Agnieszka Witoszek

Najważniejsze zmiany w przepisach o ochronie danych osobowych

Podstawa prawna:

Rozporządzenie Parlamentu Europejskiego i Rady 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); zwane dalej RODO.

- Stosowane bezpośrednio.
- W razie wątpliwości – obowiązek proeuropejskiej wykładni prawa krajowego.
- Przestają obowiązywać krajowe regulacje dotyczące ochrony danych osobowych, ale osiągnięty „dorobek organizacyjny” pozostaje.
- Preambuła RODO – legalna wykładnia

Część I

Reforma prawa UE

Źródła informacji na temat RODO i interpretacji jego przepisów:

- Nowa ustawa o ochronie danych osobowych, wytyczne Urzędu Ochrony Danych Osobowych
- Wytyczne, Opinie, Wskazówki Grupy Roboczej Art.29 (po 25 maja 2018 zostanie zastąpiona Europejską Radą Ochrony Danych),
- Orzecznictwo (w przyszłości),
- Kodeksy dobrych praktyk (w poszczególnych branżach) zaakceptowane przez organ nadzorczy (GIODO lub inny organ powołany w jego miejsce lub jako kolejny organ ochrony danych),
- Wytyczne, stanowiska organów nadzorczych,
- **Wprowadzone systemy certyfikacji;**

Organ nadzorczy:

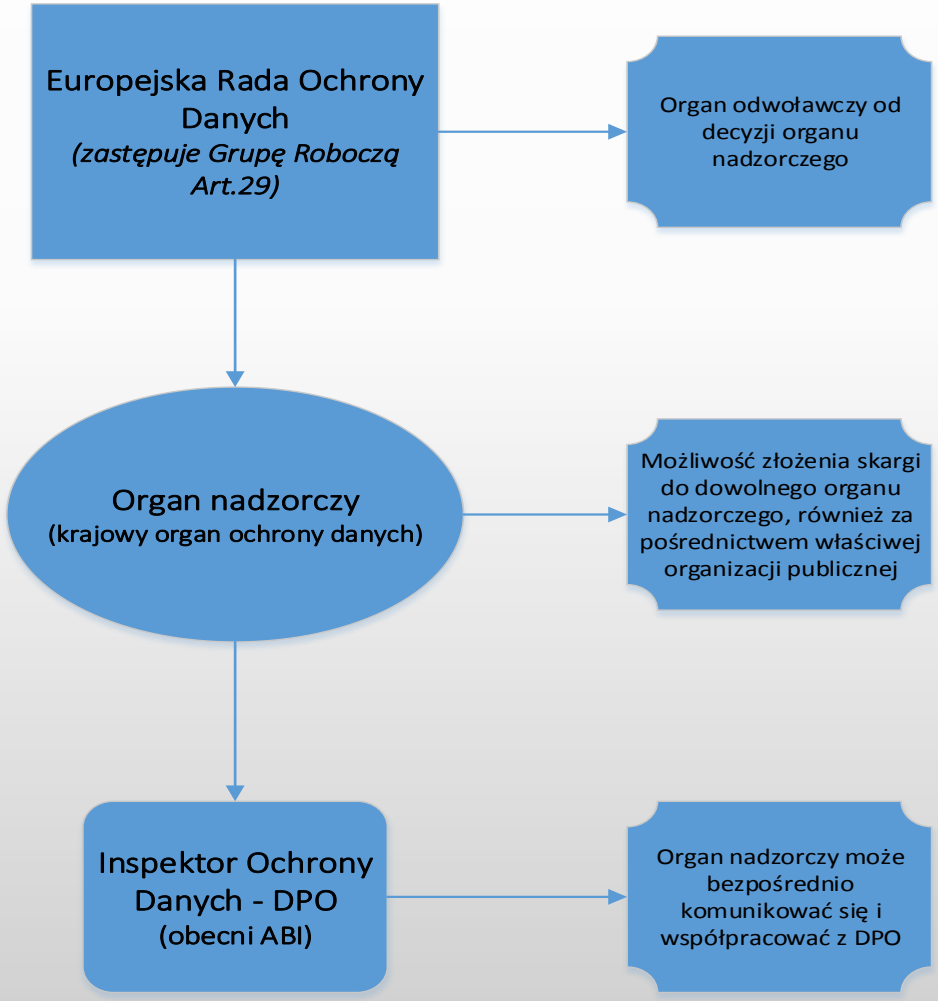
niezależny organ publiczny (co najmniej jeden) ustanowiony przez państwo członkowskie w celu monitorowanie stosowania RODO w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii

Co się nie zmieni pomimo wejścia w życie RODO?

- Administrator danych osobowych ma zapewnić odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych – **obowiązek rozliczalności**
- Obowiązek wskazania przez ADO właściwej przesłanki przetwarzania danych osobowych (art.6 ust.1 RODO), czyli wykazać, że przetwarza dane zgodnie z prawem
- Obowiązek przetwarzania przez ADO zgodnie z zasadami przetwarzania danych osobowych: zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności (art.5 ust.1 RODO)

Co zmienia RODO?

<u>Łatwiejsze składanie skarg do organu nadzorczego na łamanie prawa ochrony danych osobowych.</u>



Obowiązki ADO – bez względu na wielkość podmiotu i rodzaj przetwarzanych danych osobowych

- Rozszerzony obowiązek informacyjny – zarówno wobec pracowników, jak i podmiotów zewnętrznych, np. pacjenci, kontrahenci,
- Pobieranie w określonych przypadkach zgód na przetwarzanie danych osobowych i zarządzanie nimi,
- Wykonywanie praw osób, których dane przetwarzamy,
- W przypadku powierzania danych – umowa powierzenia z rozszerzonymi uprawnieniami kontrolnymi i odpowiedzialnością solidarną (możliwość wysuwania roszczeń regresowych),
- Tworzenie, utrzymywanie i usprawnianie procedur, nadawanie uprawnień do przetwarzania danych – właściwe, proporcjonalne do zagrożeń zabezpieczanie danych osobowych

Definicje istotne dla sektora medycznego.

„dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

„dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

„dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – *w tym o korzystaniu z usług opieki zdrowotnej* – ujawniające informacje o stanie jej zdrowia;

Ocena skutków przedsięwzięć dla ochrony prywatności (Ocena wpływu na prywatność – Data Protection Impact Assessment).

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

Grupa Robocza Art.29

<u>Opinia Grupy Roboczej Art.29 wprost wskazuje, że DPIA ma być wykonywane dla operacji przetwarzania danych wrażliwych.</u>

Wytyczne dotyczące praktycznego stosowania DPIA.

Identyfikacja, analiza, postępowanie z ryzykiem (zarządzenie ryzykiem):

- ISO/IEC 31000

Przykłady ogólnych wskazówek/przewodników dotyczących DPIA:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 201627.
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014.
- FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015.
- UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014.
- Wytyczne amerykańskie, australijskie

1. Ocena wpływu na prywatność – Data Protection Impact Assessment

- Analiza ryzyka dla wszystkich obszarów działania odnośnie bezpieczeństwa danych.

Przykłady:

- Nowe oprogramowanie
- Zakup sprzętu medycznego (dane osobowe, medyczne, genetyczne, biometryczne)
- Monitoring szpitalny
- Zarządzenia dyrektora, umowy z podmiotami zewnętrznymi, zmiany lokalizacji komórek organizacyjnych, np. archiwum

2. Uwzględnianie ochrony danych w fazie projektowania i domyślna ochrona danych.

REZOLUCJA W SPRAWIE PRYWATNOŚCI W FAZIE PROJEKTOWANIA

32 Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności Jerozolima, 27 – 29 października 2010 r.

W.R.Wiewiórowski, „Nowe europejskie regulacje w zakresie prywatności w fazie projektowania i prywatności w domyślnych ustawieniach", GIODO / WPiA Uniwersytet Gdański 2012 (wersja z 1 marca 2012 r.)

Ochrona danych w fazie projektowania: privacy by design.

Nie należy utożsamiać ani mylić z **privacy by default** czyli prywatnością jako ustawieniem domyślnym, przykład: portale społecznościowe (może stanowić jeden z elementów **privacy by design**).

Prywatność w Fazie Projektowania: Zasady Podstawowe

- Podejście proaktywne, nie reaktywne i zaradcze, nie naprawcze
- Prywatność jako ustawienie domyślne
- Prywatność włączona w projekt
- Pełna funkcjonalność: Suma dodatnia, nie suma zerowa
- Ochrona od początku do końca cyklu życia informacji
- Widoczność i przejrzystość
- Poszanowanie dla prywatności użytkowników

Privacy by design.

- Nowa usługa medyczna,
- Nowy sprzęt medyczny,
- Nowy sposób świadczenia usług, nowe miejsca świadczenia usług,
- Stworzenie nowych stanowisk pracy, nowych komórek organizacyjnych

Zawsze przeprowadzamy analizę w jaki sposób wprowadzić, ustanowić np. usługę, produkt czy przeprowadzić zmianę organizacyjną, aby uwzględnić ochronę danych osobowych i wykazać poszanowanie prywatności.

3. Rozliczalność.

- ADO musi być w stanie udowodnić, że właściwie chroni dane osobowe, w szczególności dane wrażliwe – ciężar dowodu po stronie ADO.
- Wszystkie operacje, przedsięwzięcia muszą być udokumentowane.

Np.:

- właściwe, stosowne do kategorii przetwarzanych danych procedury i środki techniczne, organizacyjne itp,.

- Przeprowadzanie skutków ochrony danych
- Uwzględnianie ochrony danych w fazie projektowania
- Szkolenie kadry
- Włączanie ABI (DPO) we wszystkie sprawy związane z ochroną danych i zapewnienie mu niezależności

Rozliczalność

Opinia 3/2010 Grupy Roboczej art. 29 w sprawie zasady rozliczalności. Przyjęta w dniu 13 lipca 2010 r.

„(…) termin ten wyraża sposób wykonywania odpowiedzialności i umożliwienie stosownej weryfikacji. Odpowiedzialność (ang. responsibility) i rozliczalność (ang. accountability) stanowią dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania. Dostatecznie zaufanie można rozwinąć jedynie, gdy wykaże się, że odpowiedzialność skutecznie funkcjonuje w praktyce. (…)”

4. Prawo do przenoszenia danych.

Art. 20 Rozporządzenia

- Przekazywanie danych w odpowiednim formacie podmiotom danych oraz wskazanym przez nie ADO, np. w celu kontynuacji leczenia

5. Rozbudowany obowiązek informacyjny (wobec pacjentów i pracowników).

- Kto będzie przetwarzał moje dane?
- W jakim celu?
- Jakie są moje prawa?
- Czy mam obowiązek podania danych, a jeśli tak to z czego on wynika?

- Dane kontaktowe inspektora ochrony danych
- Zamiar przekazania danych osobowych do państwa trzeciego
- Okres przechowywania danych (ew. przesłanki usunięcia)
- **Profilowanie**

6. Prowadzenie rejestru czynności przetwarzania danych.

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:

1)imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;

2)cele przetwarzania;

3)opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

4)kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

5)gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej;

6)jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

7)jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa tj.: pseudonimizacja i szyfrowanie danych osobowych, zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, przywracanie dostępności danych w razie incydentu fizycznego lub technicznego, regularność testowania i oceniania skuteczności ww. środków.

Kiedy mamy obowiązek prowadzić rejestr?

Zgodnie z Art.30 ust. 5 RODO do prowadzenia ww. rejestru zobowiązani są administratorzy i podmioty przetwarzające, które zatrudniają 250 lub więcej osób oraz gdy:

- dokonują systematycznego przetwarzania mogącego powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą, lub
- dokonują przetwarzania szczególnych kategorii danych osobowych, o których mowa w art.9 ust.1, lub
- przetwarzają dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Warto zwrócić uwagę, że każdy podmiot przetwarzający dane dotyczące zdrowia musi prowadzić rejestr i to bez względu na ilość zatrudnianych pracowników. Dane dotyczące zdrowia należą bowiem do szczególnych kategorii danych osobowych, o których mowa w art.9 ust.1. Obowiązek ten będzie ciążył np. zarówno na szpitalu jak i indywidualnej praktyce lekarskiej.

7. Obowiązek zgłoszenia do organu nadzorczego naruszenia danych osobowych (w niektórych przypadkach- również osobie, której dane dotyczą).

Kary finansowe w przypadku niezgłoszenia równie dotkliwe bądź większe.

W stwierdzeniu wagi naruszenia może pomóc wcześniejsza analiza ryzyka.

Np.:

- Co to jest awaria systemu informatycznego? – kryteria
- Kiedy mówimy o podejrzeniu ujawnienia danych osobowych?

8. Kary finansowe nakładane na ADO.

Art. 83 ust. 5 Rozporządzenia:

„administracyjna kara pieniężna”

(…) do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (…)

Kara nakładana będzie przez krajowy organ ochrony danych (do budżetu Państwa):

GIODO

9. Powierzanie danych osobowych.

- Zanim dane zostaną powierzone, ADO ma obowiązek sprawdzenia czy procesor spełnia wymagania Rozporządzenia – konieczność udokumentowania.
- Procedury kontroli procesora.

Jakie elementy powinna zawierać umowa powierzenia?

- jednoznacznie wskazany procesor (podmiot przetwarzający) i administrator danych;
- precyzyjnie określony zakres przekazywanych danych osobowych;
- określa jak długo dane będą przetwarzane na mocy umowy i co stanie się z danymi osobowymi po wygaśnięciu umowy;
- wyraźnie wskazany zakres odpowiedzialności procesora i zakres oraz rodzaj stosowanych przez niego środków ochrony danych osobowych;
- precyzuje w jaki sposób Administrator Danych Osobowych będzie dokonywał kontroli prawidłowości przetwarzanych danych osobowych przez procesora;
- określa odpowiedzialność za niewłaściwe przetwarzanie danych osobowych przez Procesora;

10. Zmiana statusu i obowiązków ABI.

ABI = Inspektor ochrony danych osobowych – funkcja doradcza i weryfikacyjna względem ADO, zatrudniany przez ADO, ale pozostający w bezpośrednim kontakcie z GIODO, quasi-audytor.

Niezależny, podległy bezpośrednio najwyższemu kierownictwu.

Wymagana wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych osobowych

Zakaz wydawania instrukcji.

ADO gwarantuje niezależność DPO wobec GIODO (organu nadzorczego).

DPO stanowić ma punkt kontaktowy dla GIODO i podmiotów ochrony danych (pracowników, pacjentów, kontrahentów, innych interesariuszy).

Kiedy mamy obowiązek powołania DPO (IOD)?

Ogólne rozporządzenie o ochronie danych w art. 37 us.t 1 przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających w następujących przypadkach, gdy:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- 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.
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10.

Dziękuję za uwagę

Agnieszka Witoszek