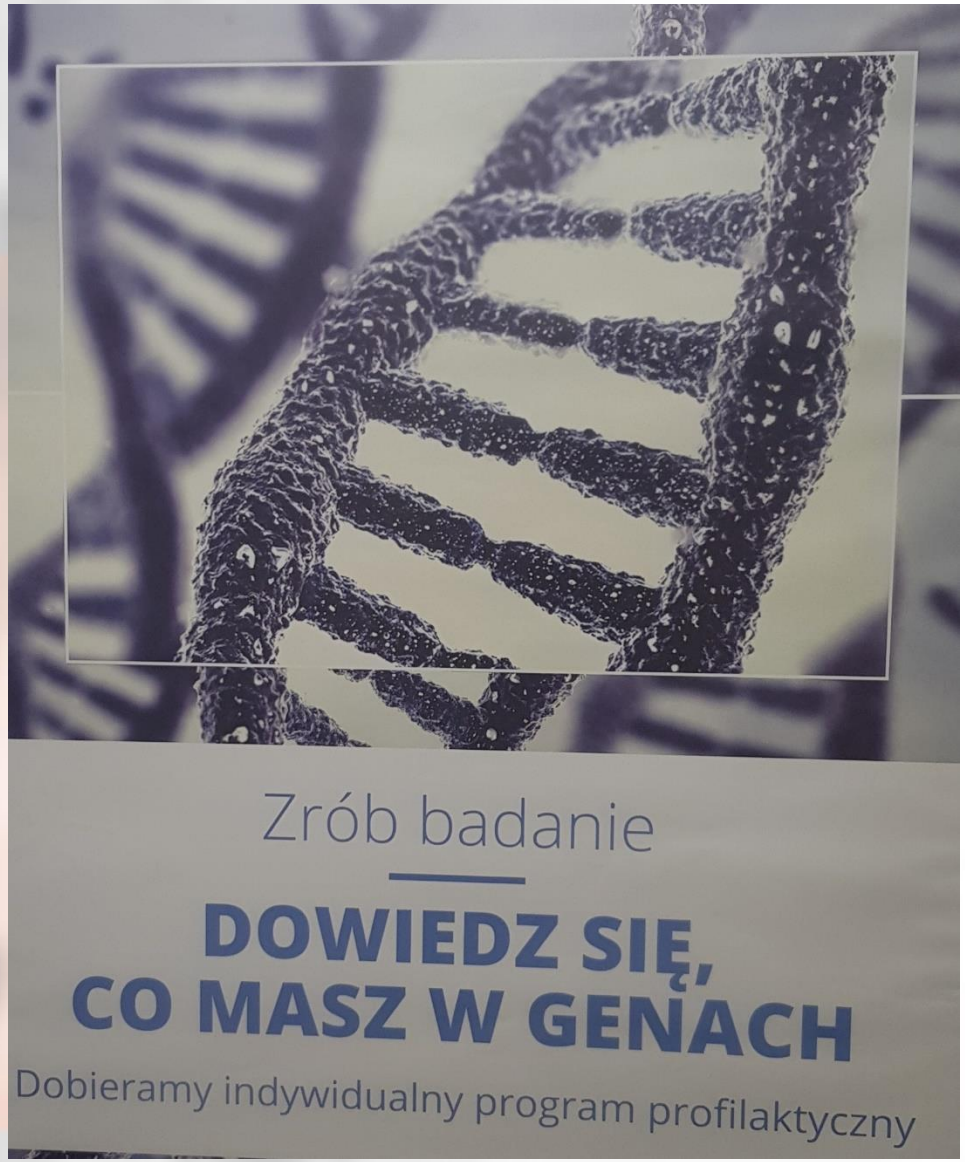
Urząd Ochrony Danych Osobowych

RODO – NAJISTOTNIEJSZE ELEMENTY DLA ŚWIADCZENIODAWCY: „CHECK LIST” KONTROLE, FORMY ZABEZPIECZENIA BAZ DANYCH

Tomasz Soczyński
Dyrektor Zespołu Informatyki
Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@giodo.gov.pl



Urząd
Ochrony
Danych
Osobowych

Urząd Ochrony Danych Osobowych

REFORMA PRAWA UE

- Dostosowanie zasad ochrony danych do aktualnego stanu wiedzy
- Podejście oparte na **ryzyku**
- **Rozliczalność** – wykazanie przestrzegania przepisów o ochronie danych

Urząd Ochrony Danych Osobowych

ZASADA LEGALIZMU

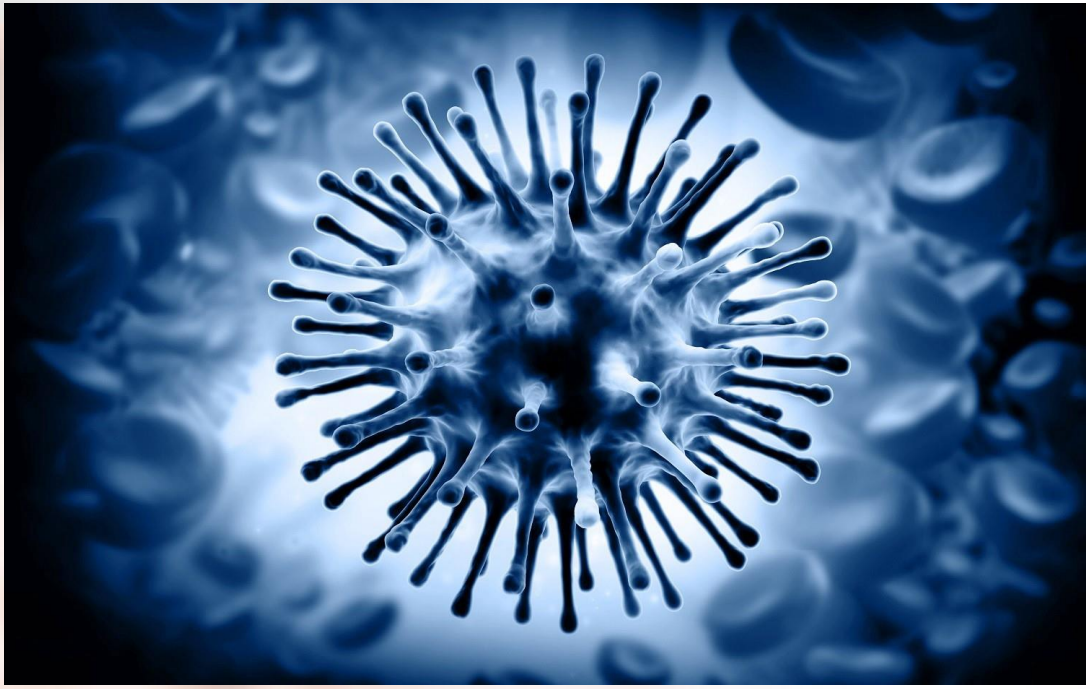
ZASADA ZWIĄZANIA CELEM

ZASADA MERYTORYCZNEJ POPRAWNOŚCI

ZASADA ADEKWATNOŚCI

ZASADA OGRANICZENIA CZASOWEGO

Urząd
Ochrony
Danych
Osobowych



https://cdn-images-1.medium.com/max/1600/1*4ssA7nMq9Sf4XND2SU5l4w.jpeg

Myxovirus influenzae

W RODO… pojęcie dane wrażliwe zastąpiono pojęciem dane osobowe szczególnej kategorii, oraz uzupełniono katalog dawnych danych wrażliwych o pojęcie danych dotyczących zdrowia ….

Art. 3

„dane dotyczące zdrowia” oznaczają dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;

Urząd Ochrony Danych Osobowych

ART. 9 UST.1 RODO

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej **lub danych dotyczących zdrowia,** seksualności lub orientacji seksualnej tej osoby.

Urząd Ochrony Danych Osobowych

Warunkowe przetwarzanie *szczególnych kategorii danych osobowych* (Art. 9 ust. 2) jest możliwe, jeśli:

.....

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, **zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia** społecznego na podstawie prawa UE lub prawa państwa członkowskiego, lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem **warunków i gwarancji,** określonych w rozporządzeniu;

.....

Urząd Ochrony Danych Osobowych

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

IDENTYFIKACJA RYZYKA PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

Urząd Ochrony Danych Osobowych

- **Kodeksy postępowania** (opracowanych np. dla danej branży, zaakceptowanych przez organy nadzoru).

- **Mechanizm certyfikacji** przez organ nadzoru lub akredytowane jednostki certyfikujące (akredytacji może udzielić organ nadzoru)

OBOWIĄZEK ZABEZPIECZENIA DANYCH OSOBOWYCH

Urząd Ochrony Danych Osobowych

- **Privacy by design** – obowiązek uwzględnienia ochrony danych osobowych w fazie projektowania
- **Privacy by default** – obowiązek wprowadzenia domyślnej ochrony danych osobowych
- Obowiązek dokonywania **oceny skutków** planowanych operacji przetwarzania danych

OBOWIĄZEK ZABEZPIECZENIA DANYCH OSOBOWYCH

Urząd Ochrony Danych Osobowych

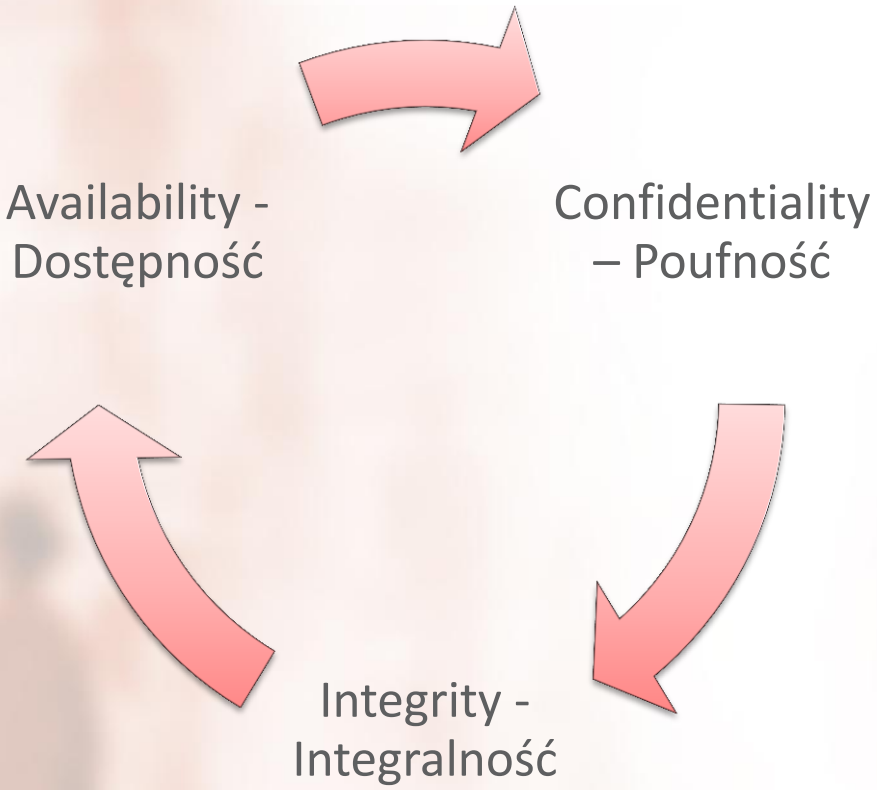
- Obowiązek stosowania odpowiednich środków organizacyjno-technicznych
- Dopuszczone do przetwarzania danych osobowych mogą być tylko osoby upoważnione
- Przy doborze środków administrator powinien uwzględniać najnowsze osiągnięcia techniczne oraz koszty wdrożenia tych środków
- Obowiązek przeprowadzenia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

Urząd Ochrony Danych Osobowych

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?


Availability -
Dostępność
Confidentiality
– Poufność
Integrity -
Integralność

Urząd Ochrony Danych Osobowych

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?

Urząd Ochrony Danych Osobowych

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

Urząd Ochrony Danych Osobowych

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.

Urząd Ochrony Danych Osobowych

OBOWIĄZKI DOKUMENTACYJNE RODO

- Polityki ochrony danych
- Rejestr czynności przetwarzania
- Naruszenia ochrony danych osobowych
- Ocena skutków dla ochrony danych
- Decyzja o niepowołaniu inspektora ochrony danych

Urząd Ochrony Danych Osobowych

REJESTR CZYNNOŚCI PRZETWARZANIA (ART. 30)

1. 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:

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

b) cele przetwarzania;

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

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

e) 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;

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

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

Urząd Ochrony Danych Osobowych

POLITYKI OCHRONY DANYCH (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

POLITYKA PRYWATNOŚCI

Przejrzystość i dostępność informacji dla osób o tym, jak przetwarzane są ich dane osobowe, jest kluczowym elementem RODO.

Jednym ze sposobów zachowania transparentności jest opracowanie i upublicznienie Polityki prywatności zawierającej kluczowe informacje umożliwiające skuteczną ochronę prywatności.

DECYZJA O NIEPOWOŁANIU INSPEKTORA OCHRONY DANYCH

Urząd Ochrony Danych Osobowych

- Niepowołanie IOD musi być udokumentowane
- Udokumentowanie oznacza uzasadnienie dlaczego IOD nie został wyznaczony

W sytuacji, gdy z przepisów nie wynika obowiązek wyznaczenia DPO, GR Art. 29 zaleca administratorom i podmiotom przetwarzającym udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia DPO, celem wykazania, iż stosowne czynniki zostały uwzględnione.

(Wytyczne dotyczące inspektorów ochrony danych (‘DPO’))

DOKUMENTACJA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH (ART. 33)

Urząd Ochrony Danych Osobowych

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

DOKUMENTACJA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH (ART. 33)

Urząd Ochrony Danych Osobowych

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Urząd Ochrony Danych Osobowych

OCENA SKUTKÓW DLA OCHRONY DANYCH (ART. 35)

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. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

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

Urząd Ochrony Danych Osobowych

Dziękuję za uwagę!

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@giodo.gov.pl