

Zmiany w ochronie danych osobowych

25 maja 2018 roku weszły w życie przepisy unijnego rozporządzenia ogólnego (RODO) oraz polskiej ustawy o ochronie danych osobowych. Potrzebne są jeszcze szczegółowe zmiany w około 150 innych ustawach. Nowe, obowiązujące już przepisy wprowadziły dość istotne zmiany w obowiązującym porządku prawnym.

Należy mieć jednocześnie na uwadze, że stosowanie regulacji już obowiązujących może wywołać dalsze potrzeby zmian przepisów prawnych. Wynika to z faktu, że dane osobowe są absolutnie wszędzie i w praktyce mogą się pojawić nowe wyzwania.

Podstawa prawna zmian

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119 z 4 maja 2016 r.);
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L 119 z 4 maja 2016 r.).
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

Cel zmian

RODO oraz uszczegóławiające przepisy krajowe mają zapewnić osobom fizycznym narzędzia ochrony swoich danych i wzmacniać ochronę osób fizycznych.

Przepisy skończyć mają z podpisywaniem w ciemno zgód na przetwarzanie danych osobowych przez osoby składające ofertę pracy, czy podpisujące umowę abonamentową, albo zapisujące się na newsletter.

Rozporządzenie domaga się "od wszystkich administratorów danych, by wszelkie informacje kierowane do osób, których dane dotyczą, były formułowane jasnym i prostym językiem, by były zwięzłe i zrozumiałe. Szczególnie istotne będzie to zaś wówczas, gdy informacje i komunikaty będą kierowane do dzieci, które muszą móc je bez trudu zrozumieć"¹.

Celem wprowadzenia nowej regulacji jest także ujednoczenie przepisów dotyczących ochrony danych osobowych na obszarze Unii Europejskiej. Dzięki temu wszystkie podmioty w krajach UE będą miały takie same warunki konkurencji.

Celem RODO jest także zwiększenie transparentności prowadzonej działalności zarówno przez podmioty gospodarcze, jak i administrację.

Do nowych regulacji (RODO) stosuje się zasadę bezpośredniego obowiązywania prawa wspólnotowego. Tym samym nie jest konieczny proces inkorporowania tj. włączania tych przepisów do przepisów krajowych.

Zasada bezpośredniego stosowania prawa wspólnotowego – zasada, która odnosi się do sposobu i zakresu stosowania prawa wspólnotowego przez organy państwa członkowskiego.

Zasada opiera się na następujących założeniach:

- prawo wspólnotowe jest stosowane bezpośrednio w każdym z krajów członkowskich,*
- prawo wspólnotowe ma bezpośrednią skuteczność wobec: instytucji, podmiotów prawa i obywateli każdego z państw członkowskich,*
- nawet jeśli norma prawna wprowadzona do systemu prawa wspólnotowego nie została implementowana do systemu prawa krajowego, to ma ona swoje zastosowanie na terenie całej Wspólnoty, także tego kraju².*

Pomimo tego, że nie jest konieczny proces inkorporowania prawa, to stosowanie RODO wymaga zmian w przepisach szczegółowych. W Polsce RODO wymaga dokonania licznych zmian w około 150 ustawach zapewniających dostosowanie krajowego porządku prawnego do nowych norm prawnych.

¹<http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html>,
online: 02.02.2018 r.

²https://pl.wikipedia.org/wiki/Zasada_bezpo%C5%9Bredniego_stosowania_prawa_wsp%C3%B3lnotowego,
online: 02.02.2018 r.

Podstawowe definicje według nowego prawa

- **Dane osobowe** - dane, które oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
- **Możliwa do zidentyfikowania osoba fizyczna** - 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;
- **Dane genetyczne** - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- **Dane biometryczne** - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
- **Przetwarzanie danych osobowych** - 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;
- **Szczególne kategorie danych osobowych** - pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;

- **Naruszenie ochrony danych osobowych** - 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.

Zasady przetwarzania danych osobowych

RODO przewiduje następujące „Zasady dotyczące przetwarzania danych osobowych”:

- **zasada zgodności z prawem, rzetelności i przejrzystości** - dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- **zasada ograniczenia celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- **zasada minimalizacji danych** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- **zasada prawidłowości** – dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- **zasada ograniczenia przechowywania** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
- **zasada integralności i poufności** - dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasadnicze zmiany w ochronie danych osobowych

Rozporządzenie to największa zmiana w podejściu do ochrony danych osobowych od dwudziestu lat. RODO wprowadza dużo nowości. Poniżej charakterystyka najistotniejszych zmian.

1. Nowe i rozszerzone prawa obywateli

Przepisami RODO wprowadzone zostaje: „prawo do bycia zapomnianym”, skierowane do obywateli, którzy życzą sobie, by ich dane osobowe zostały usunięte, uprawnienie do żądania przeniesienia danych oraz wzmocnione prawo dostępu i wglądu obywatela w jego dane.

Główny Inspektor Danych Osobowych tłumaczy, że z prawa do bycia zapomnianym skorzystamy w sytuacji, w której chcemy, by nasze dane nie były przetwarzane, a na przykład określona instytucja czy firma nie mają podstawy do takiego przetwarzania. Jak zauważa Komisja Europejska "narzędzie to ma chronić prywatność osób, niekoniecznie umożliwiać usuwanie informacji z przeszłości albo ograniczanie wolności prasy"³.

Osoby, których dane dotyczą, będą także miały rozszerzone prawo sprzeciwu wobec przetwarzania ich danych, w tym prawo do zakazania marketingu bezpośredniego z wykorzystaniem danych osobowych, co ma niebagatelne znaczenie dla firm bazujących na analizie danych.

2. Zgody

Przepisami RODO zostają wprowadzone nowe lub uzupełnione zasady uzyskiwania ważnych i weryfikowalnych zgód na przetwarzanie danych osobowych od osób, których dane dotyczą.

Nowością jest określenie po raz pierwszy zasad przetwarzania danych biometrycznych (takich jak wizerunek twarzy czy odciski palców) w zatrudnianiu, w sektorze bankowym i ubezpieczeniowym. Dane takie będą mogły zostać pozyskane przez bank oraz ubezpieczycieli celem weryfikacji tożsamości klientów. W przypadku zatrudnienia, przetwarzanie przez pracodawcę danych biometrycznych obejmować ma tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę⁴.

3. Rozbudowanie obowiązku informacyjnego

Przepisy RODO wskazują liczne informacje, które muszą być uwzględnione w komunikacji sposobu przetwarzania danych osobowych kierowanej do osób, których dane dotyczą.

³ <https://www.forbes.pl/biznes/zmiany-przepisow-o-ochronie-danych-giodo-komentuje/b1r458t>,
online: 02.02.2018 r.

⁴ <http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html>,
online: 02.02.2018 r.

4. Ograniczenia profilowania

Profilowanie, czyli zbieranie informacji o osobach oglądających oferty w internecie, czy szukających tradycyjnie jakiegoś towaru czy usługi, nie będzie zakazane. Jednak osoby profilowane będą musiały zostać poinformowane nie tylko o tym, że są obiektem zainteresowania algorytmów marketingowych, ale również o konsekwencjach z tego wynikających. Wprowadzony został obowiązek uzyskania zgody na profilowanie przed rozpoczęciem zbierania danych, surowy obowiązek informowania o profilowaniu oraz konieczność akceptacji braku zgody na profilowanie.

5. Bezpośrednia odpowiedzialność przetwarzającego dane

Organizacje przetwarzające dane osobowe pochodzące z innych firm, w trakcie świadczenia usług na ich rzecz (jak na przykład firmy dostarczające rozwiązania w chmurze czy firmy hostingowe), ponoszą bezpośrednią odpowiedzialność za złamanie zapisów RODO, włączając w to ryzyko otrzymania kary finansowej. Co więcej, wymagane są bardziej restrykcyjne niż wcześniej obowiązki w zakresie tworzenia umów o przetwarzaniu.

6. Obowiązkowa inwentaryzacja danych i wymagania związane z dokumentacją

Kontrolujący i przetwarzający dane są zobowiązani od przygotowania i utrzymania wszechstronnych rejestrów dotyczących przetwarzanych danych, uwzględniających m.in.: powody przetwarzania danych, kategorie podmiotów danych i danych osobowych, adresatów danych, rejestry międzynarodowych transferów danych, rejestry naruszeń i incydentów, rozwój i utrzymanie zasad ochrony prywatności dla każdej linii produktowej, przechowywanie potwierdzonych zgód na przetwarzanie danych itd.

7. Ocena wpływu ochrony danych

Wykonanie takiej analizy jest obowiązkowe przed podjęciem działań „wysokiego ryzyka”, takich jak na przykład profilowanie na dużą skalę, czy wykorzystanie danych szczególnych kategorii (takich jak dane dotyczące zdrowia).

8. Zgłaszanie naruszeń

Obowiązkiem administratorów danych jest zgłaszanie w ciągu 72 godzin od wykrycia do właściwego organu nadzoru przypadków naruszeń, które mogą skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone. Może także wystąpić konieczność zawiadomienia konkretnej osoby, bez zbędnej zwłoki, o przypadku wystąpienia dużego ryzyka naruszenia jej praw lub swobód.

9. Wyznaczenie Inspektora Ochrony Danych Osobowych

Nowa regulacja przewiduje wprowadzenie do systemu ochrony danych osobowych nowego podmiotu tj. Inspektora Ochrony Danych (IOD) w miejsce funkcjonującego wcześniej

Administradora Bezpieczeństwa Informacji (ABI). Powołanie IOD jest obowiązkowe w podmiotach publicznych oraz organizacjach, których główna działalność wiąże się z przetwarzaniem danych osobowych w dużej skali. Inspektor musi dysponować wiedzą ekspercką w zakresie ochrony danych osobowych.

10. Rejestr danych

Rozporządzenie znosi obowiązek zgłaszania rejestru danych do organów ochrony danych o przetwarzaniu danych (w Polsce: Główny Inspektor Ochrony Danych Osobowych). Do tej instytucji muszą być zgłaszane przypadki naruszenia danych osobowych.

Kto jest zobowiązany do ochrony danych osobowych

Nowe przepisy obejmują wszystkie podmioty, które gromadzą i wykorzystują dane dotyczące osób fizycznych, w tym firmy, organy administracji publicznej, organizacje pozarządowe. W praktyce są to m.in. korporacje, małe firmy, urzędy gmin, sklepy internetowe, szkoły, ośrodki pomocy społecznej czy domy kultury, stowarzyszenia i fundacje.

Wprowadzanie zmian

Administratorzy danych osobowych - firmy czy organizacje pozarządowe - muszą dostosować bazy danych do przepisów RODO, o ile jeszcze tego obowiązku nie zrealizowały. Między innymi muszą sprawdzić dotychczasowe rozwiązania z zakresu ochrony danych osobowych i w wielu przypadkach je zmodyfikować.

Konieczne jest przeszukanie wszystkich zasobów teleinformatycznych, co będzie nie lada wyzwaniem, gdyż dane mogą być nie tylko w bazach, ale również w plikach tekstowych zlokalizowanych na komputerach użytkowników, plikach ze skanami dokumentów itp.⁵

Niestosowanie się do nowych zasad przetwarzania danych osobowych może m.in. skutkować odpowiedzialnością finansową – administracyjnymi karami pieniężnymi nawet do 20 milionów euro lub 4 proc. całkowitego rocznego światowego obrotu.

Niezależnie od tego osoba, której prawa zostały naruszone, może też dochodzić swoich roszczeń przed sądem cywilnym.

Z drugiej strony, wejście w życie nowych przepisów wymusza ułatwienia, oszczędności i rozwój innowacyjności.

⁵ Tamże.

Gdzie szukać wsparcia, pomocy we wdrażaniu przepisów RODO?

Instytucje

- Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, Infolinia: 606-950-000 czynna w dni robocze od: 10.00 – 13.00

Portale

- Urząd Ochrony Danych Osobowych: www.uodo.gov.pl

Bezpłatne poradniki

- [K. Szymielewicz, „Nowa filozofia w ochronie danych osobowych: od oceny ryzyka do spójnej strategii w organizacji”, Fundacja Panoptykon, Warszawa 2017.](#)
- [P. Litwiński, "Przewodnik po RODO dla małych i średnich przedsiębiorców", Ministerstwo Przedsiębiorczości i Technologii, Warszawa 2018.](#)

Opracowała: Iwona Raszeja-Ossowska

Tekst ma charakter informacyjno - edukacyjny.

Nie jest opinią prawną.

Źródła:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119 z 4 maja 2016 r.),
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L 119 z 4 maja 2016 r.).
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).
4. Szymielewicz K., „Nowa filozofia w ochronie danych osobowych: od oceny ryzyka do spójnej strategii w organizacji”, Fundacja Panoptykon, Warszawa 2017.
5. Litwiński P., "Przewodnik po RODO dla małych i średnich przedsiębiorców", Ministerstwo Przedsiębiorczości i Technologii, Warszawa 2018.
6. <https://blog-daneosobowe.pl/czym-sa-dane-osbowe-wg-rod0/>, online: 02.02.2018 r.
7. <http://www.lex.pl/czytaj/-/artykul/rodo-nowe-prawo-o-ochronie-danych-juz-obowiazuje>, online: 04.08.2018 r.

8. <http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html>, online: 02.02.2018 r.
9. <http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL>, online: 02.02.2018 r.
10. <https://www.forbes.pl/biznes/zmiany-przepisow-o-ochronie-danych-giodo-komentuje/b1r458t>, online: 02.02.2018 r.
11. https://pl.wikipedia.org/wiki/Zasada_bezpo%C5%9Bredniego_stosowania_prawa_w_sp%C3%B3lnotowego, online: 02.02.2018 r.