na wniosek podmiotu ukaranego prowadzącego działalność gospodarczą, może udzielić ulgi w wykonaniu administracyjnej kary pieniężnej, która:

1) nie stanowi pomocy publicznej;

2) stanowi pomoc *de minimis* albo pomoc *de minimis* w rolnictwie lub rybołówstwie – w zakresie i na zasadach określonych w bezpośrednio obowiązujących przepisach prawa Unii Europejskiej dotyczących pomocy w ramach zasady *de minimis*;

3) stanowi pomoc publiczną zgodną z zasadami rynku wewnętrznego Unii Europejskiej, której dopuszczalność została określona przez właściwe organy Unii Europejskiej.

Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub

światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Europejska Rada Ochrony Danych

EROD jest niezależnym organem europejskim, który działa na rzecz spójnego stosowania zasad ochrony danych w całej Unii Europejskiej oraz promuje współpracę pomiędzy organami ochrony danych UE. Rada składa się z przedstawicieli krajowych organów ochrony danych i Europejskiego Inspektora Ochrony Danych (EIOD). Ma ona siedzibę w Brukseli. Europejska Rada Ochrony Danych posiada sekretariat, którego obsługę zapewnia EIOD.

Zadania i obowiązki Rady (EROD):

1) tworzenie ogólnych wskazówek (w tym wytycznych, zaleceń i najlepszych praktyk) w celu wyjaśnienia przepisów prawa;
2) doradzanie Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych i nowych proponowanych przepisów prawa w Unii Europejskiej;
3) przyjmowanie spójnych ustaleń w transgranicznych sprawach dotyczących ochrony danych;
4) promowanie współpracy i skutecznej wymiany informacji oraz najlepszych praktyk pomiędzy krajowymi organami nadzorczymi.

Rada sporządza również roczne sprawozdanie z swoich działań, które jest publikowane i przedkładane Parlamentowi Europejskiemu, Radzie i Komisji.

Europejska Rada Ochrony Danych nie świadczy indywidualnych usług doradczych. Należy zwrócić uwagę, że osobom prywatnym lub organizacjom, które mają pytania związane z przepisami w zakresie ochrony danych, zaleca się odwiedzenie strony internetowej organu nadzorczego w kraju zamieszkania lub w którym mają siedzibę.

Wpływ RODO na działalność podmiotów

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów RODO.

Dane osobowe

W dzisiejszym brzmieniu definicji dowolna informacja może stanowić dane osobowe.

W rozumieniu RODO za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby 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.

Na pytanie czy określone dane są danymi osobowymi nie da się odpowiedzieć, jeśli nie weźmie się pod uwagę kontekstu tych danych. Informacja *zarabia 4 tys. zł miesięcznie* albo *właściciel zielonego Forda Mustanga* nic nie mówi o osobie, ale nabierze charakteru danych osobowych, gdy zostanie połączona:

- z danymi dotyczącymi konkretnej zidentyfikowanej osoby (np. *zarabia 4 tys. zł* połączone z *Jan Nowak mieszkający na ul. Łąkowej w Tarnowie*),
- z danymi, które umożliwią przy niewielkim nakładzie pracy zidentyfikowanie osoby (np. *burmistrz miasta X* i *zarabia 4 tys. zł).*

Te dane, które wcześniej nie miały charakteru danych osobowych nabrały go z danymi identyfikującymi osobę (imię, nazwisko i adres) lub pozwalającymi na jej identyfikację (piastowanie urzędu w określonej miejscowości). Widać tutaj bardzo wyraźnie, że najważniejszym składnikiem zestawu informacji o osobie będą dane umożliwiające jej identyfikację, ustalenie tożsamości.

Co więcej - określone informacje na temat osoby będą danymi osobowymi tylko dla tego, kto będzie miał możliwość powiązać je z danymi osoby, której tożsamość zna lub będzie w stanie ją ustalić. I przez analogię - te same informacje nie będą danymi osobowymi dla tego, kto nie ma takiej możliwości.

Dane wrażliwe (sensytywne)

RODO wyróżnia kategorię danych osobowych, którym należy się szczególna ochrona ze względu na ich znaczenie dla sfery prywatności osoby. Są to dane ujawniające informacje o osobie opisane w art. 9 ust. 1 i art. 10 RODO:

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Dane tego rodzaju określa się najczęściej terminem dane *sensytywne* lub dane *wrażliwe*. Rzadziej używa się terminu dane *nieodporne*.

Dane wrażliwe same w sobie zazwyczaj nie są danymi osobowymi i muszą wstępować w połączeniu z danymi pozwalającymi zidentyfikować osobę, aby można było uznać je za dane osobowe. Zatem informacja *osoba karana wpisana do krajowego rejestru karnego* nie będzie danymi wrażliwymi, jeśli nie będzie powiązana z konkretną osobą.

Przykłady kategorii danych wrażliwych:

- pochodzenie rasowe, etniczne (azjata, mulat),
- poglądy polityczne (lewicowiec, prawicowiec),
- przekonania religijne lub filozoficzne (wierzący, ateista, agnostyk),
- przynależność wyznaniowa (katolik, świadek jehowy),
- przynależność partyjna (członek określonej partii),
- przynależność związkowa (należy do określonego związku, nie należy do żadnego związku),
- stan zdrowia (zdrowy, chory na określoną chorobę, impotent, w ciąży, często chorujący),
- kod genetyczny (informacja o genomie),
- nałogi (narkoman, alkoholik, palacz),
- życie seksualne (gej, lesbijka, heteroseksualny, informacja o zakupach w „sex-shopie", impotent, prawiczek, dziewica),
- informacja o skazaniach (dane z Krajowego Rejestru Karnego, informacja o karalności lub niekaralności),
- orzeczenia o ukaraniu (zakaz prowadzenia pojazdów, pozbawienie prawa wykonywania zawodu albo zajmowania określonych stanowisk),

• mandaty karne (mandat za nieprzestrzeganie przepisów drogowych, za wykroczenie skarbowe),
• inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym (postępowanie przed sądem cywilnym, karnym, administracyjnym, wszystkie wyroki, postanowienia, nakazy zapłaty i wynikające z nich informacje; informacja o tym, że ktoś jest rozwiedziony).

Dane wrażliwe sprawiają czasami kłopot, bo z definicji informacja o tym, że np. ktoś pali nałogowo papierosy czy fajkę, nosi okulary lub jest w ciąży stanowi już informację wrażliwą, ujawnia informację o nałogach lub stanie zdrowia.

Sklep z odzieżą ciążową zbierający informacje takie jak miesiąc ciąży będzie więc przetwarzał dane wrażliwe.

Dane wrażliwe muszą wprost wyrażać charakter informacji. Informacje *Pan X regularnie słucha audycji radiowej o charakterze religijnym* lub *Pani Y bierze regularnie udział we mszy świętej* wyrażają jedynie pewne prawdopodobieństwo określonych przekonań religijnych. Nie stanowią one informacji wrażliwych.

Danymi wrażliwymi będzie też zaprzeczenie, zanegowanie określonej kategorii danych sensytywnych. Oświadczenie o tym, że osoba nie była karana, nie ma żadnych nałogów, nie należy do partii, jest zdrowa, nigdy nie otrzymała mandatu karnego będzie stanowić dane sensytywne.

Dane zwykłe

W zasadzie należałoby zacząć od definicji *danych zwykłych*, jednakże kolejność ta celowo jest odwrotna, tak można łatwiej wyjaśnić, czym są dane zwykłe: to wszystkie dane osobowe, które nie są wrażliwe. Do zwykłych danych będą się zaliczać m.in.:

- nazwiska i imiona,
- imiona i nazwiska rodziców, także panieńskie (rodowe),
- data i miejsce urodzenia,
- wszelkiego rodzaju adresy - zamieszkania, pobytu,
- numer PESEL, NIP,
- miejsce pracy, zawód, wykształcenie,
- informacja o przebytych kursach, posiadanych umiejętnościach,
- numery dokumentów (dowodu, prawa jazdy),
- numer telefonu, adres e-mail, adres strony www,
- numer bądź identyfikator komunikatora (gadu-gadu, skype, MSN).

W zasadzie wszystkie dane identyfikujące osobę i umożliwiające z nią kontakt będą danymi zwykłymi.

Przetwarzanie danych

Przetwarzanie danych jest bardzo szerokim, rozległym pojęciem, głównie ze względu, że RODO swoim zakresem obejmuje rozmaite formy przetwarzania.

Definicja przetwarzania znajduje się art. 4 pkt 2) i jest następująca:

> Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Należy zwrócić szczególną uwagę na wyrazy:

- operacje (działania),
- na danych osobowych (wykonywane na danych).

Wykaz tych operacji w RODO jest przykładowy, w gruncie rzeczy mogą to być dowolne działania, pod warunkiem, że wykonywane są na danych osobowych.

Powszechne sądzi się, że przetwarzanie danych, szczególnie komputerowe, oznacza operacje na danych takie jak np. przekształcanie ich z jednej postaci do drugiej, wytworzenie informacji z danych (raportu), dodawanie, zmianę bądź usuwanie zgromadzonych rekordów. Dlatego dla wielu dość kontrowersyjne jest uznawanie przechowywania danych za ich przetwarzanie. Nic dziwnego, samo przechowywanie to czynność statyczna, i trudno uznać ją za „operację" na danych, chociaż oczywiste jest, że zgromadzone dane najpierw trzeba przechowywać, aby je przetwarzać.

Literalne, dosłowne interpretowanie tej definicji prowadzić może niekiedy do absurdów, np. można uznać, że firma kurierska transportując przesyłkę z dokumentami czy też nośniki z danymi zapakowane w kopertę bądź paczkę przetwarza dane osobowe, bo poprzez fakt ich tymczasowego posiadania przechowuje je, a więc przetwarza dane osobowe (mimo że nie wie, jaka jest jej zawartość). Natomiast firmy prowadzące archiwa dokumentów będą faktycznie przetwarzać dane osobowe, mimo że przechowują tylko papiery - bo przechowywanie w tym wypadku oznacza także sortowanie, porządkowanie, co wymaga niekiedy zapoznania się z danymi osobowymi.

Zbieranie danych

Dane można zbierać od osoby, której dane dotyczą, albo od innej osoby. Dane można też otrzymać od innego podmiotu np. kupując je. W każdym z tych przypadków wchodząc w posiadanie danych, co do których decyduje się o celach i środkach ich przetwarzania, należy rozumieć to jako *zbieranie danych*.

Przesłanki legalności

Aby można było przetwarzać dane osobowe, trzeba spełniać tzw. *przesłanki legalności* przetwarzania danych osobowych, czyli mieć po prostu zapewnioną prawną podstawę do przetwarzania danych osobowych.

RODO wymienia je w art. 6, w którym stwierdza się, że w szczególności przetwarzanie danych jest dopuszczalne, gdy:

- osoba, której dane dotyczą wyrazi na to zgodę,
- jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych *[...]* a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczę,

Administrator danych osobowych

W bardzo dużym uproszczeniu administratora danych osobowych można określić jako „właściciela" zebranych danych, który decyduje o tym, co się z nimi dzieje np. po co się je zbiera, co można z nimi robić, komu przekazać, etc. Pojęcie administratora danych zdefiniowane jest w RODO w art. 6 pkt 7: *rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.* Jest to jedno z najważniejszych dla przedsiębiorcy pojęć, dlatego że przedsiębiorca będzie administratorem danych.

Bardzo istotne w tej definicji jest nie tyle kto, ale o czym może decydować. Ten, kto ma możliwość decydowania o celach i o środkach przetwarzania danych jest właśnie administratorem danych. wykorzystania (np. nie może użyć ich w innym celu).

Roli administratora danych nie można się pozbyć i nie da się też jej delegować,

nie można wyznaczyć np. kogoś, komu powierzono obowiązki związane z ochroną i zabezpieczeniem danych osobowych jako administratora danych.

Określenie *administrator danych* z początku może kojarzyć się z administratorem budynku lub administratorem sieci komputerowej. W słowniku języka polskiego czytamy, że administrator to ktoś, kto „administruje, zarządza czymś; zarządca". W prawie europejskim administratora danych opisuje się terminem *controller,* którego nie dało się wprost przenieść na grunt polski, bo trudno sobie wyobrazić, aby wyraz ten przetłumaczono jako np. regulator albo sterownik.

Kto zgodnie z prawem może w ogóle być administratorem danych? W art. 4 pkt 7 wspomniano, że przez administratora rozumie się oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Przedsiębiorstwa działające jako spółki akcyjne bądź spółki z ograniczoną odpowiedzialnością, podobnie jak osoby fizyczne prowadzące działalność gospodarczą objętą są tą definicją - są to osoby fizyczne i prawne przetwarzające dane w związku z działalnością zarobkową. Za przedsiębiorców uważa się także wspólników spółki cywilnej w zakresie wykonywanej przez nich działalności gospodarczej. Działalnością gospodarczą jest m.in. każda działalność zawodowa, wykonywana w sposób zorganizowany i ciągły. Mogą jednak zdarzyć się takie przypadki działalności zarobkowej, które nie będą spełniać definicji działalności gospodarczej np. wynajmowanie przez rolników pokoi.

Przetwarzanie danych w celach zawodowych określić można jako *profesjonalne wykonywanie działalności opartej na posiadanych umiejętnościach lub wymaganych kwalifikacjach zawodowych,* chodzi tutaj przede wszystkim o wolne zawody, które niekiedy określa się zawodami „zaufania publicznego", takie jak m.in. lekarz, adwokat, notariusz. W grę także będzie wchodzić praca socjalna określona w ustawie o pomocy społecznej jako działalność zawodowa.

Podmiotem niepublicznym, realizującym zadania publiczne będą np. szpitale prowadzone przez niepubliczne zakłady opieki zdrowotnej (NZOZ), które na podstawie kontraktów finansowane są przez państwo z Narodowego Funduszu Zdrowia.

Działalność statutowa będzie dotyczyć stowarzyszeń, spółdzielni, fundacji, które działają na podstawie statutu, np. działalność statutowa stowarzyszenia to działalność zgodna z jego Statutem, w którym wymienione są cele działalności stowarzyszenia i sposoby ich realizacji.

W przypadku osób prawnych administratorem danych będzie np. spółka, towarzystwo, stowarzyszenie. Zarząd nie będzie administratorem danych, on

reprezentuje podmiot, więc w istocie reprezentuje administratora danych.

Zbiór danych osobowych

Dane osobowe ze względu na ich ilość, strukturę i kryteria dostępności dzieli się na:

- pojedyncze,
- w zestawach,
- w zbiorach.

Zestaw danych to po prostu pewna ilość danych osobowych w nieuporządkowanej formie (np. teczka nieuporządkowanych dokumentów zawierających dane osobowe). Zdefiniowanie pojęcia zbioru danych osobowych sprawia nieco trudności, bo jest to pojęcie dość abstrakcyjne. Definicję zbioru RODO określa następująco (art. 4 pkt 6):

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

Nie jest to jak się czasami uważa, baza danych. Termin rzeczywiście wywodzi się od baz danych, bo na początku regulacje dotyczące ochrony danych osobowych brały pod szczególną uwagę głównie systemy informatyczne, jednak zbiór może zawierać także dane osobowe w postaci tradycyjnej, papierowej.

Z definicji RODO wynika, że dla istnienia zbioru musi pojawić się zestaw danych i określone kryteria dostępu (struktura). Za zestaw danych o charakterze osobowym rozumie się po prostu dane osobowe w pewnej ilości. Ten zestaw może zamienić się w zbiór, jeśli pojawi się dostępność tych danych według pewnych kryteriów, które pozwalają te dane np. wyszukiwać. Kryteria przede wszystkim powinny mieć charakter osobowy, może to być miejscowość, nazwisko, PESEL. Może też być np. data.

Zestawy danych przetwarzane w systemach informatycznych w tabelach z danymi np. arkusze kalkulacyjne Microsoft Excel lub tabele dowolnych relacyjnych baz danych z bardzo dużym prawdopodobieństwem będą spełniać wymogi definicji zbioru. Dane w takich „tabelach" mogą zostać uporządkowane według wartości dowolnej kolumny, to oznacza, że „kryteriów dostępu" będzie wiele; w szczególnym wypadku tyle ile kolumn.

Zgoda

Przez zgodę rozumie się dobrowolne, konkretne, świadome i jednoznaczne

okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych (art. 4 pkt. 11).

Zgoda będzie stosowana wszędzie tam, gdzie prawo (dowolny akt prawa) nie daje swoimi zapisami zezwolenia na przetwarzanie danych osobowych. Należy pamiętać, że udzielona zgoda może być odwołana w dowolnym czasie.

Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, np. z faktu zaakceptowania regulaminu sklepu internetowego albo z faktu, że ktoś przysłał maila ze swoimi danymi do przedsiębiorcy.

Przekazywanie i udostępnianie danych

W życiu codziennym termin udostępnianie oznacza zazwyczaj zgodę na skorzystanie z udostępnionego dobra i najczęściej nie niesie za sobą zmiany właściciela. Przekazanie zaś odwrotnie, bardzo często wiąże się ze zmianą właściciela, np. przekazuje się pieniądze albo jakieś rzeczy. Zwykliśmy uważać też, że odbiorcą jest ten, który odbiera coś zazwyczaj od przekazującego

Upoważnienie do przetwarzania danych osobowych

Warto na samym początku rozróżnić pojęcie powierzenia oraz upoważnienia do przetwarzania danych. O powierzeniu mówimy w sytuacji, kiedy przetwarzanie danych odbywa się na podstawie umowy przez zewnętrzny podmiot. Z kolei upoważnienie to nadanie uprawnienia do przetwarzania danych osobowych pracownikowi wewnątrz struktury tego samego przedsiębiorstwa.

Upoważnienie do przetwarzania danych stanowi uprawnienie do przetwarzania określonych danych osobowych nadane pracownikowi przez administratora danych. Jest to nic innego jak udzielenie jakby zgody przez przedsiębiorcę na przetwarzanie. Forma upoważnienia może być dowolna, może to być nawet służbowy mail.

Obowiązująca do 24 maja br. ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych w art. 37 wymagała, aby system informatyczny, który pozwala na przetwarzanie danych osobowych był obsługiwany wyłącznie przez osoby, które zostały do tego upoważnione przez administratora danych osobowych. Podobne rozwiązanie wynika z art. 29 RODO, choć nie zostało jednoznacznie wskazane, aby istniał obowiązek pisemnego nadawania upoważnienia pracownikowi do przetwarzania danych osobowych. Wciąż jednak zalecane jest stosowanie upoważnień papierowych w celu kontroli nad tym, kto posiada dostęp do danych. Dobrym rozwiązaniem jest także prowadzenie rejestru upoważnień, czyli wykazu

pracowników wraz ze wskazaniem zakresu ich dostępu do danych i czynności przetwarzania oraz stałe jego aktualizowanie.

Przepisy prawa nie przewidują szczegółowych wytycznych co do treści upoważnienia do przetwarzania danych osobowych. Taki dokument powinien zawierać informacje o aktualnym administratorze oraz dane pracownika, któremu przyznawane jest uprawnienie wraz z datą i miejscem wystawienia.

Kolejnym niezbędnym elementem w dokumencie jest wskazanie zakresu danych, które pracownik będzie miał prawo przetwarzać. W związku z tym, że RODO skupia się na procesach przetwarzania danych w upoważnieniu powinny znaleźć się informacje o tym, do jakich procesów przetwarzania pracownik będzie miał dostęp.

Upoważnienie powinno również zawierać zapis mówiący o tym, że przetwarzanie danych osobowych przez wskazanego pracownika będzie odbywać się zgodnie z poleceniami administratora i przez określony czas – zwykle do momentu zakończenia zatrudnienia w danej firmie. Warto dodać też zapis umożliwiający cofnięcie upoważnienia w dowolnym momencie.

Zalecanym elementem upoważnienia jest również nałożenie na pracownika obowiązku zachowania poufności nie tylko przez okres, w którym przetwarza on dane, ale również po cofnięciu upoważnienia oraz ewentualnym rozwiązaniu umowy o pracę.

Upoważnienie powinno być sporządzone w formie pisemnej, aby pracownik mógł się pod nim podpisać. W ten sposób potwierdza, że jest świadomy ciążącej na nim odpowiedzialności oraz zakresu, w jakim będzie mógł przetwarzać dane. Upoważnienie może być osobnym dokumentem, jak również stanowić dodatkowy punkt w umowie o pracę podpisywanej w momencie rozpoczęcia zatrudnienia (o ile początkowy zakres obowiązków przewiduje przetwarzanie danych osobowych).

Administrator może również prowadzić rejestr osób posiadających takie uprawnienia. Na gruncie poprzednio obowiązujących przepisów prowadzenie rejestru było obowiązkiem administratora. W nowym porządku prawnym, po rozpoczęciu stosowania RODO, nie ma już konieczności prowadzenia takiej ewidencji, a prowadzenie rejestru należy wyłącznie do dobrych praktyk.

Rejestr upoważnień może być przydatny w przypadku kontroli oraz konieczności wskazania, którzy pracownicy posiadali dostęp do poufnych danych i mogą być odpowiedzialni za wystąpienie incydentu, np. wycieku danych. Prowadzenie rejestru jest praktycznym rozwiązaniem – administrator ma wszelkie upoważnienia zebrane w jednym miejscu i może je na bieżąco aktualizować.

Upoważnienia powinny być stale aktualizowane w następujących

przypadkach:

- zmiana zakresu obowiązków pracownika,
- rozpoczęcie współpracy z nowym pracownikiem,
- rozwiązanie umowy z pracownikiem upoważnionym do przetwarzania danych.

Jedynie osoby posiadające nadane przez administratora upoważnienia są uprawnione do przetwarzania danych w zakresie ustalonym w tym dokumencie. Dokonywanie jakichkolwiek zmian bez upoważnienia będzie stanowiło naruszenie przepisów o ochronie danych osobowych i może skutkować karami dla administratora.

Powierzenie przetwarzania danych

Powierzenie przetwarzania danych osobowych jest kolejnym bardzo ważnym zagadnieniem dla przedsiębiorcy. Zlecając innej firmie wykonanie usługi, w ramach której będzie ona przetwarzać dane w imieniu zleceniodawcy (np. w celu wysłania wyciągów bankowych), firma ta będzie *podmiotem, któremu powierzono przetwarzanie danych osobowych*. Podmiot ten nie może decydować o celu przetwarzania danych, jego „władza" nad danymi osobowymi ograniczona jest do tego, na co mu się zezwoli w umowie.

Inspektor Ochrony Danych Osobowych (IODO)

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych narzuca na przedsiębiorcę jako administratora danych osobowych obowiązek monitorowania zabezpieczenia danych osobowych.

Jak rozpoznać dane osobowe

W swojej praktyce zawodowej bardzo często spotykam się z sytuacjami, w których przedsiębiorcy i pracownicy nie mają pewności, czy określone dane są osobowe, czy nie. Aby przekonać się, że to nie jest wcale takie proste wystarczy zapytać kilka osób, czy ich zdaniem sam numer PESEL bądź sam adres e-mail stanowi dane osobowe. Z pewnością zdania odpowiadających będą się różnić. Dlatego identyfikacji danych osobowych poświęcić należy szczególną uwagę.

Prowadząc biznes przetwarza się rozmaite dane osobowe, głównie dane osobowe pracowników, klientów i potencjalnych klientów. Wiedza o tym, jakie dane są, a jakie nie są danymi osobowymi wpływa na to, czy należy im zapewniać odpowiednią ochronę i stosować się do RODO. To w efekcie przekłada się na

finanse, co w trudnych ekonomicznie czasach ma znaczenie szczególne.

Czasami od razu widać, że określone informacje to dane osobowe, a czasami nie. Takie same dane w jednych okolicznościach są osobowe, a w innych nie. Warto więc nauczyć się jak rozpoznawać, kiedy określone dane są osobowe, a to nie zawsze będzie takie proste.

RODO nie prezentuje wprost katalogu informacji stanowiących dane osobowe i trzeba samodzielnie podejmować trud oceny, jakie dane są „osobowe". Definicja danych osobowych w RODO jest następująca (art. 4):

1) „dane osobowe" oznaczają 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.

Zatem w danych osobowych szczególnie istotna jest możliwość identyfikowania osoby, której dane dotyczą. Dlatego też przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, w większości przypadków, nieuniknione jest dokonanie zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

Na codzień intuicja podpowiada, jakie informacje są danymi osobowymi, np. wiemy, że *imię, nazwisko i adres zamieszkania* to dane osobowe. Gdyby jednak ktoś zapytał, dlaczego tak jest, trudno byłoby odpowiedzieć. Możliwe, że tak sądzimy, gdyż takie dane znajdują się m.in. w dowodzie osobistym, prawie jazdy i służą do ustalania naszej tożsamości. A dlaczego samego adresu nie uważa się za dane osobowe? Intuicja podpowiada, że sam adres określa lokalizację domu, a nie identyfikuje osoby, bo pod jednym adresem może przebywać kilka osób, a nawet rodzin. To akurat słuszny wniosek, jednak w przypadku danych osobowych w rozumieniu RODO posługiwanie się intuicją może często prowadzić do błędnych wniosków, gdyż zgodnie z RODO tożsamość osoby można ustalić posiadając w zasadzie dowolną informację (art. 4 pkt. 1):

To, jak szybko uda się ustalić jej tożsamość posiadając określone informacje to tylko kwestia nakładu pracy. Przy odpowiedniej ilości czasu, pieniędzy i pracy prawie każda informacja pozwoli określić, kogo dotyczą posiadane informacje.

Osoba może być zidentyfikowana bezpośrednio i pośrednio. Informacje, które bezpośrednio identyfikują osobę to bez wątpienia np. imię, nazwisko i adres. Pośrednio osobę mogą zidentyfikować nawet takie dane jak *właściciel czerwonego Lexusa* czy *najbogatszy Polak*. To w efekcie prowadzi do wielu wątpliwości, jakie konkretnie dane i w jakich okolicznościach stanowią dane osobowe, a w jakich nie. Działania takie sprowadzają przedsiębiorcę w pewnym sensie do roli śledczego, który musi dochodzić, czy dane informacje pozwalają ustalić tożsamość osoby, czy jeszcze nie. W większości przypadków do ustalenia tożsamości osoby niezbędne będzie kilka informacji czy też kilka danych o osobie, gdyż sama pojedyncza informacja jako taka w zasadzie nie pozwala na określenie tożsamości osoby, której dotyczy, może za wyjątkiem wizerunku (zdjęcia).

W obrocie gospodarczym warto wyodrębnić dodatkowy rodzaj informacji związanych z osobą - dane umożliwiające kontaktowanie się z osobą, dotarcie do niej. Dane umożliwiające kontakt nie zawsze będą danymi osobowymi (szczególnie samodzielnie), bo same w sobie nie umożliwiają identyfikacji tożsamości osób, jednak mają szczególne znaczenie dla ich prywatności. Dla przykładu numer telefonu wraz z wysokością wynagrodzenia nie stanowi danych osobowych w rozumieniu RODO, jednak zawiera w sobie istotną informację o wartości klienta, jego „mocy" zakupowej i - co więcej - pozwala się z nim skontaktować.

Z punktu widzenia RODO najbardziej istotna jest możliwość identyfikowania osoby, ustalenia jej tożsamości. Gdy będzie można określić, jakiej osoby dotyczą określone informacje, będzie można uznać je za dane osobowe. „Wszelkie informacje", które oderwie się od danych pozwalających na identyfikację osoby, przestaną automatycznie być danymi osobowymi. Zatem te same informacje będą danymi osobowymi w jednych okolicznościach, a w innych nie. Te okoliczności to głównie możliwości zestawienia danych z innymi danymi przez tego, który jest we władaniu danych, prowadzące do ustalenia tożsamości osoby, której dane dotyczą. Weźmy np. takie dane:

Tabela z przykładowymi danymi			
identyfikator	średnia	profil	potencjał
2781	4300 zł	VIP	7800 zł
2782	570 z	normalny	3430 zł

Takie informacje dla osoby postronnej niewiele będą znaczyć, nie umożliwią ustalenia niczyjej tożsamości, nie są to dane osobowe. Jednak dla przedsiębiorcy i jego pracowników, posiadających dostęp do systemów, w których znajdują się informacje umożliwiająca identyfikację osoby, której te dane dotyczą, będą to

dane osobowe. Bo oni będą mogli ustalić, jaka osoba kryje się pod określonym identyfikatorem, a poprzez to ustalić jej tożsamość, zidentyfikować ją. I także dlatego, że będą wiedzieć, co się kryje np. pod wartościami opisanymi „średnia", „potencjał" lub „profil".

Jak widać, informacje osobowe mają charakter subiektywny, oceny i w większości przypadków będą zależne od kontekstu, w którym się znajdują.

Najczęściej spotykane rodzaje danych

Już wiemy, że w zasadzie dowolny zestaw informacji o osobie może stanowić dane osobowe, wszystko zależy od tego, czy ten, kto jest w ich posiadaniu będzie mógł ustalić tożsamość osoby i jak szybko uda mu się to zrobić.

Poniżej podam przykłady zestawów danych, omówię, w jakim zakresie i z jakimi danymi oraz kto będzie miał możliwość ustalenia tożsamości osoby, a przez to dla kogo określone informacje będą danymi osobowymi. Wiedza ta pozwoli zrozumieć, jakie są zasady określania, które informacje to dane osobowe.

Imię i nazwisko

Imiona powstały na skutek potrzeby identyfikowania osób w niewielkich społecznościach. Tam, gdzie te społeczności były większe, wykształciły się przydomki, a nawet nazwiska. Nazwiska pochodzą z Chin, gdzie tworzono je w ramach hołdu swoim przodkom, a ich historia zaczyna się ok. 2852 p.n.e. Rzymianie 300 lat p.n.e. zaczęli używać systemu nazywania opartego na imieniu, nazwie rodu i nazwie rodziny. Taki system spotkać można u naszych górali np. Bachleda-Curuś. W Polsce nazwiska pojawiły się dość późno, bo w XV w., do tego czasu stosowano przydomki (Leszek *Biały*, Władysław *Wygnaniec)*.

Obecnie imię i nazwisko jest podstawą identyfikowania osoby w społeczeństwie i tak jak wizerunek w bezpośrednim kontakcie identyfikuje osobę, tak imię i nazwisko pomagają identyfikować ją we wszelkiego rodzaju dokumentach, wykazach, spisach, ewidencjach. W działalności gospodarczej trudno sobie wyobrazić identyfikowanie osoby bez tak zasadniczych danych, jak imię i nazwisko.

W dużych społeczeństwach imiona i nazwiska często się powtarzają. W Polsce najczęściej spotykane pięć nazwisk nosi aż 657 tysięcy osób:

Najbardziej popularne nazwiska w Polsce w 2009 r.

Nazwisko	Liczba osób o tym nazwisku

Nowak	207348
Kowalski/-a	140471
Wiśniewski/-a	111174
Wójcik	100064
Kowalczyk	98739
Nowak	207348

Samych imion i nazwisk nie należy traktować jako dane osobowych, tworzą one jedynie zbiór pewnej ilości osób o określonym imieniu i nazwisku, nie pozwalają na jednoznacznie ustalenie tożsamości danej osoby. Imiona i nazwiska unikatowe bez wątpienia ułatwiają zidentyfikowanie osoby, mimo to wciąż nie stanowią same danych osobowych, bo jak jednak przedsiębiorca miałby stwierdzić, że dane imię i nazwisko jest właśnie unikatowe? Dlatego następujące przykładowe dane nie identyfikują jednoznacznie osób:
- Jan Nowak,
- Paulina Chmielewska,
- Zuzanna Wiśniewska,
- Anna Kępa,

Wiele osób publikuje swoje dane na portalach społecznościowych, posiadając imię i nazwisko osoby można czasami znaleźć ją w internecie, warto jednak zauważyć, że bez dodatkowej informacji takiej jak np. wizerunek, miejscowość zamieszkania, trudno ją jednoznacznie zidentyfikować.

Samo imię i nazwisko dopiero w połączeniu z inną dodatkową informacją o osobie może stać się danymi osobowymi np.:

- Jan Kępa - uczeń szkoły podstawowej nr 6 w Siedlcach,
- Mateusz Morawiecki - premier,
- Paweł Litwiński - adwokat,
- Lidia Burdzy - koordynator ds. szkoleń, ODO 24 sp. z o.o.,
- Stefan Żeromski ze Strawczyna.

Imię i pierwsza litera nazwiska nie stanowią danych osobowych, np. *Sebastian D., Paweł T.*, ale podane z dodatkowymi informacjami mogą już niekiedy umożliwiać identyfikację osoby. Przykładem może być informacja w serwisie Interia.pl: *Ja się nigdy nie przyznałem do popełnienia tego czynu - mówi reporterce Interwencji Krystian B., filozof, pisarz, autor skandalizującej powieści »Amok«*. Mimo że nie są tutaj podane pełne dane osoby, to publikacja ujawnia

dane osobowe, bo na podstawie takich informacji jak imię, zawód, autor określonych dzieł pozwala na szybkie określenie tożsamości autora - wystarczy jedynie chwile poszukać w zasobach sieci Internet.

Adres i kod pocztowy, dzielnica miasta

Adres identyfikuje miejsce. Właściwie miejsce na ziemi identyfikują współrzędne geograficzne, jednak oznaczenie GPS N:52°13'54" E:21°0'21" niewiele mówi i jest niewygodne do korzystania, znacznie łatwiej zapamiętać lokalizację w postaci słownej *Plac Defilad 1 w Warszawie*. To jest tak samo, jak z „miejscami" w internecie, znacznie łatwiej zapamiętać www. difin.pl niż 194.181.6.21.

Sam adres nie jest daną osobową, identyfikuje on tylko określone miejsce. Niektórzy uważają, że można zidentyfikować osobę przez samą możliwość kontaktu z nią, bo pod danym adresem będzie pewnie jakaś osoba. Jednak trudno sobie wyobrazić, jak by to miało nastąpić, poprzez wysłanie listu na wskazany adres? Zapukanie do drzwi i zapytanie *kim jesteś, jak się nazywasz?* Pod wskazanym adresem może mieszkać kilka osób, więc trudno uznać, że to jest jakakolwiek identyfikacja, a cóż dopiero jednoznaczna.

Adres w połączeniu z dodatkową informacją mógłby już identyfikować w niektórych przypadkach osobę. Na pewno połączony z imieniem i nazwiskiem pozwala ustalić tożsamość osoby, przez co wtedy staje się w takim kontekście daną osobową. Tak zresztą zwykliśmy uważać intuicyjnie, takie dane zawarte są przecież w dowodzie osobistym, prawie jazdy czy dowodzie rejestracyjnym samochodu. Można uznać nawet, że adres połączony z samym imieniem będzie już danymi osobowymi, bo umożliwi kontakt z konkretną osobą.

Niekiedy sam adres zestawiony z danymi niekoniecznie na pierwszy rzut oka osobowymi, może stanowić dane osobowe. Tak będzie w przypadku adresu lokalu połączonego z informacją o zaleganiu z czynszem wobec spółdzielni mieszkaniowej i wysokością zaległości. Nie można publikować takich informacji, bo będzie to w istocie udostępnienie danych osobowych, gdyż inni członkowie spółdzielni mogą z łatwości sprawdzić, kto widnieje w rejestrze członków spółdzielni, a przez to ustalić tożsamość osoby nieregulującej czynszu.

Niektóre firmy zbieraj sam kod pocztowy podczas zakupów. Kod pocztowy pozwala na określenie ulicy w dużych miastach lub miejscowości bądź regionu. Przedsiębiorca wiążąc kody pocztowe ze sprzedanymi towarami, może zbadać np. w jakich regionach, które towary sprzedają się najlepiej. Sam kod pocztowy nic jest daną osobową, nawet połączony z informacją o zakupach. W mniejszych

miejscowościach sprzedawcy pytają o kod i o dzielnicę - ale to także nie są samodzielnie dane osobowe.

Geolokalizacja

Geolokalizacja to informacja określająca położenie geograficzne obiektów (osoby, przedmiotu). Położenie to można wyznaczać z użyciem wielu rozmaitych środków takich jak np.:

- nadajniki telefonii komórkowej,
- sieci bezprzewodowe (WiFi),
- system GPS,
- połączenie z siecią internet,
- karty zbliżeniowe miejskie,
- karty zbliżeniowe w budynku z czytnikami (ang. geofeticing, tu brakuje polskiego określeniu, ja używam terminu geogrodzenie),
- RFID (radiowe etykiety produktów stosowane w sklepach),
- sieć bankomatowa lub terminali POS (to gdzie wypłacamy albo płacimy kartami).

Na dane geolokalizacyjne należy patrzeć pod dwoma kątami:

- dane, które są dopisywane do danych osobowych - wtedy dane geolokalizacyjne stają się automatycznie danymi osobowymi,
- dane geolokalizacyjne, jako dane, które mogą umożliwiać ustalenie tożsamości osoby (samodzielnie, bądź w połączeniu z innymi danymi, nieosobowymi).

Geolokalizacja niekiedy pozwala przedstawić dane w funkcji czasu, czyli pokazywać trasę, szybkość oraz czas przebywania w określonych miejscach.

Do geolokalizacji przydatna, a właściwie niezbędna jest mapa, na której można oznaczać lokalizację obiektu. Np. informacja o tym, że zdjęcie danej osoby zostało wykonane w lokalizacji N:52°13`54" E:21°0'21" będzie prawie bezużyteczna, jeśli nie będziemy można jej „przetłumaczyć" na położenie na mapie. Dopiero takie informacje związane z jakimś określonym faktem będą mogły stanowić użyteczne dane i będą mogły być wykorzystane, aby np. zidentyfikować osobę.

Informacja o tym, gdzie określona osoba przebywa lub przebywała co prawda nie ustala wprost jej tożsamości, ale niesie za sobą bardzo dużo informacji np. na podstawie takich danych geolokalizacyjnych połączonych w funkcji czasu można ustalić pewne wzorce przemieszczania się, a z nich wyciągnąć wnioski, że:

- tam gdzie w nocy nie ma aktywności (przemieszczania się), osoba zapewne mieszka,

- tam gdzie rano się przemieszcza - zapewne pracuje.

Już na podstawie chociażby tych danych można ustalić tożsamość osoby. Gdy dane zbierane są przez długi okres, można z nich wnioskować znacznie więcej.

Geolokalizacja umożliwia zebranie znacznie bogatszych informacji, np. przekonania religijne (coniedzielna wizyta w kościele), informacja o stanie zdrowia (przebywanie w szpitalu, w specjalistycznych przychodniach) itp. Zbieranie takich informacji jest w zasadzie tożsame śledzeniu. Każdy może sobie wyobrazić, czego dowiedziałby się posiadacz takich danych, gdyby wiedział, gdzie się przemieszczamy. Uważa się nawet, że na bazie zebranych danych z telefonu komórkowego algorytmy wkrótce będą w stanie przewidzieć, gdzie jego posiadacz może znaleźć się za określony czas.

Dlaczego geolokalizacja wydaje się taka ważna? Dzisiaj większość telefonów posiada odbiornik GPS, a więc jest w stanie ustalić swoje położenie geograficzne, zaś możliwość połączenia z internetem pozwala te dane przesyłać. Przykładowo podczas korzystania z bezpłatnej nawigacji Google telefon nieustannie wysyła do serwera informację o lokalizacji.

Informacje geolokalizacyjne posiadają także operatorzy telefonii komórkowej, gdyż nadajniki sieci komórkowej rejestrują, w jakim obszarze (komórce) znajduje się aktualnie telefon, a zatem i jego posiadacz.

Nawet sieci bezprzewodowe (Wi-Fi) pozwalają ustalić położenie geograficzne. Z nazwą sieci związany jest tzw. MAC - sprzętowy identyfikator urządzenia. Google zbiera z całego świata takie informacje za pomocą telefonów komórkowych. Później, aby ustalić swoje położenie, wystarczy przesłać do Google informacje o tym, jakie sieci bezprzewodowe są w okolicy, a ten sprawdzi ich położenie na mapie i w ten sposób lokalizacja działa szybciej.

Geolokalizacja ma coraz powszechniejsze zastosowanie przykładem czego są hipermarkety, w których śledzi się koszyki z odbiornikiem RFID. W sklepie są rozmieszczone nadajniki i mogą śledzić, gdzie przemieszcza się i jak długo zatrzymuje się przy określonych towarach ten, kto trzyma w ręku koszyk. Na podstawie tak zebranych informacji można przy kasie np. skierować do niego odpowiednio dopasowaną reklamę.

Dane geolokalizacyjne zapisywane są także często w zdjęciach, gdy są wykonywane przez aparat z funkcją GPS, głównie telefon, gdyż GPS jest najbardziej popularny w telefonach komórkowych, a te z kolei wyposażane są standardowo w aparat fotograficzny. Korzystając z danych geolokalizacyjnych z łatwością można ustalić miejsce wykonania zdjęcia, często nawet konkretny adres.

Elektroniczne czytniki książek także zapisuj informacje o tym m.in. w jakim

miejscu jego posiadacz się znajduje i co aktualnie czyta tak jest w przypadku np. Amazon Kindle.

Korzystanie z informacji geolokalizacyjnych stanowi spore zagrożenie dla prywatności osób i warto odnotować fakt, że w sprawie geolokalizacji w dniu 16 maja 2011 r. grupa robocza art. 29 przyjęła *Opinię 13 2011 (WP185) w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych, czyli smartfonach.*

Warto też zauważyć, że na zbieranie takich danych ustawa prawo telekomunikacyjne nakłada ograniczenia (art. 166), ale - co ciekawe - tylko wobec przedsiębiorców telekomunikacyjnych.

Numer dokumentu

Dla ustalenia czy numery dokumentów będą stanowić dane osobowe warto przytoczyć przykład karty miejskiej. Otóż dla zwykłego obywatela, który miałby dostęp do karty miejskiej z samym tylko jej numerem ustalenie tożsamości jej właściciela wymaga jednak pewnego czasu i działań. Dlatego dla niego sam numer karty miejskiej nie będzie stanowił danej osobowej.

Numer karty miejskiej jest daną osobową, ale tylko dla tych osób, które na jego podstawie mogą ustalić tożsamość jej właściciela to np. pracownicy przewoźnika upoważnieni do przetwarzania informacji zawartych w systemie informatycznym związanym z funkcjonowaniem karty miejskiej.

W stosunku do dowodu osobistego, paszportu, prawa jazdy i innych dokumentów można przyjąć, że numer i seria tych dokumentów nie stanowią danych osobowych „dla zwykłego obywatela". Barierą jest tutaj możliwość uzyskania informacji o tożsamości posiadacza dokumentu na podstawie tych informacji. Nie dotyczy to osób, które posiadają dostęp do rejestrów, w których takie dane są przechowywane, a co za tym idzie, pozwalają na ustalenie tożsamości osoby, której dokumenty dotyczą.

Jakie informacje są w numerach dokumentów potwierdzających tożsamość? W numerze prawa jazdy znajduje się informacja o organie, który je wydał. Posiadając numer dowodu osobistego można metodami statystycznymi wywnioskować, kiedy dokument został wydany. Warto pamiętać, że dokument tożsamości, a dokument potwierdzający tożsamość to nie to samo. Przykładowo prawo jazdy potwierdza tożsamość, ale nie jest dokumentem tożsamości. Warto zauważyć, że numer skradzionego dowodu będzie daną osobową dla administratora „Systemu Dokumenty Zastrzeżone" oraz zapewne dla banków mających dostęp do tej bazy.

Karty zbliżeniowe służące do wejść i wyjść do budynku posiadają numery. Będą one dla administratora systemu kart danymi osobowymi, jeśli będą w systemie powiązane z określoną osobą.

Podsumowując, każdy numer dokumentu będzie daną osobową dla jego wystawcy, o ile ten prowadzi ewidencję, komu te dokumenty wystawia i na jaki czas. Dla innych osób najczęściej sam ten numer nie będzie daną osobową.

Numer PESEL

Numer PESEL nadaje się głównie obywatelom polskim, chociaż mogą go otrzymać także cudzoziemcy, jeśli są zameldowani w kraju na dłuższy pobyt. PESEL jest swojego rodzaju identyfikatorem osoby, który nie zmienia się od momentu jego nadania. Zakłada się, że nie ma dwóch takich samych numerów PESEL, więc jest to identyfikator unikalny, co zresztą podkreślono w ustawie o ewidencji ludności i dowodach osobistych używając wyrazu „jednoznacznie" (art. 3la ust. 1):

Numer Powszechnego Elektronicznego Systemu Ewidencji Ludności, zwany w niniejszej ustawie „numerem PESEL" jest to 11-cyfrowy, stały symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery - liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego.

W społeczeństwie zwykło się przykładać dużą uwagę do zachowywania numeru PESEL w tajemnicy, podczas gdy w gruncie rzeczy numer ten jest niczym innym jak tylko identyfikatorem. Można upraszczając powiedzieć, że osoby w społeczeństwie są ponumerowane i PESEL jest po prostu numerem osoby. Wartość tego numeru nie jest jakaś szczególna, jest to po prostu cyfrowy symbol służący do identyfikacji osoby, a właściwie ją ułatwiający. Niemniej jednak do zachowania numeru PESEL w poufności należy przykładać szczególną uwagę.

Z powodu swojej unikalności jest bardzo chętnie używany przez przedsiębiorców. Dzięki numerowi PESEL można w systemie odnaleźć i połączyć różne rekordy (wpisy) dotyczące tej samej osoby, ale zapisane inaczej. Gdyby nie numer PESEL, trudno byłoby ocenić, czy to są te same osoby, czy nie.

Zwykło się uważać, że sam numer PESEL stanowi dane osobowe w rozumieniu RODO. Organ państwowy nie może sądzić inaczej, gdyż tak jest zapisane w ustawie o ewidencji ludności, jest to *stały symbol numeryczny,*

jednoznacznie identyfikujący osobę, zaś RODO stanowi, że dane osobowe to wszelkie informacje dotyczące osoby, *której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny*.

Spójrzmy jednak na te 11 cyfr, które składają się na numer PESEL, przez pryzmat RODO. Jaki przekaz informacyjny one niosą ze sobą? Dowiemy się z nich daty urodzenia i płci jego posiadacza. Nie poznamy jego tożsamości, bo aby ją poznać, należy uzyskać dostęp do dodatkowych informacji powiązanych z numerem PESEL, a więc w istocie do bazy, w której są numery PESEL powiązane z danymi pozwalającymi na jej identyfikację. Sam numer PESEL dla tych, którzy nie mają bezpośrednio dostępu do rejestru PESEL albo innej bazy danych z numerami PESEL i danymi o osobie nie powinien stanowić danych osobowych.

Argumentem, który dodatkowo przemawia za tym, że samego numeru PESEL nie powinno się traktować jako dane osobowe jest chociażby to, że są to ciągi 11 cyfr i można je samodzielnie wygenerować, co zresztą często się robi, aby mieć dane do testowania programów komputerowych.

Mimo że sam numer PESEL w praktyce nie powinien być uznawany za dane osobowe, to lepiej go będzie (z przezorności) tak traktować, mając na uwadze fakt, że RODO powołuje się na „numer identyfikacyjny".

Na pewno fragment numeru PESEL, np. kilka jego pierwszych lub ostatnich cyfr nie stanowi danych osobowych. Warto odnotować fakt, że PESEL pozbawiony tylko jednej cyfry pozwala na uzupełnienie tej brakującej, można ją wyliczyć korzystając ze specjalnego algorytmu.

Niekiedy numery PESEL będą upubliczniane. Przykładowo Krajowy Rejestr Sądowy upublicznia numery PESEL składu Zarządu spółek. Do niedawna numer ten był także publikowany w wykazie certyfikatów księgowych.

Oznaczenia licencji na wykonywanie zawodu

Niekiedy osoby będą posiadać nadane numery związane z licencją na wykonywanie zawodu. Przykładami takich numerów będą:

- Numer Prawa Wykonywania Zawodu lekarza i lekarza dentysty,
- licencja ubezpieczeniowa agenta, brokera,
- licencja zarządcy nieruchomości,
- licencja pośrednika w obrocie nieruchomościami,
- numer licencji księgowego.

Czemu służą takie numery? Głównie temu, aby korzystający z ich z usług mieli możliwość sprawdzić, czy dana osoba rzeczywiście posiada uprawnienia do

wykonywania określonego zawodu lub czynności. Rola tych numerów podobna jest do numerów dokumentów tożsamości. Różnica jest taka, że numery licencji są często upublicznione w ogólnodostępnych rejestrach, tak bowiem można sprawdzić wiarygodność posługującego się numerem. Przykładowo na stronach Komisji Nadzoru Finansowego można sprawdzić, czy dana osoba posiada uprawnienia agenta ubezpieczeniowego bądź jest jego pracownikiem.

Nie zawsze sam numer będzie pozwalał na ustalenie tożsamości osoby nim się posługującej. Należy jednak brać pod uwagę, że niekiedy numery licencji, a nawet same certyfikaty są publikowane przez osoby np. w internecie, dlatego za każdym razem należy przeanalizować, czy taki numer pozwoli zidentyfikować osobę. Jakiś czas temu numer sam certyfikatu księgowego można było uważać za daną osobową, gdyż wykaz certyfikatów księgowych opublikowany na stronie internetowej Ministerstwa Finansów zawierał imię, nazwisko i numer PESEL.

Oczywiście sam numer licencji (w każdym prawie przypadku) będzie daną osobową dla tego, który zarządza bazą nadanych numerów.

Numer telefonu

Kiedyś telefon służył całej rodzinie, ale od czasów telefonii komórkowej sytuacja się zmieniła, dzisiaj numer telefonu bardziej związany jest z konkretną osobą niż z miejscem. Numer telefonu stanowi szczególną informację, gdyż umożliwia bezpośredni kontakt z osobą, mimo że w rozumieniu RODO sam (rozumiany jako cyfry) nie jest daną osobową. RODO skupiając się na ochronie danych silnie podkreśla konieczność identyfikacji osoby (ustalenia jej tożsamości), a dane kontaktowe wymykają się w pewnym sensie spod tego rozporządzenia, gdyż możliwość kontaktu nie musi prowadzić do ustalenia tożsamości. Może, ale nie musi.

Pomimo faktu, że numer telefonu nie jest samodzielnie daną osobową, to stanowi informacje, które mogą umożliwiać naruszenie sfery prywatności, dlatego w działalności gospodarczej lepiej traktować go tak, jakby to były dane osobowe.

Numer telefonu w połączeniu z imieniem albo z nazwiskiem należy uznawać bez wątpienia za dane osobowe, bo jedna z tych danych określa częściowo tożsamość osoby (a już na pewno ułatwia określenie tożsamości). Numer telefonu zestawiony z innymi informacjami o osobie, mimo iż nie zawsze stanowią dane osobowe, należy traktować bardzo ostrożnie.

Sam numer telefonu dla operatora świadczącego usługi telekomunikacyjne będzie danymi osobowymi. Ma on w swojej bazie klientów dane, pozwalające powiązać numer z danymi osoby i w ten sposób ją zidentyfikować.

Numer gadu-gadu

Gadu-gadu jest popularnym w Polsce komunikatorem internetowym (*ang. instant messenger).* Komunikator to program, który pozwala wysyłać natychmiastowe komunikaty pomiędzy dwoma lub więcej komputerami. Można powiedzieć, że to taka jakby poczta, tylko natychmiastowa. Kiedyś tego rodzaju programy nazywało się chat *(ang. chat* - rozmowa). Użytkownik Gadu-Gadu otrzymuje unikalny identyfikator, złożony z cyfr. Posiadając identyfikator Użytkownika można sprawdzić, jakie wpisał o sobie informacje, ale nie są one weryfikowane podczas zakładania konta, w związku z czym nie muszą być wiarygodne. Na tej podstawie należy uznać, że numer Gadu-Gadu samodzielnie nie jest daną osobową, będzie nią wtedy, gdy zostanie powiązany z danymi o osobie. Dla dostawcy usługi Gadu-Gadu oczywiście będą to dane osobowe.

Adres e-mail

Adres poczty elektronicznej (e-mail) pozwala na kontakt z osobą, podobnie jak numer telefonu, różni się jednak od niego większym przekazem informacyjnym. Numer telefonu nie niesie ze sobą żadnych dodatkowych informacji, co najwyżej może wskazywać operatora (Play, Orange, Plus, etc.), natomiast adres poczty elektronicznej może określać np. miejsce zatrudnienia, przynależność do pewnej organizacji lub ujawniać określone cechy osoby.

Firmowe adresy zawierają w sobie imię i nazwisko i pozwalają ustalić zakład pracy. Możliwość kontaktu połączona z identyfikacją osoby z imienia i nazwiska oraz zakładu pracy pozwala na ustalenie tożsamości użytkownika tego adresu i z tego powodu firmowy adres e-mail uznawany jest za dane osobowe. Nie ma znaczenia, że adres taki jest upubliczniany, powszechnie dostępny.

Jak to jest, że w adresie poczty „zaszyte" są takie informacje? Przykładowo adres poczty elektronicznej leszek.kepa@superiodo.pl składa się z dwóch części:

- nazwy konta - np. **leszek.kepa**
- domeny - **superiodo.pl**

Do domeny można dodać przedrostek www i w przeglądarce internetowej sprawdzić co się mieści pod tak utworzonym adresem. Nie zawsze pod odgadniętym w ten sposób adresem znajdzie się firmowa strona internetowa, jednak to jeszcze nie zamyka drogi do identyfikacji, do jakiego podmiotu należy adres pocztowy, a właściwie do kogo należy domena.

Domena jest elementem adresu DNS (ang. *domain name system),* wykorzystywanego do nazywania urządzeń w sieci internet. Pocztę w internecie przekazują sobie komputery i muszą wiedzieć, jak się ze sobą komunikować.

Komputery w sieci internet komunikują się z użyciem numerów IP. Przykładowo numer IP komputera, na którym znajdują się strony internetowe Wirtualnej Polski to 212.77.100.101. Taki adres trudno zapamiętać i wprowadzono system DNS, który zamienia numery IP na nazwy domenowe. Ludziom łatwiej jest zapamiętać nazwę wp.pl niż numer IP. Dokładnie z tego samego powodu korzysta się z książki telefonicznej w telefonie komórkowym, bo łatwiej zapamiętać imię i nazwisko niż numer telefonu. Gdyby nie było systemu DNS, adresy poczty elektronicznej wyglądałyby mniej więcej tak leszek.kepa@62.179.1.4.

Domeny nie można mieć na własność, można jedynie z niej korzystać, tak jak korzysta się z numeru telefonu. Dlatego posiadacza domeny określa się mianem abonenta. Informację o tym, kto jest abonentem danej domeny można uzyskać dzięki usłudze WHOIS. Jeśli domena jest firmowa tj. kupiona przez firmę, to w bazie WHOIS znajdą się jej nazwa, siedziba i telefon. I w ten sposób posiadając firmowy adres e-mail osoby można uzyskać następujące informacje o osobie:

- imię,
- nazwisko,
- nazwa zakładu pracy,
- adres zakładu pracy,
- numer telefonu do zakładu pracy.

Dlatego firmowe adresy poczty elektronicznej należy uznawać za dane osobowe. Podobnie ma się rzecz z adresami uczelnianymi, które otrzymują studenci.

Adresów skrzynek pocztowych na darmowych serwerach pocztowych nie należy uważać za dane osobowe, gdyż maksimum czego można się dowiedzieć, to imię i nazwisko, a i to nie musi być do końca prawdziwe, bo nic nie stoi na przeszkodzie, aby założyć konto pocztowe, podając dowolne, nieprawdziwe dane. Zatem adresy takie jak leszek.kepa@gmail.com, czy paulina.chmielewska@wp.pl nie powinny być uznawane za dane osobowe.

Prowadząc serwis, w którym będą rejestrować się osoby i podawać swoje adresy e-mail należy uznać, że będzie się zbierać dane osobowe, bo zawsze trafi się ktoś, kto poda adres służbowy poczty elektronicznej.

Adres strony internetowej

W internecie można znaleźć sporo osobistych witryn takich jak www.jankowalski.pl. Aby zarejestrować taką domenę, nie trzeba nazywać się Jan Kowalski. Wystarczy jedynie uzasadnić wybór takiej domeny (np. serwis poświęcony genezie takich imion i nazwisk) - a więc w konsekwencji nazwa

domeny nie „definiuje" właściciela. Samej nazwy domeny nie uznaje się za dane osobowe, chociaż może ona umożliwiać identyfikację osoby poprzez dane zamieszone na witrynie albo opublikowane w bazie WHOIS (o ile osoba wyraziła zgodę na ich opublikowanie).

Loginy i nicki

W systemach komputerowych użytkownik „przedstawia się" systemowi (identyfikuje) używając identyfikatora, a na potwierdzenie, że ma prawo się nim posługiwać podaje hasło (uwierzytelnia). Na identyfikatory mówi się także login.

W sieci internet używa się dodatkowo jeszcze nicków. Nick jest przybranym identyfikatorem, którego używa się w celu określenia swojej tożsamości w społeczności internetowej, nick (ang. *nickname)* oznacza przezwisko, pseudonim. Nicki mają przede wszystkim zastosowanie na forach dyskusyjnych, czatach (programach do internetowych pogaduszek) i blogach (internetowych pamiętnikach), stanowią swojego rodzaju podpis osoby. Bardzo często spotykane są w świecie cyberprzestępców, którzy wolą posługiwać się nimi, aby zachować anonimowość.

Loginy nie są danymi osobowymi, dopóki nie zostaną połączone z innymi danymi, pozwalającymi na ustalenie tożsamości osoby. Ta sama zasada odnosi się do nicków. Np. nick **odosklep** w serwisie aukcyjnym nie stanowi danych osobowych, gdyż nie pozwala na ustalenie tożsamości osoby nim się posługującej. Tożsamość uda się ustalić dopiero po zawarciu umowy z osobą (po zalicytowaniu), wówczas licytujący otrzyma wiadomość z danymi drugiej strony. Dla administrującego serwisem aukcyjnym nicki będą stanowić dane osobowe, gdyż posiada on możliwość powiązania go z informacjami o osobie np. z imieniem, nazwiskiem, adresem zamieszkania i adresem poczty elektronicznej.

Numer rejestracyjny samochodu, VIN

Numery rejestracyjne pojazdu ujawniają przede wszystkim region, w którym samochód jest zarejestrowany. Pierwsza litera oznacza województwo, a następna lub dwie oznaczają powiat. Jeżeli jest tylko jedna litera, samochód zarejestrowany jest w powiacie grodzkim lub dzielnicy Warszawy. Po tych literach następuje „wyróżnik pojazdu". Tablice rejestracyjne występują w sześciu rodzajach: zwyczajne, tymczasowe, indywidualne, zabytkowe, dyplomatyczne, służb specjalnych.

Sam numer rejestracyjny nie zawiera w sobie żadnej interesującej informacji i jako taki nie może być uznany samodzielnie za dane osobowe. Jednak są od tego

wyjątki. W małej społeczności numer rejestracyjny będzie stanowić daną osobową, gdyż numer kojarzy się z samochodem, a ten bezpośrednio z jego właścicielem, który może być „znany w okolicy". Dlatego np. na osiedlu spółdzielnia nie może wywiesić listy numerów rejestracyjnych źle parkujących samochodów albo w inny sposób naruszających wewnętrzne przepisy administratora, bo dochodzić będzie do udostępniania danych osobowych.

Numer rejestracyjny wraz z imieniem i nazwiskiem posiadacza pojazdu stanowi dane osobowe.

Ciekawą sprawą jest, że w większości ofert sprzedaży pojazdu, jakie można znaleźć w internecie, numery rejestracyjne pojazdów są zamaskowane. Niektórzy sądzą, że prawdopodobnie z obawy przed urzędami skarbowymi, gdyż nierzadko wartość transakcji jest zaniżana, aby zapłacić niższy podatek. Wydaje się jednak, że bardziej chodzi o ochronę prywatności - sprzedający nie chce, aby znajomi i rodzina poznali wartość transakcji, poza tym zdjęcie z numerami rejestracyjnymi mogłoby zostać niewłaściwie przez kogoś użyte, co stanowiłoby potencjalne źródło kłopotów.

Publikowanie na stronach internetowych źle zaparkowanych samochodów wraz z ich numerami rejestracyjnymi należy traktować z dużym dystansem - do takich materiałów mogą mieć dostęp osoby, które są w stanie zidentyfikować posiadacza samochodu. Może niekoniecznie jest to udostępnianie danych osobowych, ale bez wątpienia można w ten sposób naruszać dobra osobiste i sferę prywatności.

Numer VIN (ang. *Vehicle Indentification Numer)* jest numerem oznaczającym pojazd, a właściwie jego nadwozie. Z numeru VIN można dowiedzieć się wielu szczegółów o samochodzie, natomiast o właścicielu niewiele. Samego numeru VIN nie można uznać za dane osobowe, jednak z pewnością VIN będzie nimi dla organu rejestrującego, pod warunkiem, że pojazd jest zarejestrowany. Może też być danymi osobowymi dla zakładu ubezpieczeń, który ubezpieczył samochód.

Przez internet, np. na stronie www.autobaza.pl/sprawdz-pojazd można sprawdzić numer VIN, zdekodować informacje zawarte w nim, i sprawdzić czy występuje w internetowych bazach pojazdów skradzionych. Natomiast na stronach Ubezpieczeniowego Funduszu Gwarancyjnego (UFG) można sprawdzić czy dany pojazd posiada ubezpieczenie OC - wystarczy podać numer rejestracyjny bądź VIN.

Numer IP

Numer IP identyfikuje urządzenia w sieci Internet. Zobaczmy, w jakich okolicznościach numer IP będzie dotyczył osób fizycznych i kiedy będzie danymi

osobowymi.

Wiemy już, że komputery w sieci internet komunikują się z użyciem numerów IP. Numer IP jest swojego rodzaju internetową tablicą rejestracyjną komputera, pozwalającą się z nim komunikować w sieci używającej protokołu IP. Tego protokołu używa sieć internet i większość sieci lokalnych, domowych i firmowych. Żeby wyobrazić sobie, o co chodzi z numerami IP, zacznę od adresu MAC. Urządzenia w sieci komputerowej posiadają tzw. adres MAC (ang. *media access control).* W świecie samochodów odpowiednikiem adresu MAC mógłby być numer VIN samochodu. Adres MAC jest zawsze taki sam i skojarzony jest ze sprzętem. Przykładowy adres MAC wygląda następująco: 08:00:27:03:DA:77. Adres MAC identyfikuje właściwie nie tyle komputer, co jego kartę sieciową. Oznacza to, że gdy np. laptop może korzystać z sieci bezprzewodowej Wi-Fi i może także jednocześnie korzystać z sieci przewodowej (na „kabel"), to są w nim dwie karty sieciowe, a każda z nich ma swój własny adres MAC. Oznacza to też, że mógłby mieć dwa adresy IP. Tak jak telefon komórkowy na dwie karty SIM. Jeśli do komputera zostanie podłączony modem 3G (tzw. internet przez komórkę), to ten modem staje się jednocześnie kartą sieciową i ta karta otrzyma numer IP od operatora.

Numer IP może zostać nadany:

- ręcznie - np. przez administratora sieci, co obecnie zdarza się niezmiernie rzadko,
- automatycznie - na pewien określony czas.

Automat, który nadaje numery IP nazywa się serwerem DHCP (ang. *dynamic host configuration protocol).* Komputer, który może przyjąć numer IP musi być odpowiednio skonfigurowany (np. w ustawieniach karty sieciowej powinien mieć włączoną opcję „uzyskaj adres IP automatycznie"), większość komputerów i innych urządzeń np. smartfonów już jest tak skonfigurowanych, dzięki temu wystarczy włączyć urządzenie do sieci i ono wypożyczy numer IP od serwera DHCP automatycznie. Numer dzierżawiony jest na określony czas. Jeśli komputer zostanie wyłączony, a następnie po terminie tej dzierżawy zostanie włączony, to może (chociaż nic musi) uzyskać zupełnie inny numer IP. Serwer DHCP wypożyczając numery IP zapisuje, komu je wypożyczył (jakiemu adresowi MAC) i w jakim okresie.

Wypożyczony adres IP można poznać po tym, że parametr *DHCP włączone* ma wartość *Tak* oraz są określone terminy dzierżawy numeru IP.

Każde urządzenie, które komunikuje się w sieci internet, przedstawia się swoim numerem IP. Podczas oglądania stron internetowych serwer WWW, serwujący strony internetowe, zapisuje datę, czas i numer IP oglądającego. Jednak

numer, jaki odnotuje serwer WWW nie zawsze będzie tym samym numerem, jaki ma komputer. Jeśli komputer podłączony jest do internetu za pośrednictwem routera bezprzewodowego, to w sieci nie będzie widoczny numer IP komputera, tylko numer IP routera. Dodatkowo w przeglądarce można ustawić tzw. serwer proxy (internetowego pośrednika w oglądaniu stron), przez którego będą „przechodzić" oglądane strony WWW i wtedy w internecie komputer będzie widoczny pod numerem IP tego pośrednika.

Dla przeciętnej osoby numer IP nie może być daną osobową, nie identyfikuje on jednoznacznie osoby, ani nawet nie identyfikuje jednoznacznie komputera. Identyfikuje tzw. interfejs sieciowy komputera, routera bądź modemu GSM. Wiarygodność numeru IP jest mała, bo dość łatwo schować się za innym numerem IP albo podszyć się pod inny numer IP (tzw.. *IP spoofing).*

Widać więc, że jeśli już numer IP miałby być daną osobową, a raczej składnikiem danych osobowych, to tylko dla dostawcy usług internetowych, który przy pewnym nakładzie pracy może ustalić tożsamość osoby korzystającej z sieci.

Numer rachunku bankowego

Numer rachunku bankowego (NRB) składa się z 26 cyfr. W cyfrach od 3 do 10 znajduje się numer rozliczeniowy jednostki organizacyjnej banku, więc można ustalić w jakim banku, a nawet w którym jego oddziale założone jest konto.

Sam numer rachunku bankowego w zasadzie nie prowadzi do identyfikacji osoby, ale wyjątkiem będą tutaj banki, szczególnie bank macierzysty posiadacza rachunku, które w swoich systemach mogą odnaleźć podany numer i zidentyfikować osobę. Dla przeciętnej osoby numer rachunku nie będzie stanowić danych osobowych. Informacja o numerze rachunku, kwocie i dacie przelewu także nie będzie stanowić danych osobowych. Takie dane staną się „osobowe" dopiero wtedy, gdy zostaną połączone z danymi osobowymi, identyfikującymi osobę.

Dane osoby fizycznej prowadzącej działalność gospodarczą

Podmioty gospodarcze można podzielić na dwa rodzaje:

- osoby prawne oraz osoby ułomne tj. jednostki organizacyjne niebędące osobami prawnymi,
- osoby fizyczne.

Dane osób prawnych, w tym ułomnych, nie podlegają RODO (nie są przedmiotem rozporządzenia), bo nie są to dane dotyczące osób fizycznych.

Natomiast dane osób prowadzących działalność gospodarczą podlegają RODO i są chronione tak, jak dane „zwykłych" osób.

Dzisiaj dane osoby prowadzącej przedsiębiorstwo (np. imię, nazwisko, PESEL) stanowią dane osobowe, nie zmienia tego nawet fakt, że dane te są jawne.

Do osób fizycznych prowadzących działalność gospodarczą nie powinno się raczej wysyłać tzw. niezamówionych informacji handlowych. Nawet jeśli w CEIDG udostępniły biurowy adres poczty elektronicznej, który w wielu przypadkach normalnie nie stanowiłby danych osobowych (np. biuro@superiodo.pl), to poprzez fakt, iż adres ten związany jest z konkretną osobą fizyczną, nie można wysyłać na taki adres niechcianego mailingu.

Co więcej - takie adresy należy traktować jako dane osobowe, bo identyfikują określoną osobę fizyczną prowadzącą działalność gospodarczą. Są one dostępne publicznie i poprzez fakt ich udostępnienia w bazie CEIDG związane z określoną osobą, a zatem prowadzą do łatwej identyfikacji osoby.

Numer NIP, REGON

NIP i REGON są doskonale znane przedsiębiorcom. NIP jest numerem identyfikacji podatkowej, jego nadanie następuje w drodze decyzji wydanej przez naczelnika urzędu skarbowego, a zobowiązani do jego posiadania są wszyscy, którzy są podatnikami.

Od 1 września 2011 r., zgodnie z art. 3 ust. 1 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników, istnieją dwa identyfikatory podatkowe, tj.:

- numer PESEL - w przypadku podatników będących osobami fizycznymi objętymi rejestrem PESEL nieprowadzących działalności gospodarczej lub niebędących zarejestrowanymi podatnikami podatku od towarów i usług,
- NIP w przypadku pozostałych podmiotów podlegających obowiązkowi ewidencyjnemu, o którym mowa w art. 2 ustawy.

W numerze NIP znajduje się informacja o urzędzie skarbowym, który go nadał (pierwsze cyfry). Numer NIP jest więc w zasadzie czymś na kształt numeru PESEL, tyle że w odniesieniu do podatników. Osoba postronna nie uzyska żadnych informacji z Krajowej Ewidencji Podatników, w której te numery się znajdują, bo dostęp do niego jest ograniczony głównie do organów publicznych takich jak sądy, komornicy, organy podatkowe, celne, itd. Chociaż NIP identyfikuje także osoby fizyczne, to mało kto będzie mieć możliwość zidentyfikowania osoby z jego użyciem. Z użyciem numeru NIP można jednak zidentyfikować podmiot prowadzący działalność gospodarczą, wyszukując

jego dane w rejestrze REGON.

Numer REGON jest identyfikatorem podmiotu gospodarki narodowej wpisanego do rejestru REGON. Przedsiębiorca jest takim podmiotem.

W rejestrze wpisane są następujące rodzaje podmiotów:

- osoby prawne,
- jednostki organizacyjne niemające osobowości prawnej,
- osoby fizyczne prowadzące działalność gospodarczą, w tym prowadzące indywidualne gospodarstwa rolne.

Z rejestru dostępne są o podmiocie m.in. następujące dane:

- numer identyfikacyjny REGON,
- nazwa podmiotu i adres siedziby,
- numer telefonu i faksu siedziby, adres poczty elektronicznej oraz strony internetowej, o ile podmiot poda te dane do rejestru,
- numer identyfikacji podatkowej NIP,
- forma prawna, forma własności,
- wykonywana działalność, w tym rodzaj przeważającej działalności,
- daty związane z podmiotem - data powstania, rozpoczęcia działalności, zawieszenia i wznowienia działalności, wpisu do ewidencji lub rejestru, zakończenia działalności itd.,
- nazwy organu rejestrowego, nazwa rejestru (ewidencji) i nadany w rejestrze numer.

Prowadzący rejestr zadbał o prywatność osób fizycznych podkreślając na swojej witrynie internetowej, że *nie udostępnia się osobom trzecim informacji o numerze telefonu i faxu, adresie poczty elektronicznej oraz strony internetowej osoby fizycznej prowadzącej działalność gospodarczą podlegającej wpisowi do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG).* Zawartość rejestru można sprawdzić na stronie internetowej http://www.stat.gov.pl/rtgon/podając numer Regon lub NIP.

Pojęcie osoby fizycznej prowadzącej działalność gospodarczą w rozumieniu ustawy o statystyce publicznej (czyli dla GUS) jest nieco szersze niż np. w ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców, gdyż obejmuje zarówno osoby fizyczne prowadzące działalność gospodarczą, a co za tym idzie wpisane do rejestru CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej), jak też dodatkowo inne osoby prowadzące działalność na własny rachunek oraz w celu osiągnięcia zysku, a także osoby prowadzące indywidualne gospodarstwo rolne.

Numery karty płatniczej

Numer karty płatniczej co do zasady jest poufny i nie powinno się go nikomu ujawniać, co zresztą leży w interesie posiadacza karty. Numery te są szczególnie chronione w obrocie. Dla banku numer ten będzie danymi osobowymi, dla innych osób nie, gdyż z jego użyciem nie będą w stanie ustalić tożsamości osoby. Polski przedsiębiorca nie będzie takich danych gromadził, nawet jeżeli będzie przyjmował płatności kartami, dlatego, że musiałby spełnić surowe wymagania zabezpieczenia danych opisywane m.in. w standardach takich jak PCI DSS (ang. *Payment Card Industry - Data Security Standard).*

Jednak, *kiedy płacimy kartą, pojawiają się w bazie cztery ostatnie cyfry z jej numeru. W połączeniu z kodem pocztowym pozwala to z dużą trafnością wskazać konkretną osobę, bo rzadko zdarza się, żeby u dwóch mieszkających w pobliżu osób występowała ta sama kombinacja ostatnich cyfr na karcie płatniczej.* Pozwala to wyodrębnić transakcje określonej osoby, ale mimo to wciąż dla sklepu nie są to dane osobowe, jednak, jeśli baza danych zostanie sprzedana firmie, która ma możliwość powiązania cyfr na karcie z konkretnymi nazwiskami, to sprawa robi się poważniejsza.

Dane biometryczne

Biometria jest dziedziną nauki, zajmującą się „pomiarami istot żywych" w celu określenia ich indywidualnych cech. Kojarzy się głównie z analizą cech dłoni (linie papilarne, kształt dłoni) i oka (tęczówka oka, siatkówka), jednak biometria bada wszystko, co pozwala na identyfikowanie indywidualnych cech, wśród których są m.in.:

- owal twarzy, rozkład punktów charakterystycznych (oczy, usta) lub temperatur na twarzy,
- geometria (kształt) ucha,
- układ naczyń krwionośnych na dłoni lub przegubie ręki,
- kształt linii zgięcia wnętrza dłoni, układ linii papilarnych.

Biometria interesuje się także cechami behawioralnymi, związanymi z zachowaniem, takimi jak np.:

- sposób chodzenia,
- podpis odręczny,
- sposób pisania na klawiaturze,
- cechy charakterystyczne ruchu ust i poruszania gałki ocznej.

Biometria wykorzystywana jest głównie w takich dziedzinach jak:

weryfikacja tożsamości, autoryzacja dostępu do systemów informatycznych, czy identyfikacja. Dane biometryczne przetwarzane przez ogólnie dostępne systemy biometryczne są z reguły danymi zwykłymi. Pojedyncza dana biometryczna nie stanowi danych osobowych, na jej podstawie nie da się zidentyfikować osoby, bo trzeba mieć wcześniej zebrane informacje o osobie, połączone z jej wzorcem biometrycznym. Przykładowo odcisk palca będzie bezużyteczny, jeśli nie będzie wiadomo do kogo należy.

Dane biometryczne to szczególne dane, bo te dane przez całe życie określonej osoby są takie same. Bardzo ciekawie zauważa to Grupa robocza art. 29 w opinii na temat rozwoju technologii biometrycznych, która stwierdza, że dane biometryczne można zmienić albo usunąć, ale źródła, które pozwoliło na ich utworzenie (osoby) nie da się zmienić bądź usunąć tak jak robi się to z danymi.

Wizerunek, zdjęcie

Dzięki postępowi technologicznemu przestrzeń do przechowywania danych stała się tańsza, I to umożliwiło masowe powstawanie galerii zdjęć online oraz portali społecznościowych, które zawierają mnóstwo fotografii. Wizerunek osoby to nic innego jak specyficzna odmiana danych biometrycznych, ale ma on szczególne znaczenie, gdyż jest to w zasadzie jedyna z informacji, która z łatwością pozwala na identyfikację osoby fizycznej, a więc stanowi dane osobowe samodzielnie.

Niektóre serwisy społecznościowe używają biometrycznej technologii rozpoznawania twarzy. Przykładowo ładując zdjęcie do serwisu Facebook od razu pojawia się podpowiedź, kto ze znajomych na nim się znajduje.

Przetwarzając w firmie takie dane należy mieć na uwadze przepisy rozdziału 10 ustawy o prawie autorskim i prawach pokrewnych, a w szczególności art. 81 ust. 1 i 2:

1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.
2. Zezwolenia nie wymaga rozpowszechnianie wizerunku:

- osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
- osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

W orzeczeniu Sądu Najwyższego z dnia 27 lutego 2003 r. (sygn. akt IV CKN 1819/00), stwierdza się, że naruszenie prawa do wizerunku osoby fizycznej może nastąpić tylko wtedy, gdy fotografia opublikowana bez zgody danej osoby wykonana została w sposób umożliwiający jej identyfikację.

Sytuacje, w których dane są (bądź nie) osobowe

Wiemy, że nie istnieje oficjalny wykaz kategorii danych, o których można by powiedzieć, że są lub nie są danymi osobowymi. Już teraz widać, że wiele zależy od kontekstu, w jakim dane się znajdują albo właściwie od tego, z jakimi innymi informacjami dane mogą być zestawiane, a przez to, jaką informację o osobie mogą przekazywać.

Takie same dane o osobie w jednych sytuacjach mogą być danymi osobowymi, a w innych nimi nie będą.

Obowiązek zgłaszania naruszenia danych osobowych

Według przepisów RODO w sytuacji, gdy administrator danych osobowych stwierdzi **naruszenie danych osobowych lub wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, ma obowiązek bez zbędnej zwłoki zawiadomić osoby, których naruszenia dotyczą.

Kiedy możemy mówić o wysokim ryzyku naruszenia praw i wolności?

To sytuacja, gdy naruszenie prowadzi do powstania uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych.

Może to oznaczać np.:

- utratę kontroli nad własnymi danymi osobowymi,
- dyskryminację,
- ograniczenie praw,
- kradzież lub sfałszowanie tożsamości,
- oszustwo,
- stratę finansową,
- uszczerbek na reputacji,
- nieuprawnione odwrócenie pseudonimizacji,
- naruszenie dobrego imienia,
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
- wszelkie inne znaczne szkody gospodarcze lub społeczne.

Co istotne, to administrator będzie musiał ocenić, czy jest mało prawdopodobne, że dane naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Przez **naruszenie ochrony danych osobowych** rozumiemy 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. Nie chodzi wyłącznie o przypadki włamań do systemów informatycznych, ale tak prozaiczne zdarzenia, jak np. zgubienie laptopa czy wysłanie e-maila do niewłaściwej osoby (o ile oczywiście prowadzą do nieuprawnionego dostępu do danych osobowych).

Istnieją oczywiście **wymagania co do tego, jak powinno wyglądać zawiadomienie**. I tak głównym celem zawiadomienia jest uświadomienie osobom fizycznym, że ochrona ich danych osobowych została naruszona i poinformowanie ich o krokach, które powinny podjąć, by zabezpieczyć się przed negatywnymi skutkami. Administrator powinien wybrać metodę kontaktu, która zmaksymalizuje szanse właściwego zawiadomienia osoby fizycznej. Przede wszystkim powinno ono zostać napisane prostym i jasnym (zrozumiałym, ojczystym) językiem oraz zawierać opis charakteru naruszenia i jego konsekwencje. Ponadto powinno zawierać opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniom ochrony danych, a także informacje o Inspektorze Ochrony Danych w danej firmie czy instytucji.

Na szczęście istnieją wyjątki od tych przepisów i w pewnych sytuacjach nie ma obowiązku wysyłania zawiadomienia. Dotyczy to trzech sytuacji.

1. **Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony** i zostały one zastosowane do danych osobowych, których dotyczy naruszenie. Chodzi o zastosowanie przez Administratora takich środków jak szyfrowanie danych, które sprawia, że zmieniana jest zawartość plików bądź wiadomości w taki sposób, że ich treść jest bezużyteczna dla osoby trzeciej. Może to być także pseudonimizacja danych, czyli użycie liczby zamiast imienia i nazwiska rzeczywistej osoby. Wszystko po to, by nie można ich było przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowych informacji.
2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, poprzez np. przeprowadzenie oceny skutków tzw. DPIA. **Raporty DPIA są ważnymi narzędziami dla odpowiedzialności**, jako że pomagają administratorom danych nie tylko być w zgodności z wymaganiami RODO, ale także udowodnić, że odpowiednie środki były przedsięwzięte do zapewnienia zgodności z regulacjami (zobacz też art. 24 Rozporządzenia). Innymi słowy,

DPIA jest procesem budowania i demonstrowania zgodności z zapisami RODO.

3. **Naruszenie praw lub wolności osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku.** W takim przypadku administrator musi jednak wydać publiczny komunikat (np. na stronie internetowej) lub zastosować podobny środek, tak aby osoby, których dane wyciekły, zostały poinformowane o naruszeniu „w równie skuteczny sposób".

Niezawiadomienie osób, których dane zostały naruszone, zawiadomienie ich zbyt późno lub w niewłaściwy sposób **jest zagrożone karą administracyjną** w wysokości do 10 mln euro lub 2 proc. rocznego światowego obrotu z poprzedniego roku obrotowego.

1. Warto więc opracować i wdrożyć **procedurę postępowania na wypadek wystąpienia incydentu bezpieczeństwa.** W procedurze powinny znaleźć się: cel jej wdrożenia, zakres stosowania, opis etapów zarządzania incydentem od jego wykrycia do zamknięcia oraz przypisana pracownikom odpowiedzialność i role związane z reagowaniem na incydenty.
2. Procedura może także stanowić element polityki bezpieczeństwa. Dobrze jest zawrzeć w procedurze katalog najczęstszych zagrożeń i incydentów, które mogą prowadzić do naruszenia bezpieczeństwa danych osobowych oraz określić modelowy sposób zachowania pracowników i obowiązek informowania o domniemanych incydentach lub podejrzanych wydarzeniach wyznaczonych osób.

Obowiązek zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu

Oprócz zawiadomienia osoby, której dane osobowe zostały naruszone, konieczne jest również zgłoszenie do organu nadzorczego – bez zbędnej zwłoki lub w miarę możliwości w ciągu 72 godzin od stwierdzenia naruszenia. Jeśli ten termin zostanie przekroczony należy dodatkowo dołączyć wyjaśnienie tego opóźnienia.

Administrator może być zwolniony z tego obowiązku, gdy istnieje małe prawdopodobieństwo, by naruszenie ochrony danych osobowych skutkowało ryzkiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie musi zawierać następujące informacje:

- charakter naruszenia,
- dane Inspektora Ochrony Danych,
- konsekwencje naruszenia,

- środki podjęte w celu zaradzenia naruszeniu ochrony danych.

Certyfikacja w RODO

Cel wprowadzenia certyfikacji oddaje bardzo dokładnie motyw 100 preambuły do RODO. Wskazuje on, iż „aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi".

Warto zwrócić tu uwagę, że posiadanie certyfikatu nie jest obowiązkowe - zgodnie z RODO: „certyfikacja jest dobrowolna, a proces jej uzyskania musi być przejrzysty". Zatem to od decyzji administratora danych czy podmiotu przetwarzającego będzie zależało, czy wystąpi o certyfikat. Co ważne, certyfikat będzie udzielany na maksymalny okres 3 lat a jego przedłużenie będzie możliwe, o ile nadal spełnione będą stosowne wymogi (art. 42 ust. 7 RODO).

Warunki i tryb dokonywania certyfikacji

Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, zwanej dalej „certyfikacją", dokonuje Prezes Urzędu lub podmiot certyfikujący, na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek. Z kolei mając na względzie odciążenie polskiego organu nadzoru od spoczywających na nim licznych obowiązków, zdecydowano, aby kompetencję do akredytacji podmiotów certyfikujących przyznać Polskiemu Centrum Akredytacji (art. 12 ust. 1 uodo). Prezes Urzędu udostępnia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej kryteria certyfikacji.

Wniosek o certyfikację zawiera co najmniej:
1) nazwę podmiotu ubiegającego się o certyfikację albo jego imię i nazwisko oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;
2) informacje potwierdzające spełnianie kryteriów certyfikacji;
3) wskazanie zakresu wnioskowanej certyfikacji.

Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów certyfikacji albo ich kopie oraz w przypadku certyfikacji dokonywanej przez Prezesa Urzędu, dowód wniesienia opłaty, o której mowa w art. 26 (wysokość tej opłaty odpowiada przewidywanym kosztom poniesionym z tytułu wykonywania czynności związanych z certyfikacją). Prezes Urzędu, ustalając wysokość opłaty, bierze pod uwagę zakres certyfikacji, przewidywany przebieg i długość postępowania certyfikującego oraz koszt pracy pracownika wykonującego czynności związane z certyfikacją. Maksymalna wysokość opłaty nie może przekroczyć czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o certyfikację, ogłaszanego przez Prezesa GUS na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r. poz. 1383, ze zm.). Prezes Urzędu na swojej stronie podmiotowej w BIP podaje wysokość opłaty, którą podmiot, o którym mowa powyżej, obowiązany jest ponieść z tytułu czynności związanych z certyfikacją. Opłata ta stanowi dochód budżetu państwa.

Wniosek o certyfikację składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym. Przy czym wniosek składany do Prezesa Urzędu w postaci elektronicznej musi być opatrzony kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.

Prezes Urzędu albo podmiot certyfikujący rozpatruje wniosek o certyfikację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku, po zbadaniu spełniania kryteriów certyfikacji, zawiadamia wnioskodawcę o dokonaniu albo odmowie dokonania certyfikacji.

Wniosek złożony do Prezesa Urzędu, niezawierający informacji, o których mowa w pkt 1, pozostawia się bez rozpoznania. Jeżeli wniosek nie zawiera informacji, o których mowa w pkt 2 lub 3, lub nie spełnia wymagań, o których mowa w art. 17 ust. 2 lub 3 uodo, Prezes Urzędu wzywa wnioskodawcę do ich uzupełnienia wraz z pouczeniem, że ich nieuzupełnienie w terminie 7 dni od dnia doręczenia wezwania spowoduje pozostawienie wniosku bez rozpoznania.

W przypadku stwierdzenia, że podmiot ubiegający się o certyfikację nie spełnia kryteriów certyfikacji, Prezes Urzędu albo podmiot certyfikujący odmawia jej dokonania. Odmowa dokonania certyfikacji przez Prezesa Urzędu następuje w drodze decyzji.

Dokumentem potwierdzającym certyfikację jest certyfikat, który zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) numer lub oznaczenie certyfikatu;
4) zakres, w tym okres, na jaki została dokonana certyfikacja;
5) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

Prezes Urzędu albo podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu udzielono certyfikacji, nie spełnia lub przestał spełniać kryteria certyfikacji. Cofnięcie certyfikacji przez Prezesa Urzędu następuje również w drodze decyzji.

Prezes Urzędu prowadzi publicznie dostępny wykaz podmiotów, którym udzielono certyfikacji, oraz podmiotów, któremu cofnięto certyfikację. Prezes Urzędu udostępnia wykaz na swojej stronie podmiotowej w Biuletynie Informacji Publicznej i dokonuje jego aktualizacji.

Prezes Urzędu w terminie 3 miesięcy przed certyfikacją, a także po dokonaniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających, mających na celu ustalenie czy podmioty, które zostały certyfikowane spełniają kryteria. Prezes Urzędu zawiadamia podmiot, o których mowa powyżej, o zamiarze przeprowadzenia tego rodzaju czynności sprawdzających. Czynności te przeprowadza się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia podmiotowi zawiadomienia o zamiarze ich przeprowadzenia. Jeżeli czynności sprawdzające nie zostaną przeprowadzone w terminie 30 dni od dnia doręczenia zawiadomienia, ich przeprowadzenie wymaga ponownego zawiadomienia.

Czynności sprawdzające przeprowadza się na podstawie imiennego upoważnienia wydanego przez Prezesa Urzędu. Czynności sprawdzających dokonuje się w obecności administratora, podmiotu przetwarzającego, producenta lub podmiotu wprowadzającego usługę lub produkt na rynek lub osoby przez niego upoważnionej. Z czynności sprawdzających sporządza się protokół i przedstawia go administratorowi, podmiotowi przetwarzającemu, producentowi albo podmiotowi wprowadzającemu usługę lub produkt na rynek.

DANE OSOBOWE W TYPOWYCH DZIAŁACH FIRMY

Jednym z najważniejszych celów działalności organizacji jest rozwój. Umiejętność sprawnego, bezpiecznego i zgodnego z prawem przetwarzania