Urząd Ochrony Danych Osobowych

OBOWIĄZKI PRZEDSIĘBIORCÓW WYNIKAJĄCE Z RODO

Piotr Drobek
Dyrektor
Zespołu Analiz i Strategii
UODO

Urząd Ochrony Danych Osobowych

REFORMA PRAWA UE

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679

z dnia 27 kwietnia 2016 r. **(RODO)**

Urząd Ochrony Danych Osobowych

DO 24 MAJA 2018 ROKU

- Ustawa z 29.08.1997 r. o ochronie danych osobowych
- Rozporządzenia wykonawcze

OD 25 MAJA 2018 ROKU

- Ogólne rozporządzenie o ochronie danych (RODO)
- Ustawa z 10.05.2018 r. o ochronie danych osobowych
- Pozostawione w mocy przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych

Urząd Ochrony Danych Osobowych

DOPRECYZOWANIE TREŚCI RODO

- Ustawa z 10.05.2018 r. o ochronie danych osobowych
- Nowelizacja przepisów sektorowych, np. Kodeks pracy

DOPRECYZOWANIE TREŚCI RODO

Urząd Ochrony Danych Osobowych

- Wytyczne Grupy Roboczej Art. 29
- Wytyczne Europejskiej Rady Ochrony Danych
- Opinie i wyjaśnienia Prezesa UODO
- Wykaz operacji wymagających przeprowadzenia oceny skutków dla ochrony danych
- Poradniki i wskazówki Prezesa UODO
- Zalecenia Prezesa UODO w sprawie zabezpieczeń

WYTYCZNE GR ART. 29/EROD

Urząd Ochrony Danych Osobowych

Kolejne dokumenty:

- Zgoda
- IOD
- Ocena skutków dla ochrony danych osobowych
- Zgłaszanie naruszeń ochrony danych
- Zasada przejrzystości
- Certyfikacja
- Mechanizmy współpracy
- Profilowanie
- Zasady działania Europejskiej Rady Ochrony Danych

Urząd Ochrony Danych Osobowych

PUBLIKACJE PREZESA UODO

- **Wskazówki w sprawie monitoringu wizyjnego**
- **Poradnik – odo w szkołach i placówkach oświatowych**
- **Poradnik – odo w wyborach**

W przygotowaniu m.in.

- **Poradnik odo w zatrudnieniu**
- **Poradnik odo w marketingu**

MONITOROWANIE PRAC NAD WDROŻENIEM RODO

http://www.giodo.gov.pl

http://www.uodo.gov.pl

- Stanowiska GIODO/ Prezesa UODO
- Poradniki i inne materiały informacyjne

REFORMA PRAWA UE

Nowe rozwiązania dla lepszej zgodności przetwarzania danych z przepisami rozporządzenia

- Kodeksy postępowania i certyfikacja

POJĘCIE DANYCH OSOBOWYCH

- Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”).

- Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

SZCZEGÓLNE KATEGORIE DANYCH

- Dane ujawniające pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- Dane genetyczne
- Dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej
- Dane dotyczące stanu zdrowia
- Dane dotyczące seksualności lub orientacji seksualnej

Podobnie traktowane: Dane dotyczące wyroków skazujących i naruszeń prawa

ADMINISTRATOR DANYCH

- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

PODMIOT PRZETWARZAJĄCY

- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora
- Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą

POWIERZENIE PRZETWARZANIA DANYCH

- Zawieranie umów powierzenia przetwarzania danych
- Obowiązki podmiotów przetwarzających
- Podpowierzenie przetwarzania

POWIERZENIE PRZETWARZANIA DANYCH

- Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie:
- umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

OBOWIĄZKI ADMINISTRATORA DANYCH

<u>Nowe</u> obowiązki:

1. **konieczność zapewnienia określonych warunków w procesie zautomatyzowanego podejmowania decyzji w indywidualnych sprawach (profilowanie) – art. 22**
2. **uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych – art. 25**
3. **rejestrowanie czynności przetwarzania – art. 30**
4. **zgłaszanie naruszenia ochrony danych organowi nadzorczemu**
5. **zawiadamianie podmiotu danych o naruszeniu ochrony danych osobowych – art. 34**
6. **ocena skutków dla ochrony danych – art. 35**
7. **obowiązek określenia czasu przetwarzania danych**
8. **obowiązek przeniesienia danych**
9. **wyznaczenie inspektora ochrony danych jako czynność obligatoryjna w niektórych przypadkach a nie wyłącznie fakultatywna**

ZASADY PRZETWARZANIA DANYCH

Zasady przetwarzania danych – niezmienne wartości

ZASADY PRZETWARZANIA DANYCH

UODO	RODO
✓legalizm ✓celowość ✓merytoryczna poprawność ✓adekwatność ✓ograniczenie czasowe	✓zgodność z prawem, rzetelność i przejrzystość ✓ograniczenie celu ✓minimalizacja danych ✓prawidłowość ✓ograniczenie przechowywania integralność i poufność rozliczalność

INNOWACJE WPROWADZANE PRZEZ OGÓLNE ROZPORZĄDZENIE

Rozliczalność
czyli

Obowiązek przestrzegania zasad ochrony danych i zdolność do wykazania tego

poprzez

Wdrożenie wewnętrznych mechanizmów i procedur

DLA REALIZACJI ZADAŃ PRZEZ ADMINISTRATORA ISTOTNE JEST:

Podsumowując …

zasady przetwarzania danych – niezmienne wartości

niemniej

1. **analiza nowego ukształtowania niektórych przesłanek przetwarzania**
2. **analiza nowych pojęć i definicji**
3. **analiza modelu komunikowania o procesie przetwarzania**

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

- **Dane zwykłe** – art. 6 RODO
- **Szczególne kategorie danych –** art. 9 i 10 RODO

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

Przetwarzanie zgodne z prawem

- zgoda - dobrowolne, konkretne, świadome i jednoznaczne **okazanie woli**; oświadczenie / **wyraźne działanie**
- Umowa
- obowiązek prawny ciążący na administratorze

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

Przetwarzanie zgodne z prawem

- ochrona żywotnych interesów
- zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej
- prawnie uzasadnione interesy

ZGODA

W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem będzie przetwarzanie danych osobowych dziecka, które ukończyło 16 lat.

Zasada przejrzystości – art. 12

Administrator podejmuje **odpowiednie środki**, aby w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem** – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się **na piśmie lub w inny sposób**, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji **można udzielić ustnie**, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Zasada przejrzystości – art. 12

Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć **standardowymi znakami graficznymi**, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.

OBOWIĄZEK INFORMACYJNY

- To nie tylko noty informacyjne!
- Aktywne i pasywne sposoby informowania.
- Warstwowe przekazywanie informacji on line / off line
- Prosty język

OBOWIĄZEK INFORMACYJNY

- Zbieranie danych od osoby, której dane dotyczą – art. 13 RODO
- Zbieranie danych z innych źródeł – art. 14

Art. 24 UODO	Art. 13 RODO
✓ adres siedziby i pełna nazwa ✓cel zbierania danych ✓Odbiorcy lub kategorie odbiorców ✓ prawo dostępu do treści swoich danych oraz ich poprawiania ✓Informacja o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej	✓Tożsamość administratora i dane kontaktowe ✓dane kontaktowe IOD ✓Cel przetwarzania i **podstawa prawna** ✓**Prawnie uzasadniony interes** ✓Odbiorcy danych lub kategorie odbiorców ✓**Przekazanie danych do państwa trzeciego** ✓**Okres przechowywania** ✓Prawa osób ✓Odwołanie zgody ✓**Prawo do złożenia skargi** ✓Informacja o obowiązku lub dobrowolności podania danych i konsekwencjach niepodania danych ✓**Zautomatyzowane podejmowanie**

Art. 25 UODO	Art. 14 RODO
✓ adres siedziby i pełna nazwa ✓cel zbierania danych ✓Zakres danych ✓Odbiorcy lub kategorie odbiorców ✓Źródło danych ✓ prawo dostępu do treści swoich danych oraz ich poprawiania ✓Prawo sprzeciwu	✓Tożsamość administratora i dane kontaktowe ✓dane kontaktowe IOD ✓Cel przetwarzania i **podstawa prawna** ✓**Prawnie uzasadniony interes** ✓Odbiorcy danych lub kategorie odbiorców ✓Kategorie danych ✓**Przekazanie danych do państwa trzeciego** ✓**Okres przechowywania** ✓Źródło danych ✓Prawa osób ✓**Odwołanie zgody** ✓**Prawo do złożenia skargi** ✓**Zautomatyzowane podejmowanie decyzji**

OGRANICZENIA OBOWIĄZKU INFORMACYJNEGO – ART. 13

Jedynie gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami

OGRANICZENIA OBOWIĄZKU INFORMACYJNEGO – ART. 14

- a) osoba, której dane dotyczą, dysponuje już tymi informacjami;

- b)udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
  w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie.

OGRANICZENIA OBOWIĄZKU INFORMACYJNEGO – ART. 14

- c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub

- d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

PRAWA OSÓB

- rozbudowane obowiązki administratora
- ułatwienia i więcej praw dla podmiotów danych

PRAWA OSÓB

- Bezpłatny dostęp do danych osobowych
- Miesiąc na odpowiedź
- Przejrzystość

PRAWA OSÓB

Obowiązek informacyjny – chcesz moje dane, powiedz mi po co?

- 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
  - Profilowanie

PRAWA OSÓB

- Prawo dostępu
- Prawo do sprostowania/uzupełnienia danych

PRAWA OSÓB

- Prawo do ograniczenia przetwarzania
- Przenoszalność danych

PRAWA OSÓB

- Prawo sprzeciwu

PRAWA OSÓB

- Zagadnienie profilowania

Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się

dopuszczalność i ograniczenia – motywy 29, 30, 38, 60, 63, 70, 71, 73, 91

PRAWA OSÓB

Prawo do bycia zapomnianym
czyli prawo do usunięcia danych

a

wyjątek z art. 17 ust. 3 lit. b RODO

STATUS ABI – STATUS DPO

Administrator Bezpieczeństwa Danych Osobowych (ABI)

=

Inspektor Ochrony Danych (DPO)

WYZNACZENIE ABI/DPO
Uprawnienie czy obowiązek?

do 24.05.2018 r.

uprawnienie (zgodnie z UODO)

od 25.05.2018 r.

obowiązek/uprawnienie (zgodnie z RODO)

WYZNACZANIE DPO WEDŁUG RODO

Obowiązek wyznaczenia DPO:

- organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości
- rodzaj głównej działalności podmiotu

WYZNACZENIE INSPEKTORA OCHRONY DANYCH

OBOWIĄZKOWE WYZNACZENIE DPO

Zgodnie z rozporządzeniem obowiązkiem niektórych administratorów i przetwarzających będzie powołanie DPO.

Taki obowiązek będzie w przypadku wszystkich organów i podmiotów publicznych (niezależnie od zakresu przetwarzanych danych)

w stosunku do podmiotów, które w ramach swojej głównej działalności regularnie i na dużą skalę monitorują osoby

lub jeżeli główna działalność podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych dotyczących wyroków skazujących lub naruszeń prawa

WYZNACZENIE INSPEKTORA OCHRONY DANYCH

DUŻA SKALA

GR podaje przykłady przetwarzania danych na dużą skalę, m.in.

- **przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności.**

WYZNACZENIE INSPEKTORA OCHRONY DANYCH

REGULARNE I SYSTEMATYCZNE MONITOROWANIE

Grupa daje również wskazówki co do tego jak definiować termin „regularne” np. jako występujące w określonych odstępach czasu przez ustalony okres, natomiast „systematyczne” jako np. występujące zgodnie z określonym systemem; zorganizowane lub metodyczne.

Jako przykład regularnego i systematycznego monitorowania wskazano, m.in.

- śledzenie lokalizacji w aplikacjach telefonicznych
- scoring kredytowy lub ubezpieczeniowy
- monitorowanie danych o stanie zdrowia za pośrednictwem urządzeń przenośnych.

NIEZALEŻNOŚĆ DPO

- **Motyw 49 i art. 18 ust. 2 dyrektywy 95/46/WE** administrator danych może powołać urzędnika do spraw ochrony danych osobowych (personal data protection official), który musi sprawować swoją funkcję w sposób **całkowicie niezależny.**

- **Art. 36a ust. 8 UODO** - funkcję ABI może pełnić osoba, która ma zapewnione środki i organizacyjną odrębność, niezbędne do **niezależnego** wykonywania przez niego zadań.

- **Motyw 97 RODO** inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób **niezależny.**

POZYCJA DPO

UDZIAŁ DPO WE WSZYSTKICH ZAGADNIENIACH ZWIĄZANYCH Z OCHRONĄ DANYCH OSOBOWYCH

W opinii GR bardzo ważne jest, by DPO był angażowany od najwcześniejszego etapu we wszystkie kwestie związane z przetwarzaniem danych osobowych.

Informowanie DPO i jego udział w początkowych fazach jakiegokolwiek przedsięwzięcia związanego z przetwarzaniem danych osobowych powinno być standardową procedurą w organizacji.

KONFLIKT INTERESÓW

DPO może wykonywać inne zadania i obowiązki, ale administrator danych ma zapewnić, żeby nie powodowało to konfliktu interesów.

GR wyjaśnia, że co do zasady konflikt interesów będą powodować stanowiska kierownicze. Ponadto DPO nie może zajmować w organizacji stanowiska związanego z określaniem sposobów i celów przetwarzania danych.

Aspekt ten powinien być analizowany osobno dla każdego podmiotu.

GR zaleca w tym zakresie m.in. :

- **zidentyfikowanie stanowisk niekompatybilnych z funkcją DPO;**
- **opracowanie wewnętrznej polityki dotyczącej konfliktu interesów;**
- **ustalenie, że nie ma konfliktu interesów w funkcjonowaniu obecnego DPO, w celu zwiększenia świadomości na temat tego wymogu;**
- **zapewnienie, by ogłoszenia o rekrutacji na stanowisko DPO były precyzyjne i niwelowały ryzyko powstania konfliktu interesów**

Urząd Ochrony Danych Osobowych

Ustawa z 29.08.1997 r.

Art. 36 ust. 2

Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Urząd Ochrony Danych Osobowych

Rozporządzenie MSWiA z 29.04.2004 r.

Na dokumentację składa się:

- **polityka bezpieczeństwa**
- **instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

Dokumentację prowadzi się w formie pisemnej.

Dokumentację wdraża administrator danych.

Urząd Ochrony Danych Osobowych

Rozporządzenie MSWiA z 29.04.2004 r.

Polityka bezpieczeństwa zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Urząd Ochrony Danych Osobowych

Rozporządzenie MSWiA z 29.04.2004 r.

Instrukcja zarządzania systemem informatycznym zawiera w szczególności:

1. **procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;**
2. **stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;**
3. **procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;**

Urząd Ochrony Danych Osobowych

Rozporządzenie MSWiA z 29.04.2004 r.

Instrukcja zarządzania systemem informatycznym zawiera w szczególności:

4. **procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;**
5. **sposób, miejsce i okres przechowywania:**

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych

4. **sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;**
5. **sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;**
6. **procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.**

Urząd Ochrony Danych Osobowych

ZASADA ROZLICZALNOŚCI

ART. 5 ust. 2 RODO

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

Art. 24 ust. 1 RODO

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.

Urząd Ochrony Danych Osobowych

ZASADA ROZLICZALNOŚCI

Art. 24 ust. 2 RODO

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Urząd Ochrony Danych Osobowych

OBOWIĄZKI ADMINISTRATORA

- Rejestr czynności przetwarzania
- Dokumentowanie wszelkich naruszeń ochrony danych i i związana z nimi procedura postępowania
- Dokumentowanie różnych działań (np. zgoda, ocena skutków dla ochrony danych, ocena konfliktu interesu IOD)

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

- zatrudnia więcej niż 250 osób (bez względu na formę zatrudnienia)
- przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą
- przetwarzanie nie ma charakteru sporadycznego
- przetwarzanie obejmuje szczególne kategorie danych osobowych,

ROLA IOD W TWORZENIU REJESTRU

Urząd Ochrony Danych Osobowych

Prowadzenie rejestru „czynności przetwarzania” to obowiązki administratora albo podmiotu przetwarzającego.

Jednak GR podkreśla, że katalog zadań IOD wskazany w art. 39 nie jest zamknięty i na mocy od dawna ustalonej praktyki to IOD tworzy i prowadzi zwykle rejestry w oparciu o dane otrzymane od pozostałych komórek organizacji.

REJESTR CZYNNOŚCI PRZETWARZANIA

Urząd Ochrony Danych Osobowych

Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

- **imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;**
- **cele przetwarzania;**
- **opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;**
- **kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;**
- **gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;**
- **jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;**
- **jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.**

REJESTR CZYNNOŚCI PRZETWARZANIA

Urząd Ochrony Danych Osobowych

Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

d)jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

REJESTR CZYNNOŚCI PRZETWARZANIA

Urząd Ochrony Danych Osobowych

Czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
Np. rekrutacja pracowników, obsługa umów sprzedaży

Kategoria czynności przetwarzania (kategoria przetwarzań) to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.
Np. przechowywanie danych klienta (administratora) rozumiane jako udostępnienie zamawiającemu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający(administrator) sam zarządza i decyduje o tym, jakie dane tam przechowuje –
np. wykonuje kopie zapasowe danych elektronicznych

RODO wyraźnie wskazuje konieczność regularnego testowania, mierzenia i oceniania skuteczności wdrożonych środków technicznych i organizacyjnych, które mają zapewnić bezpieczeństwo przetwarzania danych.

Obowiązki ADO:

- Rejestrowanie czynności przetwarzania - **ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**
- Dokumentowanie wszelkich naruszeń ochrony danych

Obowiązki ADO:

- Wdraża odpowiednie środki techniczne i organizacyjne
- Uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych
- Odpowiednie polityki danych?
- Zachęta do stosowania zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji

ZABEZPIECZENIE DANYCH OSOBOWYCH

Obowiązki ADO:

- środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych **odpowiednią do zagrożeń** oraz **kategorii danych** objętych ochroną

- zabezpieczenie danych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

OBOWIĄZEK ZABEZPIECZENIA DANYCH OSOBOWYCH

- Obowiązek stosowania odpowiednich środków organizacyjno-technicznych
- Dopuszczone do przetwarzania danych osobowych mogą być tylko osoby upoważnione
- Przy doborze środków administrator powinien uwzględniać najnowsze osiągnięcia techniczne oraz koszty wdrożenia tych środków
- Obowiązek przeprowadzenia odpowiedniej analizy ryzyka

BEZPIECZEŃSTWO PRZETWARZANIA

Zapewnienie odpowiedniego stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia danych osobowych

- ❑ Pseudonimizacja i szyfrowanie danych
- ❑ Zapewnienie poufności i integralności
- ❑ Skuteczność funkcjonowania systemów
- ❑ Jak ocenić stopień bezpieczeństwa?
- ❑ Jak wykazać wywiązywanie się z obowiązku zabezpieczenia danych?

USUWANIE DANYCH OSOBOWYCH

- Administrator informuje o okresie przechowywania danych lub kryteriach, które służą do określenia tego okresu

- Administrator uwzględniając ochronę danych w fazie projektowania musi wziąć pod uwagę również aspekt usuwania danych w cyklu zarządzania danymi

OCENA SKUTKÓW DLA OCHRONY DANYCH

Obowiązek uprzedniej analizy planowanych procesów przetwarzania danych

WYTYCZNE GRUPY ROBOCZEJ ART. 29

Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko”, do celów rozporządzenia 2016/679 (17/EN WP 248)

- Kto jest zobowiązany do przeprowadzenia DPIA?

Administrator danych, z DPO i podmiotem przetwarzającym (podmiotami przetwarzającymi).

UPRZEDNIE KONSULTACJE

Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby **wysokie ryzyko,** gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

POSTĘPOWANIE W RAZIE NARUSZENIA BEZPIECZEŃSTWA

Urząd Ochrony Danych Osobowych

- **wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;**

- **prowadzenie wewnętrznej ewidencji naruszeń;**

POSTĘPOWANIE W RAZIE NARUSZENIA BEZPIECZEŃSTWA

Urząd Ochrony Danych Osobowych

- **Zgłoszenie naruszenia Prezesowi UODO;**
- **Zawiadomienie osób, których dane dotyczą;**

Dziękuję za uwagę