INFOR AKADEMIA

www.inforakademia.pl

RODO W ORGANIZACJI- JAK PRAWIDŁOWO PRZYGOTOWAĆ SIĘ ORAZ UNIKNĄĆ KAR PIENIĘŻNYCH

Anna Sosińska
Administrator bezpieczeństwa informacji,
(certyfikat TÜV Technische Überwachung Hessen GmbH nr 244SH/13)

- **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**)

  - data wejścia w życie przepisów RODO - **24 maja 2016 r.**
  - data stosowania przepisów RODO - **25 maja 2018 r.**

INFOR AKADEMIA

PROJEKTOWANE AKTY KRAJOWE

- nowa ustawa o ochronie danych osobowych (data wejścia w życie – 25 maja 2018 r.), regulująca między innymi:

  - ✓ kompetencje organu nadzoru ds. ochrony danych osobowych
  - ✓ przepisy proceduralne przed organem ds. ochrony danych osobowych
  - ✓ inne kwestie nieuregulowane w RODO (np. sankcje)

INFOR AKADEMIA

PROJEKTOWANE AKTY KRAJOWE

- ustawa dotycząca przepisów wprowadzających ustawę o ochronie danych osobowych, czyli dostosowanie przepisów sektorowych do wymogów RODO (projekty nowelizacji 133 ustaw szczególnych)

INFOR AKADEMIA

OBOWIĄZKI ADMINISTRATORA DANYCH

1. Zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36.1. uodo).

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 rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane (RODO art. 24. 1. art. 32.)*

INFOR AKADEMIA

OBOWIĄZKI ADMINISTRATORA DANYCH

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

***a**) pseudonimizację i szyfrowanie danych osobowych;*

***b**) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*

***c**) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*

***d**) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

INFOR AKADEMIA

2. Prowadzić dokumentację opisującą sposób przetwarzania i ochrony danych (art. 36. 2. uodo)

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki bezpieczeństwa obejmują wdrożenie przez administratora ***odpowiednich polityk ochrony danych****.*

Stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków. (art. 24. 2 i 3 RODO)

INFOR AKADEMIA

3. Administrator danych może powołać administratora bezpieczeństwa informacji.
   W przypadku niepowołania administratora bezpieczeństwa informacji zadania ABI (określone w ustawie) wykonuje administrator danych (uodo art. 36a)

Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) *przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;*
b) *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*
c) *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 czym mowa w art. 10.*
   (RODO art. 37)

INFOR AKADEMIA

4. Do przetwarzania danych dopuścić wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego (art. 29 RODO).

Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego. (art. 32. 4. RODO)

5. Zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Informacje i dostęp do danych osobowych – dodatkowe obowiązki informacyjne i prawa osób, których dane dotyczą (RODO art. od 13 do 22)

6. Prowadzić ewidencję osób upoważnionych do ich przetwarzania

7. Prowadzić rejestr/wykaz zbiorów danych.

Rejestrowanie czynności przetwarzania (RODO art. 30)

Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora

Ocena skutków przetwarzania dla ochrony danych osobowych

Inne, dodatkowe, nowe obowiązki administratorów oraz prawa osób, których dane dotyczą:

- Rozszerzone obowiązki informacyjne,
- Nowe zasady uzyskiwania zgód na przetwarzanie danych
- Ograniczenie profilowania,
- Prawo do przenoszenia danych,
- Prawo do ograniczenia przetwarzania danych, do usuwania danych, prawo „do bycia zapomnianym”
- Informowanie o naruszeniach ochrony danych,
- Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych,
- Odpowiedzialność finansowa i odszkodowawcza

INFOR AKADEMIA

Nowe obowiązki informacyjne (art. 13)

- tożsamość i dane kontaktowe administratora oraz gdy zostanie powołany tożsamość i dane kontaktowe przedstawiciela
- dane kontaktowe inspektora ochrony danych
- cel przetwarzania danych oraz podstawa prawna przetwarzania (jeśli Prawnie uzasadniony interes – gdy jest podstawą przetwarzania – to jaki)
- zamiar przekazywania danych osobowych do kraju trzeciego lub organizacji międzynarodowej
- możliwości uzyskania kopii danych lub o miejscu udostępniania danych
- okres przechowywania, gdy nie jest to możliwe kryteria ustalenia
- prawo do dostępu, sprostowania, usunięcia, prawo do sprzeciwu itp.
- możliwość cofnięcia zgody w dowolnym momencie
- prawo do wniesienia skargi do organu nadzorczego
- wymóg podania danych – ustawa, umowa, warunki zawarcia umowy, dlaczego wymagane jest podanie danych i konsekwencje ich niepodania

Prawa podmiotów danych z RODO

- informacji art. 13, 14
- do dostępu art.15
- sprostowanie danych art. 16, 19
- usunięcia danych/ bycia zapomnianym art. 17, 19
- ograniczenia przetwarzania art. 18, 19
- przenoszenia danych art. 20
- sprzeciwu art. 21
- nie podlegania profilowaniu art. 21, 22

Wszystkie prawa co do zasady są wolne od opłat

INFOR AKADEMIA

Szacowanie ryzyka

Przeprowadzenie analizy ryzyka wynika z następujących artykułów RODO:

Art.24 – obowiązki administratora

Art.25 – uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Art. 32 – bezpieczeństwo przetwarzania

Art. 33 – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

Art. 35 – ocena skutków dla ochrony danych

INFOR AKADEMIA

Szacowanie ryzyka

Ważne!

- dobrać adekwatne zabezpieczenia technologiczne i organizacyjne, które mają minimalizować ryzyko mogące wyniknąć z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieautoryzowanego dostępu do danych przesyłanych, przechowywanych bądź w inny sposób przetwarzanych
- zidentyfikować i dokonać analizy ryzyk skutkujących naruszeniem praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia

INFOR AKADEMIA

Metodyka szacowania ryzyka

WAŻNE!

- RODO ***nie narzuca*** żadnych konkretnych metodyk przeprowadzania szacowania ryzyka
- Można korzystać z dowolnej metodologii

INFOR AKADEMIA

WYMAGANIA OCENY SKUTKÓW DLA OCHRONY DANYCH (art. 35 RODO)

- przeprowadza się wówczas, gdy przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych
- wymagana jest w przypadku:

a) 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;

b) 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; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

INFOR AKADEMIA

Dokumentacja ochrony danych w RODO:

1. Dokumenty obligatoryjne:

- polityka / polityki ochrony danych (art.24)
- rejestr czynności przetwarzania danych (art. 30)
- dokumentacja naruszeń ochrony danych naruszeń ochrony danych (art. 33-34)
- dokumentacja oceny skutków przetwarzania danych (art.35)

INFOR AKADEMIA

Dokumentacja ochrony danych w RODO:

2. Dokumentacja dotycząca zasad przetwarzania danych:

- klauzule informacyjne (podstawowe wersje: podmiot danych - klient (konsument/przedsiębiorca) oraz podmiot danych - pracownik) – art.13 i 14
- klauzule zgody na przetwarzanie danych osobowych – art.7
- polityka retencji danych (tabela retencyjna) – art.5 ust.1 pkt e)
- test równowagi (uzasadniony interes administratora danych) – art.6 ust.1 pkt f)

INFOR AKADEMIA

Dokumentacja ochrony danych w RODO:

3.Dokumentacja dotycząca współadministratora:

- wzór uzgodnień między współadministratorami – art.26 ust.1

4. Dokumentacja dotycząca powierzenia przetwarzania danych:

- procedura weryfikacji i wyboru processora – art.28 ust.1
- wzory umowy powierzenia przetwarzania danych osobowych (dwie wersje: podstawowa i rozszerzona) – art.28 ust.3

INFOR AKADEMIA

Dokumentacja ochrony danych w RODO:

5. Dokumentacja dotycząca inspektora ochrony danych osobowych (IOD)

- regulamin funkcjonowania inspektora ochrony danych osobowych – art.37 i n.
- dokumentacja związana z rejestrem czynności przetwarzania danych
- wzór rejestru czynności przetwarzania danych (administrator) – art.30
- wzór rejestru czynności przetwarzania danych (procesor) – art.30

6. Dokumentacja dotycząca praw podmiotów danych

- procedura załatwiania żądań podmiotu danych – art.12 i n.
- dokumentacja związana z naruszeniami ochrony danych osobowych
- procedury działania w przypadku naruszenia danych osobowych – art.33
- ewidencja naruszeń ochrony danych osobowych – art.33 ust.5
- wzór zawiadomienia organu nadzorczego o naruszeniu danych osobowych – art.33
- wzór zawiadomienia osoby, której dane dotyczą o naruszeniu danych osobowych – art.34

INFOR AKADEMIA

SANKCJE

1. Wynikające z RODO (art.83; Motywy 148, 150-151), ***sankcje administracyjne*** za *naruszenie przepisów*
   o ochronie danych osobowych (prywatności), m.in. ***kary pieniężne*** 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
- lub w przypadku naruszeń *szczególnie istotnych obowiązków* –

  w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,

INFOR AKADEMIA

SANKCJE

2. Wynikające z przepisów krajowych - art.84 (Motywy 149, 152)- RODO wskazuje na możliwość przyjęcia przez państwa członkowskie przepisów, określających inne sankcje za naruszenie RODO; mają one być ***skuteczne, proporcjonalne i odstraszające***.

INFOR AKADEMIA

SANKCJE

3. Odpowiedzialność cywilnoprawna – art. 79, 82 RODO (Motywy 141, 145, 146, 147):

„… każda osoba, której dane dotyczą ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia…”

„… każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę…”

INFOR AKADEMIA

Zgodnie z art. 84, *każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych (…), a następnie niezwłocznie o każdej późniejszej ich zmianie*

INFOR AKADEMIA

PROJEKTOWANE KARY PIENIĘŻNE

- **NA ORGANY I PODMIOTY PUBLICZNE**

  Prezes Urzędu może nałożyć w drodze decyzji administracyjnej kary pieniężne w wysokości do 100 tys. zł

INFOR AKADEMIA

PROJEKTOWANE KRAJOWE PRZEPISY KARNE

- **Art. 101.**

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, ***podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch*.**
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, biometrycznych, o stanie zdrowia, seksualności lub orientacji seksualnej, ***podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech*.**

- **Art. 102.** Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych***, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch*.**

INFOR AKADEMIA

Konieczne działania przygotowujące do RODO

PRAWNE

Umowy (przegląd umów, zwłaszcza powierzenia danych), Polityki bezpieczeństwa / Procedury, Zgody / Klauzule informacyjne/ Regulaminy / Polityki prywatności (transparentność)/ Śledzenie zmian w prawie/

kodeksy postępowania …

ORGANIZACYJNE

Szkolenia/ Podejście oparte na ryzyku / Ocena skutków dla ochrony danych - wszystkie zmiany / Zarządzanie incydentami

TECHNICZNE

Dostosowanie do wypełniania praw podmiotów danych/

Zgody na profilowanie/ Stosowanie adekwatnych zabezpieczeń (Privacy by Design)/ Rejestrowanie czynności przetwarzania - dane klientów i pracowników

INFOR AKADEMIA