Rödl & Partner

25 LAT w Polsce 1992-2017

Zaangażowani globalnie

Technologia Informacyjna i Prawo w służbie ochrony danych – #RODO2018
Wdrożenie przepisów RODO w praktyce – aspekty prawne

Jarosław Kamiński I Warszawa I 06.04.2017

Agenda

1 **Rozporządzenie UE o ochronie danych osobowych (RODO)**

1.1. Stosowanie RODO do polskich przedsiębiorców

1.2. Przegląd podstawowych, nowych instytucji oraz zmian

2 **Skutki RODO dla polskich przedsiębiorców**

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Skróty

GIODO	**G**eneralny **I**nspektor **O**chrony **D**anych **O**sobowych
ADO	**A**dministrator **D**anych **O**sobowych
ABI	**A**dministrator **B**ezpieczeństwa **I**nformacji
IOD	**I**nspektor **O**chrony **D**anych
UODO	**U**stawa o **O**chronie **D**anych **O**sobowych
RODO	**R**ozporządzenie UE o **O**chronie **D**anych **O**sobowych

Agenda

1 **Rozporządzenie UE o ochronie danych osobowych (RODO)**

1.1. Stosowanie RODO do polskich przedsiębiorców

1.2. Przegląd podstawowych, nowych instytucji oraz zmian

2 **Skutki RODO dla polskich przedsiębiorców**

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Rozporządzenie UE o ochronie danych osobowych

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)

RODO ma zastosowanie od dnia 25 maja 2018 r.

UWAGA

Bezpośrednie stosowanie RODO do państw członkowskich UE!

RODO – zakres terytorialny

Obowiązek przetwarzania danych osobowych zgodnie z przepisami RODO spoczywa na:

1) administratorach danych **mający siedzibę na terenie UE**, niezależnie od tego, czy przetwarzanie ma miejsce w UE

2) administratorach danych **nie mających siedziby na terenie UE**, którzy przetwarzają dane osób przebywających w UE, jeżeli:
   - ma to związek z **oferowaniem produktów lub usług osobom przebywającym w UE**, bez względu na fakt odpłatności lub jej braku
   - **monitorowane jest zachowanie osób przebywających w UE**, o ile ich zachowanie ma miejsce na terenie UE

Przykład

przeglądarki internetowe, np. Google

3) administratorach danych nie mających siedziby na terenie UE, ale posiadający jednostkę organizacyjną w miejscu, gdzie na podstawie prawa międzynarodowego ma zastosowanie prawo kraju członkowskiego UE.

Agenda

1 **Rozporządzenie UE o ochronie danych osobowych (RODO)**

1.1. Stosowanie RODO do polskich przedsiębiorców

1.2. Przegląd podstawowych, nowych instytucji oraz zmian

2 **Skutki RODO dla polskich przedsiębiorców**

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Nowe instytucje oraz zmiany

NOWOŚCI

- nowe podejście do ochrony danych osobowych (risk-based approach)
- ułatwienia dla grup przedsiębiorstw
- uregulowanie zasad profilowania
- **wprowadzenie kar administracyjnych**
- raportowanie do GIODO o własnych naruszeniach
- przetwarzanie danych dziecka tylko za zgodą opiekuna

ZMIANY

- rozszerzona formuła zgody na przetwarzanie danych
- rozszerzony zakres obowiązku informacyjnego
- rejestr czynności przetwarzania
- zmiana statusu ABI > IOD
- zmieniona definicja tzw. danych wrażliwych
- zwiększenie uprawnień osób, których dane dotyczą

Nowe podejście do ochrony danych osobowych (*risk-based approach*)

- obowiązek administratora danych **samooceny** pod kątem oszacowania skutków przetwarzania dla ochrony danych i ewentualnego ryzyka
  - weryfikacja przetwarzanych danych
  - ocena zagrożeń związanych z przetwarzaniem konkretnych danych osobowych
  - planowane środki, zabezpieczenia i mechanizmy w celu zminimalizowania zagrożeń
- brak sztywnych regulacji dotyczących środków służących zapewnieniu bezpieczeństwa przetwarzania danych osobowych (np. dotyczących wymogów co do hasła)
- obowiązki administratora danych uzależnione będą od ustalonego ryzyka wynikającego z konkretnych operacji przetwarzania danych

Nowe podejście do ochrony danych osobowych (*risk-based approach*)

Ocena skutków dla ochrony danych (*data protection impact assessment*)

- przed rozpoczęciem przetwarzania
- obowiązkowa, gdy:
  - charakter, zakres, kontekst i cele danego rodzaju przetwarzania z **dużym prawdopodobieństwem** mogą powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**
  - decyzją organu nadzoru (np. GIODO) dany rodzaj operacji przetwarzania podlega obowiązkowej ocenie
- obowiązek **uprzednich konsultacji** z organem nadzoru (np. GIODO), jeżeli ocena wykaże, że przetwarzanie danych powodowałoby wysokie ryzyko

Agenda

2 **Skutki RODO dla polskich przedsiębiorców**

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Wyzwania prawne przed 25.05.2018

Przed 25. maja 2018 r.:

1) Analiza rodzajów przetwarzanych danych osobowych, stosowanych środków bezpieczeństwa, weryfikacja przesłanek i podstaw przetwarzania danych osobowych oraz ustalenie kategorii i zbiorów przetwarzanych danych osobowych

2) Weryfikacja zdolności dostawców usług (podmiotów, którym powierzone zostało przetwarzanie danych osobowych) do zapewnienia zgodności przetwarzania danych zgodnie z przepisami RODO

3) Weryfikacja konieczności lub zasadności powołania **Inspektora Ochrony Danych**

4) Analiza i weryfikacja **dokumentacji kadrowej i zasad procesu rekrutacji**

5) Audyt przetwarzania danych pod kątem RODO

Wyzwania prawne przed 25.05.2018, cd.

6) Weryfikacja stron internetowych pod kątem przetwarzania danych na gruncie RODO

7) Przeprowadzenie analizy stosowanego oprogramowania pod kątem bezpieczeństwa danych i nowych wymogów RODO oraz jego ewentualna zmiana (prawo do bycia zapomnianym, *privacy by default*, *privacy by design*)

8) Weryfikacja umów powierzenia przetwarzania danych osobowych pod kątem RODO

9) Weryfikacja stosowanych **klauzul informacyjnych** oraz opracowanie nowych klauzul

Wyzwania prawne przed 25.05.2018, cd.

10) Weryfikacja stosowanych **klauzul zgody** na przetwarzanie danych oraz opracowanie nowych klauzul na gruncie RODO

11) Wprowadzenie środków umożlwiających prawidłowe zgłaszanie naruszeń danych osobowych do GIODO **(w ciągu 72h od momentu naruszenia)**

12) Szkolenia dla pracowników w zakresie nowych zasad przetwarzania danych na gruncie RODO

13) **Opracowanie dokumentacji związanej z ochroną danych na gruncie RODO oraz systematyczna (np. raz na kwartał / pół roku) weryfikacja dokumentacji pod kątem nowych wytycznych i wskazówek organów nadzorczych i Grupy Roboczej Art. 29**

Agenda

2 Skutki RODO dla polskich przedsiębiorców

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Inspektor Ochrony Danych – następca ABI

RODO wprowadza nową funkcję **Inspektora Ochrony Danych** (art. 37 – 39 RODO)

Inspektor Ochrony Danych (IOD) w świetle przepisów RODO

Administrator i podmiot przetwarzający wyznaczają Inspektora Ochrony Danych, **zawsze** gdy:

1) **przetwarzania dokonują organ lub podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

2) **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**; lub

3) **główna działalność** administratora lub podmiotu przetwarzającego polega na **przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych**, o których mowa w art. 9 ust. 1 RODO („dane wrażliwe"), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

W **innych przypadkach** wyznaczenie IOD jest **dobrowolne**

UWAGA

Prawo państwa członkowskiego może przewidywać inne przypadki, w których wyznaczenie IOD będzie obligatoryjne

Inspektor Ochrony Danych (IOD)

- wymagane **kwalifikacje zawodowe**, a w szczególności **wiedza fachowa na temat prawa i praktyk** w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań IOD wynikających z RODO
- obowiązek **zachowania tajemnicy lub poufności**
- administrator danych lub podmiot przetwarzający **publikują** dane kontaktowe IOD i **zawiadamiają** o nich organ nadzorczy
- **zapewnienie kontaktu** IOD z osobami, których dane dotyczą
- IOD może być **członkiem personelu** administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie **umowy o świadczenie usług**

Inspektor Ochrony Danych (IOD)

- IOD ma być włączany we wszystkie sprawy dotyczące ochrony danych osobowych
- administrator lub podmiot przetwarzający mają zapewnić IOD **niezależność**, **niezbędne zasoby** (finansowe i personalne) do wykonywania zadań, dostęp do danych osobowych oraz zasoby niezbędne do utrzymania wiedzy fachowej
- grupa przedsiębiorców może wyznaczyć jednego IOD, **o ile można będzie łatwo nawiązać z nim kontakt**

Inspektor Ochrony Danych (IOD)

Inspektor ochrony danych ma następujące zadania:

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

Agenda

2 **Skutki RODO dla polskich przedsiębiorców**

2.1. Analiza i audyt dotychczasowych zasad przetwarzania danych

2.2. Funkcja Inspektora Ochrony Danych

2.3. Odpowiedzialność za naruszenie przepisów RODO

Odpowiedzialność za naruszenie przepisów RODO

UWAGA

państwa członkowskie **mają obowiązek przyjąć** przepisy określające **inne sankcje** za naruszenie RODO, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym oraz podjąć wszelkie środki niezbędne do ich wykonania

Odpowiedzialność cywilnoprawna

- każda osoba, która poniosła **szkodę majątkową lub niemajątkową** w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego **odszkodowanie za poniesioną szkodę**

- w przypadku przetwarzania danych przez więcej niż jednego administratora lub podmiotu przetwarzającego – **odpowiedzialność solidarna**

- podmiotowi, który zapłacił całe odszkodowanie przysługuje **prawo żądania** od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, **zwrotu części odszkodowania** odpowiadającej części szkody, za którą ponoszą odpowiedzialność

Odpowiedzialność administracyjnoprawna

- **administracyjne kary pieniężne nakładane przez organ nadzorczy**
  - niezależne od winy
  - nakładane obok lub zamiast uprawnień korekcyjnych organu nadzorczego, np. GIODO (ostrzeżeń, upomnień, nakazów, zakazów)
  - brak konieczności jakichkolwiek działań uprzednich ze strony organu nadzorczego
  - nakładanie kar pieniężnych powinno być **skuteczne, proporcjonalne i odstraszające**

Kary pieniężne - czynniki brane pod uwagę przy ich nakładaniu

Przy nakładaniu kar i określaniu ich wysokości organ bierze pod uwagę następujące okoliczności:

1) **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
2) **umyślny lub nieumyślny** charakter naruszenia
3) **działania podjęte przez administratora** lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą
4) **stopień odpowiedzialności administratora** lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32
5) wszelkie stosowne **wcześniejsze naruszenia** ze strony administratora lub podmiotu przetwarzającego
6) **stopień współpracy z organem** nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków

Kary pieniężne - czynniki brane pod uwagę przy ich nakładaniu

Przy nakładaniu kar i określaniu ich wysokości organ bierze pod uwagę następujące okoliczności:

7) **kategorie danych osobowych**, których dotyczyło naruszenie;
8) sposób, **w jaki organ nadzorczy dowiedział się o naruszeniu**, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
9) 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;
10) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz
11) **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.

Wysokość administracyjnych kar pieniężnych

Wysokość kary uzależniona jest od rodzaju naruszenia i wynosi

do **10 MLN EUR**, a w przypadku przedsiębiorstwa – w wysokości do **2 % jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota **wyższa**

- brak prawidłowego przetwarzania danych
- brak zastosowania odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzania
- niezawiadomienie odpowiednich organów o naruszeniu bezpieczeństwa
- niewyznaczenie Inspektora Ochrony Danych w przypadku, gdy było to obowiązkowe

do **20 MLN EUR**, a w przypadku przedsiębiorstwa – w wysokości do **4 % jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota **wyższa**

- brak podstawy do przetwarzania danych
- naruszenie praw lub wolności podmiotów danych
- przekazywanie danych do podmiotów poza EOG niezapewniającego odpowiedniego poziomu bezpieczeństwa
- nieprzestrzeganie nakazów lub zakazów nałożonych przez organ nadzorczy itp.

Państwa osoba do kontaktu

Jarosław Kamiński
Adwokat, Senior Associate

Rödl & Partner
ul. Sienna 73
00-833 Warszawa
Tel: +48 (22) 244 00 27
Fax: +48 (22) 696 28 01
E-mail: jaroslaw.kaminski@roedl.pro

„Tutaj liczy się każdy" – jak w wieży z ludzi, tak i w Rödl & Partner.

Wieże budowane z ludzi w niepowtarzalny sposób symbolizują kulturę firmy Rödl & Partner. Stanowią uosobienie naszej filozofii: poczucia więzi, równowagi, odwagi oraz ducha pracy zespołowej. Unaoczniają wzrost osiągnięty własnymi siłami, który ukształtował firmę Rödl & Partner. „Força, Equilibri, Valor i Seny" (siła, równowaga, odwaga i rozwaga) to katalońskie hasło wszystkich castellerów (budowniczych ludzkich wież), które niezwykle trafnie opisuje cenione przez nich wartości. To również nasze wartości. Dlatego firma Rödl & Partner w maju 2011 nawiązała współpracę z Castellers de Barcelona, przedstawicielami tej wieloletniej tradycji budowania wież z ludzi. Stowarzyszenie z Barcelony odwołuje się także do tego niematerialnego dziedzictwa kulturowego.