Przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych (RODO)

Opracowanie:

Kancelaria J. Bójko i Wspólnicy
r. pr. Justyna Bójko
apl. adw. Kinga Rochalska

JBW KANCELARIA

Wstęp

Potrzeba reformy unijnego systemu ochrony danych osobowych sygnalizowana była w Unii Europejskiej już od dłuższego czasu. Po kilku latach prac analitycznych i uzgodnień pomiędzy organami unijnymi, 27 kwietnia 2016 r. uchwalono rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO"), które dnia 25 maja 2018 r. zastąpi zarówno obowiązującą Dyrektywę 95/46/WE, jak i regulacje krajowe, w tym m.in. polską ustawę o ochronie danych osobowych. Po wejściu w życie RODO ochrona danych osobowych będzie w sposób jednolity regulowana na szczeblu unijnym, co zapewnić ma jednolitość przepisów w skali Unii Europejskiej.

RODO wprowadza wiele fundamentalnych zmian w zasadach przetwarzania danych osobowych. Ponadto, po wejściu w życie RODO wzrośnie ryzyko związane z przetwarzaniem danych osobowych, co powoduje, iż znaczenie zgodnego z prawem zabezpieczenia danych osobowych oraz odpowiedniego reagowania na incydenty nabiera kluczowego znaczenia. Implementacja zmian w każdej organizacji wymaga przeprowadzenia właściwego audytu prawnego oraz technicznego w celu identyfikacji istniejących niezgodności i luk w zakresie ochrony danych osobowych, analizy wyników audytu pod kątem zgodności z RODO, a wreszcie – odpowiedniego wdrożenia wymagań stawianych przez Rozporządzenie. W zależności od wielkości organizacji oraz procedur w niej obowiązujących, może okazać się to procesem wyjątkowo czasochłonnym, co rodzi potrzebę niezwłocznego przystąpienia do działania tak, aby zdążyć przed datą wejścia w życie RODO – 25 maja 2018 r.

Zachęcamy Państwa do kontaktu celem omówienia potrzeb oraz przygotowania i przeprowadzenia tego złożonego procesu zarówno pod kątem prawnym, jak również – przy współpracy naszych partnerów – pod katem technicznym.

Z poważaniem,
Justyna Bójko

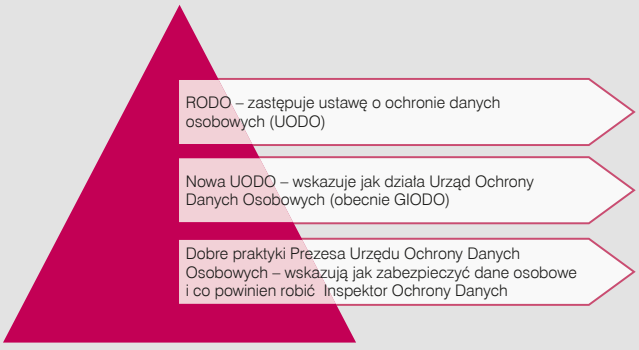
SYSTEM AKTÓW PRAWNYCH

RODO zwane także „GDPR" lub „Ogólnym Rozporządzeniem o Ochronie Danych" to 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.

RODO – zastępuje ustawę o ochronie danych osobowych (UODO). Dokument ma pierwszeństwo nad UODO

NOWA UODO – dokument mniej szczegółowy niż RODO. Będzie wskazywał m.in. jak działa Urząd Ochrony Danych Osobowych (obecnie GIODO)

Dobre praktyki Prezesa Urzędu Ochrony Danych Osobowych – będą wskazywać m.in. sposób zabezpieczenia danych osobowych oraz zakres zadań Inspektora Ochrony Danych



Kluczowe elementy przetwarzania danych

RODO ma zastosowanie do przetwarzania danych osobowych (tj. wykonywania jakiekolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie), niezależnie czy jest to dokonywane w sposób zautomatyzowany, czy też nie. Ponadto, RODO należy stosować niezależnie od tego czy dane będą przetwarzane w formie papierowej, czy też w formie elektronicznej. **RODO ma zastosowanie jedynie do osób fizycznych**. Dane osób prawnych nie są objęte zakresem stosowania Rozporządzenia. RODO w stosunku do osób fizycznych należy stosować niezależnie od ich obywatelstwa czy miejsca zamieszkania, ale w związku z przetwarzaniem ich danych osobowych na terenie Unii Europejskiej.

Dane podlegające RODO

Zgodnie z definicją danych osobowych wskazaną w RODO, Rozporządzeniu podlegają **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** (osobie, której dane dotyczą). Przepis ten wskazuje, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatorów takich jak:

1) imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy;
2) jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane niepodlegające RODO

Zgodnie z RODO informacjami, do których nie będą miały zastosowania przepisy Rozporządzenia są:

1) informacje anonimowe – czyli informacje, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną;
2) dane osobowe zanonimizowane w taki sposób, że osób, których dotyczą w ogóle nie można zidentyfikować lub już nie można zidentyfikować;
3) dane osób zmarłych.

Adresaci RODO

- RODO dotyczyć będzie praktycznie wszystkich, ponieważ nie ma już w zasadzie organizacji, które nie gromadzą w jakikolwiek sposób danych osób fizycznych!

- Przepisy RODO obejmują zarówno przedsiębiorców i osoby fizyczne będące administratorami danych osobowych, jak również podmioty przetwarzające dane osobowe osób fizycznych w imieniu administratora, którzy prowadzą działalność na terenie Unii Europejskiej (niezależnie gdzie przetwarzają dane osobowe) tj. **m.in. sklepy internetowe, biura rachunkowe, hotele, spółdzielnie, stowarzyszenia, banki, serwisy społecznościowe**.

- Przepisy RODO obejmują także organy i podmioty publiczne, a także podmioty niepubliczne realizujące zadania publiczne będące administratorami danych osobowych, jak również podmioty przetwarzające dane osobowe osób fizycznych w imieniu administratora w Unii Europejskiej (niezależnie od tego, czy przetwarzanie odbywa się na terenie Unii Europejskiej) tj. **m.in. policja, wojsko, administratorzy infrastruktury krytycznej, placówki edukacyjne, placówki medyczne, ZUS, jednostki samorządu terytorialnego**.

- RODO obejmuje również podmioty z państw trzecich, jeżeli będą przetwarzać dane osobowe osób fizycznych przebywających na terenie Unii Europejskiej, w związku z oferowaniem towarów lub usług takim osobom w Unii Europejskiej (nawet za darmo) oraz monitorowaniem ich zachowania (na terenie Unii Europejskiej).

- RODO obejmuje przetwarzanie danych osobowych osób fizycznych przez administratora niemającego jednostki organizacyjnej w Unii Europejskiej, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego tj. **placówki dyplomatyczne**.

Porównanie istotnych definicji i instytucji

DO 24 MAJA 2018 r.	OD 25 MAJA 2018 r.
ZASIĘG TERYTORIALNY	
Przepisy dotyczące ochrony danych osobowych stosuje się wobec podmiotów, które mają siedzibę w Polsce albo w państwie poza Europejskim Obszarem Gospodarczym (jedynie, gdy przetwarzają dane przy wykorzystaniu środków technicznych na terytorium Polski).	Przepisy dotyczące ochrony danych osobowych stosuje się niezależnie od miejsca przetwarzania danych, o ile realizuje je podmiot przetwarzający dane w Unii Europejskiej. Ponadto, przepisy RODO stosuje się również, gdy przetwarzane są dane osób przebywających w Unii Europejskiej nawet, jeśli dane przetwarzane są przez podmioty spoza Unii Europejskiej, w sytuacji gdy dochodzi do oferowania usług lub towarów lub monitorowania ich zachowania, do którego dochodzi na terenie Unii Europejskiej.
DEFINICJA DANYCH OSOBOWYCH	
Zgodnie z definicją zawartą w UODO za „dane osobowe" uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiające określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.	W rozumieniu RODO „dane osobowe" obejmują informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (bezpośrednio lub pośrednio), na podstawie m.in. identyfikatora takiego jak: imię i nazwisko, dane o lokalizacji, identyfikator internetowy lub jeden lub kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Definicja danych osobowych w RODO została rozbudowana w porównaniu z definicją zawartą w UODO. W RODO wskazano wprost, że dane o lokalizacji, identyfikator internetowy i informacja genetyczna to czynniki, które należy traktować, jako umożliwiające identyfikację.
PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH	
Jedną z podstaw przetwarzania danych osobowych przewidzianą przez UODO jest sytuacja, w której przetwarzanie danych osobowych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych, czy też dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.	Zgodnie z RODO przetwarzanie danych osobowych jest dopuszczalne m.in. jeżeli jest ono niezbędne dla celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa podstawowe i wolności podmiotu danych, wymagające ochrony danych osobowych, w szczególności gdy podmiot danych jest dzieckiem (co do zasady osoba, która nie ukończyła 16 lat).
INFORMOWANIE PODMIOTU DANYCH OSOBOWYCH	
Przepisy UODO nakazują m.in. podać cel przetwarzania danych, kategorie odbiorców oraz zidentyfikować administratora danych osobowych.	Przepisy RODO wymagają, by podać nie tylko cel przetwarzania danych, ale również m.in. podstawę przetwarzania danych, informację o prawie wniesienia skargi do organu nadzorczego oraz informację o okresie przez który dane będą przechowywane.
ZABEZPIECZENIE DANYCH OSOBOWYCH	
Kluczowe znaczenie w zabezpieczeniu danych osobowych w rozumieniu UODO ma „Polityka Bezpieczeństwa" oraz „Instrukcja Zarzadzania Systemem Informatycznym", o treści precyzyjnie wskazanej w aktach wykonawczych do UODO. Przygotowanie i wdrożenie takiej dokumentacji jest obowiązkowe dla każdego administratora danych osobowych.	Regulacje RODO przypisują ważną rolę kodeksom dobrych praktyk (kodeksy postepowania) podlegającym procesowi monitorowania przez organ nadzorczy oraz certyfikacji stanowiącej potwierdzenie spełnienia wymogów prawa dotyczących ochrony danych osobowych. Środki te mają towarzyszyć obowiązkowej i odpowiedniej dokumentacji ochrony danych.

Kluczowe zmiany wprowadzane przez RODO

RODO wprowadzi wiele innowacyjnych zmian w podejściu do ochrony danych osobowych, które dotychczas nie były regulowane przepisami, między innymi:

Bezpośrednia odpowiedzialność przetwarzającego dane osobowe

Podmioty przetwarzające dane osobowe pochodzące z innych firm, w trakcie świadczenia usług na ich rzecz, będą ponosić bezpośrednią odpowiedzialność za naruszenie przepisów RODO, włączając w to ryzyko otrzymania kary finansowej.

Zgłaszanie naruszeń

Obowiązkiem administratorów danych będzie 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. Ponadto może zajść konieczność zawiadomienia konkretnej osoby, bez zbędnej zwłoki, o przypadku wystąpienia dużego ryzyka naruszenia jej praw lub swobód.

Wyznaczenie Inspektora Danych Osobowych

RODO wprowadza pojęcie tzw. Inspektora Ochrony Danych (IOD, ang. Data Protection Officer – DPO). Przepisy RODO wskazują na sytuacje, w których obowiązkowym jest powołanie DPO. Powołanie DPO będzie konieczne w przypadku organów publicznych, podmiotów których działalność polegać będzie na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, tudzież danych osobowych dotyczących wyroków skazujących i naruszeń prawa, jak również podmiotów, których główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób.

Rejestr czynności przetwarzania danych osobowych

Przedsiębiorcy będą musieli prowadzić rejestr czynności przetwarzania danych osobowych, który będzie obejmował m.in. takie informacje jak cele przetwarzania czy też kategorie przetwarzanych danych osobowych. RODO przewiduje jednak pewne wyjątki od tej zasady, które mają dotyczyć przedsiębiorstw zatrudniających do 250 pracowników.

Ocena wpływu ochrony danych

Zgodnie z RODO przed podjęciem działań „wysokiego ryzyka" takich jak np. profilowanie na dużą skalę czy wykorzystanie danych szczególnych (m.in. danych dotyczących zdrowia), właściwe podmioty będą zobowiązane do przeprowadzenia analizy oceny wpływu ochrony danych.

Surowe kary

RODO wprowadza surowe kary administracyjne za naruszenie przepisów dotyczących ochrony danych osobowych. Kary będą mogły sięgać kwoty 20 mln Euro (lub w przypadku przedsiębiorstwa do 4% światowego obrotu za poprzedni rok obrotowy), a w przypadku spraw mniejszej wagi – do 10 mln Euro (lub odpowiednio do 2% obrotu). Każdy przypadek nałożenia kary będzie rozpatrywany indywidualnie przez organ nadzoru, który będzie brał pod uwagę w szczególności: skalę naruszenia, umyślność, podjęte działania zapobiegawcze, a także wcześniejsze przypadki naruszeń przez przedsiębiorcę.

KARA	NARUSZENIE PRZEPISU
20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa	• Naruszenie zasad dotyczących przetwarzania danych osobowych (art. 5 RODO) • Naruszenie warunków wyrażenia zgody na przetwarzanie danych (art. 7 RODO) • Naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą (art. 15 RODO) • Naruszenie wykonania prawa do sprostowania i usuwania danych (art. 16 RODO)
10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa	• Naruszenie zasad ochrony danych osobowych w fazie projektowania (privacy by design) oraz domyślna ochrona danych (privacy by default) (art. 25 RODO) • Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego (art. 29 RODO) • Rejestrowanie czynności przetwarzania (art. 30 RODO) • Współpraca z organem nadzorczym (art. 31 RODO) • Bezpieczeństwo przetwarzania (art. 32 RODO)

Reagowanie na incydenty

Po wystąpieniu incydentu związanego z naruszeniem przepisów dotyczących ochrony danych osobowych niezbędne są właściwe działania, które mogą zmniejszyć odpowiedzialność w zakresie naruszenia RODO.

Thales Polska Sp. z o. o., po wystąpieniu incydentu bezpieczeństwa związanego z danymi osobowymi, proponuje podjęcie poniższych działań (niezbędne minimum):

- Identyfikacja incydentu, klasyfikacja, gromadzenie informacji o incydencie
- Ustalenie strategii odpowiedzi na incydent
- Zebranie i aktywowanie zespołu kryzysowego
- Ograniczenie wpływu (zasięgu) incydentu na biznes
- Zabezpieczenie materiału dowodowego oraz szczegółowe dokumentowanie działań
- Postępowanie naprawcze: odzyskiwanie danych i przywracanie sprawności systemów
- Raportowanie do najwyższego kierownictwa
- Informacja do pracowników firmy
- Przygotowanie komunikacji PR, współpraca z mediami
- Raportowanie do właściwych organów: policja, prokuratura, ABW, GIODO, NCCyber, UKE, RCB, itd.
- Przygotowanie raportu końcowego i wyciąganie wniosków

* Działania zgodne z ISO 27001:2013 oraz dobrymi praktykami rynkowymi (US-CERT, ABW CERT. GOV.PL oraz NCCyber, National Cyber Security Centre GCHQ)

Grafika przygotowana przez: Thales Polska Sp. z o.o.

Zapraszamy do kontaktu z Kancelarią J. Bójko i Wspólnicy

Więcej informacji:

Kancelaria J. Bójko i Wspólnicy

ul. Targ Rybny 11a/4
80-838 Gdańsk

r.pr. Justyna Bójko

e.mail: j.bojko@lsw.com.pl

apl. adw. Kinga Rochalska

e.mail: k.rochalska@lsw.com.pl

tel.: + (48) 530 178 221