ENSI
KANCELARIA EKSPERTÓW

Jakie działania należy podjąć, aby dostosować firmę do wymagań rozporządzenia GDPR/RODO?

Maciej Byczkowski
European Network Security Institute

Agenda

- Nowy system przepisów dotyczących ochrony danych osobowych w UE
- Nowe wymogi dotyczące zabezpieczania danych osobowych w RODO
- Przygotowanie organizacji do wdrożenia RODO

Ogólne rozporządzenie o ochronie danych - RODO

- Rozpoczęcie stosowania: 25 maja 2018 r.
- Przepisy RODO są stosowane bezpośrednio bez konieczności dodatkowej implementacji do polskiego porządku prawnego
- RODO uchyla dyrektywę 95/46/WE oraz stanowiącą jej wykonanie polską ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Nowa ustawa uzupełniająca RODO w Polsce

- W 2017 r. planowane jest uchwalenie ustawy uzupełniającej RODO, która zastąpi obecną regulację i wejdzie w życie 25 maja 2018 r.
- Zakres przepisów o ochronie danych osobowych będzie obejmować:
  - Wykonanie odesłań zawartych w RODO
  - Doprecyzowania gdy jest to konieczne do zapewnienia skutecznego stosowania RODO w polskiej przestrzeni prawnej
- Dodatkowo prowadzony jest przegląd obowiązujących przepisów krajowych pod kątem dostosowania ich do RODO – planowana ustawa implementacyjna.

Wytyczne Grupy Roboczej Art. 29

- Przedstawione dotąd wytyczne dotyczą:
  - Inspektora ochrony danych
  - Prawa do przenoszenia danych
  - Wiodącego organu nadzorczego właściwego dla administratora danych lub podmiotu przetwarzającego
  - Ocen skutków dla ochrony danych
- Planowane kolejne wytyczne będą dotyczyć:
  - Certyfikacji
  - Kar finansowych
- Po rozpoczęciu stosowania RODO Grupa Robocza Art. 29 przekształci się w Europejską Radę Ochrony Danych

RODO - najważniejsze zmiany

- Szerszy zakres terytorialny stosowania unijnych przepisów
- Dopuszczalność współadministrowania danymi osobowymi przez kilka podmiotów
- Doprecyzowanie relacji administrator – podmiot przetwarzający (procesor/podprocesor)
- Konstrukcja prawna zgody podmiotów danych i warunków jej wyrażania
- Nowy zakres obowiązków informacyjnych
- Ustanowienie nowych praw podmiotów danych (prawo do bycia zapomnianym, prawo do ograniczonego przetwarzania, prawo do przenoszalności danych)

RODO - najważniejsze zmiany

- Modyfikacja zasad dopuszczalnego profilowania danych, w tym na potrzeby automatycznie podejmowanych decyzji
- Poszerzenie zakresu obowiązków w zakresie bezpieczeństwa danych
- Obowiązek wyznaczania, status i zadania inspektora ochrony danych
- Modyfikacja zasad dotyczących transferów danych osobowych do państwa trzeciego lub organizacji międzynarodowej
- Nowe sposoby wykazywania zgodności z przepisami o ochronie danych osobowych
- Nowe sankcje administracyjne i cywilnoprawne za naruszenie przepisów o ochronie danych osobowych

ENSI
KANCELARIA EKSPERTÓW

Zabezpieczenie danych w RODO Podejście oparte na ryzyku

Obowiązki dotyczące zabezpieczania danych osobowych w RODO

- Wdrożenie odpowiednich środków technicznych i organizacyjnych zabezpieczenia danych w oparciu o analizę ryzyka (art. 24 i 32)
- Wymogi uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25)
- Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego (art. 29)
- Prowadzenie rejestrów czynności przetwarzania danych osobowych (art. 30)
- Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33)
- Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34)
- Ocena skutków dla ochrony danych (art. 35)
- Uprzednie konsultacje z organem nadzorczym (art. 36)
- Rola Inspektora ochrony danych (art. 37 – 39)
- Kodeksy postępowania i certyfikacja (art. 40 - 42)

Co się nie zmienia?

- Podejście dotyczące doboru środków zabezpieczeń technicznych i organizacyjnych w odniesieniu do zagrożeń (ryzyka) i kategorii przetwarzanych danych (art. 36 ust. 1 u.o.d.o. – art. 24 i 32 RODO).
- Status i wykonywanie części zadań ABI przez Inspektora ochrony danych (art. 36a u.o.d.o. – art. 37 – 39 RODO)
- Wymóg zgłaszanie informacji o naruszeniach – w przypadku podmiotów z branży telekomunikacyjnej (art. 174 PT - art. 33 i 34 RODO)

Co się zmienia?

- Nowe wymagania dotyczące prowadzenia dokumentacji przetwarzania danych osobowych (art. 24 ust. 2, art. 30, art. 33 ust. 5 RODO)
- Brak szczegółowych wymagań dotyczących nadawania upoważnienia do przetwarzania danych (art. 29 RODO)
- Stosowanie kodeksów postępowania (art. 40 RODO)
- Nowe wymagania dotyczące analizy ryzyka w fazie projektowania oraz domyślnej ochrony danych (art. 25 RODO)
- Nowe rodzaje środków technicznych i organizacyjnych, w tym np. pseudonimizacja danych (art. 32 RODO)
- Nowe wymagania dotyczące oceny skutków przetwarzania danych (art. 35 RODO)
- Nowe wymagania dotyczące uprzednich konsultacji z organem nadzorczym (art. 36 RODO)
- Nowe wymagania dotyczące wyznaczenia Inspektora ochrony danych oraz jego zadań (art. 37 – 39 RODO)

Analiza ryzyka w RODO

Motyw 83:

- W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z RODO administrator lub podmiot przetwarzający **powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki –** takie jak szyfrowanie – **minimalizujące to ryzyko**
- Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie

Analiza ryzyka w RODO

Motyw 83 (cd):

- Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko:
  - związane z przetwarzaniem danych osobowych takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
  - mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych

Analiza ryzyka w RODO

- Wymogi analizy ryzyka w celu doboru środków technicznych i organizacyjnych dotyczących przetwarzania danych zgodnie z RODO
- Wymogi analizy ryzyka w celu doboru zabezpieczeń
- Wymogi analizy ryzyka w fazie projektowania
- Wymogi analizy ryzyka dotyczącej oceny skutków przetwarzania
- Wymogi dotyczące uprzednich konsultacji
- Przygotowanie do poniesienia konsekwencji:
  - Zgłaszanie naruszenia organowi nadzorczemu
  - Zawiadamianie podmiotu danych o naruszeniu
  - Dokumentowanie incydentu
  - Odpowiedzialność karna
- Rola inspektora ochrony danych w zarządzaniu ryzykiem

Wymóg stosowania zabezpieczeń

Art. 24 ust. 1 – Obowiązki ADO

- Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie **środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.**
- Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Wymóg stosowania zabezpieczeń

Art. 24 ust. 2 i 3 – Obowiązki ADO:

- Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
- Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Wymóg stosowania zabezpieczeń

Art. 25 ust. 1 - Uwzględnianie ochrony danych w fazie projektowania:

- Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, **administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania** – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Wymóg stosowania zabezpieczeń

Art. 25 ust. 2 – Domyślna ochrona danych:

- Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania
- Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności
- W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych

Wymóg stosowania zabezpieczeń

Art. 32 ust. 1 – Bezpieczeństwo przetwarzania:

- Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku

Wymóg stosowania zabezpieczeń

Art. 32 ust. 1 – Bezpieczeństwo przetwarzania:

- Rodzaje środków technicznych i organizacyjnych:
  - pseudonimizacja i szyfrowanie danych osobowych
  - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
  - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
  - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Wymóg stosowania zabezpieczeń

Art. 32 ust. 2 – Bezpieczeństwo przetwarzania:

- Oceniając, czy stopień bezpieczeństwa jest odpowiedni, **uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem**, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Ocena skutków dla ochrony danych

Art. 35 ust. 1 i 2:

- 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**
- Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony

Ocena skutków dla ochrony danych

Art. 35 ust. 3:

- Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
  - systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną
  - przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10
  - systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie

Ocena skutków dla ochrony danych

Artykuł 35 ust. 7:

- Ocena zawiera co najmniej:
  - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora
  - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów
  - **ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1**
  - środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy

Zgłaszanie naruszeń ochrony danych

Art. 33 - Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu:

- W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych
- Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia
- Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi

Kary pieniężne za brak realizacji obowiązków zabezpieczania danych

Art. 83 ust. 2:

- Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j).
- Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na m.in.:
  - stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;

Kary pieniężne za brak realizacji obowiązków zabezpieczania danych

Art. 83 ust. 4:

- Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:
  - a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, **25 – 39** oraz 42 i 43;

Docelowa dokumentacja

- Polityka ochrony danych (art. 24 ust. 2)
- Dokumentacja dotycząca przeglądów zastosowanych środków technicznych i organizacyjnych zabezpieczenia danych (art. 24 oraz 32)
- Rejestry czynności przetwarzania (art. 30):
  - ADO oraz podmiotów przetwarzających
- Procedury postępowania w sytuacji naruszenia ochrony danych osobowych, w tym dokumentacja naruszeń (art. 33)

Docelowa dokumentacja

- Dokumentacja z wykonywanych analiz ryzyka dotyczących przetwarzania danych (art. 24, 25 i 32)
- Dokumentacja dotycząca oceny skutków przetwarzania (art. 35 ust. 7)
- Dokumentacja dotycząca uprzednich konsultacji (art. 36)
- Dokumentacja wynikająca z zatwierdzonych kodeksów postępowania (art. 40)
- Dokumentacja wynikająca z zatwierdzonego mechanizmu certyfikacji (art. 42)

Przygotowanie do wdrożenia RODO

- Analiza potrzeb dotyczących wdrożenia RODO
  - Przegląd procesów przetwarzania danych
  - Wyspecyfikowanie koniecznych zmian w realizacji obowiązków związanych z przetwarzaniem i ochroną danych osobowych
    - w tym zmiany w systemach informatycznych
- Przygotowanie planu i harmonogramu wdrożenia RODO
- Wdrożenie wymagań RODO

Przygotowanie do wdrożenia RODO

- Zakres potencjalnych koniecznych zmian w systemach informatycznych:
  - Zapewnienie zbierania zgody na przetwarzanie danych w różnych celach (w tym na profilowanie)
  - Zapewnianie wyświetlania klauzul informacyjnych
  - Zapewnienie możliwości zdalnego dostępu osoby, której dane dotyczą do jej danych osobowych
  - Zapewnienie przetwarzania odpowiedniego (adekwatnego) zakresu danych w systemach:
    - *privacy by design*
    - *privacy by default*

Przygotowanie do wdrożenia RODO

- Zakres potencjalnych koniecznych zmian w systemach informatycznych:
  - Zapewnienie możliwości wnoszenia drogą elektroniczną żądań dotyczących usunięcia lub sprostowania danych osobowych
  - Zapewnienie usuwania danych z systemu:
    - Realizacja prawa do sprzeciwu na przetwarzanie danych
    - Realizacja prawa do bycia zapomnianym
    - Retencja danych zgodnie z przepisami
  - Zapewnienie prawa do przenoszenia danych
  - Zapewnienie prawa do ograniczenia przetwarzania
  - Zapewnienie możliwości pseudonimizacji danych

ENSI
KANCELARIA EKSPERTÓW

Dziękuję za uwagę!

www.ensi.net