Urząd
Ochrony
Danych
Osobowych

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Andrzej Zieliński

Z-ca Dyrektora

Zespół ds. Organów Ścigania i Sądów

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

ATRYBUTY INFORMACJI

Atrybut	Definicja
Poufność	Zapewnienie, iż informacja jest dostępna wyłącznie dla osób uprawnionych, posiadających odpowiednie prawa dostępu.
Integralność	Śledzenie procesu przetwarzania informacji we wszystkich formach występowania, po to aby uniemożliwić nieautoryzowaną modyfikację czy też wyeliminować niepoprawną metodę przetwarzania.
Dostępność	Zapewnienie, iż informacja jest dostępna dla osoby uprawnionej zawsze gdy tego potrzebuje.

BEZPIECZEŃSTWO

Nadzór nad bezpieczeństwem informacji – **system**, za pomocą którego działania organizacji w zakresie bezpieczeństwa informacji są kierowane i kontrolowane (PN-ISO/IEC 2700)

Urząd Ochrony Danych Osobowych

BEZPIECZEŃSTWO

Aktywa – wszystko co ma wartość dla organizacji.

W kontekście przetwarzania danych osobowych:

- dane osobowe (niezależnie od formy przetwarzania),
- urządzenia,
- programy,
- procedury przetwarzania informacji zarządzania systemem informatycznym,
- narzędzia programowe stosowane w celu przetwarzania informacji,
- personel.

BEZPIECZEŃSTWO

Zagrożenie: potencjalna przyczyna incydentu, którego skutkiem może być szkoda dla systemu lub instytucji.

BEZPIECZEŃSTWO

Główne źródła zagrożeń

- **Osoba**
  - haker, craker,
  - terrorysta,
  - szpieg przemysłowy,
  - pracownik (źle wykształcony, nieuczciwy).
- **Zjawisko**
  - powódź,
  - burza,
  - pożar.

BEZPIECZEŃSTWO

Zabezpieczenie -wszystko to, co modyfikuje **ryzyko.**

BEZPIECZEŃSTWO

Podatność - słabość aktywów, która może być wykorzystana przez zagrożenie.

ZWIĄZKI W ZARZĄDZANIU BEZPIECZEŃSTWEM

Urząd Ochrony Danych Osobowych

WYMOGI W ZAKRESIE BEZPIECZEŃSTWA
UODO Z 29 SIERPNIA 1997 R./USTAWA Z 14 GRUDNIA 2018 R.

Art. 36 ust. 1 / Art. 39

Administrator danych jest obowiązany zastosować środki:

- techniczne
- organizacyjne

zapewniające ochronę przetwarzanych danych osobowych **odpowiednią** do **zagrożeń** oraz **kategorii danych** objętych ochroną.

WYMOGI W ZAKRESIE BEZPIECZEŃSTWA
RODO

Art. 32

Administrator danych wdraża **odpowiednie** środki:

- techniczne
- organizacyjne

aby zapewnić **stopień bezpieczeństwa odpowiadający** ryzyku naruszenia praw lub wolności osób fizycznych.

Urząd Ochrony Danych Osobowych

WYMOGI W ZAKRESIE BEZPIECZEŃSTWA
DYREKTYWA POLICYJNA

Art. 29

Administrator danych wdraża **odpowiednie** środki:

- techniczne
- organizacyjne

dla zagwarantowania **poziomu bezpieczeństwa odpowiadającego zagrożeniu**,

zwłaszcza jeżeli chodzi o przetwarzanie szczególnych kategorii danych osobowych

ŚRODKI BEZPIECZEŃSTWA
UODO Z 29 SIERPNIA 1997 R.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

ŚRODKI BEZPIECZEŃSTWA
RODO

- **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.

ŚRODKI BEZPIECZEŃSTWA
USTAWA Z 14 GRUDNIA 2018 R.

- kontrola dostępu do sprzętu
- kontrola nośników danych
- kontrola przechowywania
- kontrola użytkowników
- kontrola dostępu do danych
- kontrola przesyłu danych
- kontrola wprowadzania danych
- kontrola transportu
- odzyskiwanie
- niezawodność i integralność

Urząd Ochrony Danych Osobowych

WYBÓR I WDROŻENIE ODPOWIEDNICH ŚRODKÓW

USTAWA Z 14 GRUDNIA 2018 r. (art. 39)

Administrator i podmiot przetwarzający stosują środki techniczne i organizacyjne (…) które w szczególności mają na **celu** [….]

DODO (art. 29)

W odniesieniu do zautomatyzowanego przetwarzania każde państwo członkowskie zapewnia, by**) po ocenie ryzyka** administrator lub podmiot przetwarzający wdrożyli środki, które […]

WYBÓR I WDROŻENIE ODPOWIEDNICH ŚRODKÓW

RODO (art. 32)

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**.

Urząd Ochrony Danych Osobowych

ROZLICZALNOŚĆ

RODO (Art. 24)

AD wdraża odpowiednie środki techniczne i organizacyjne, aby:

- przetwarzanie odbywało się zgodnie z RODO
- **móc to wykazać.**

DODO (Art. 19)

AD wdraża odpowiednie środki techniczne i organizacyjne, aby:

- przetwarzanie odbywało się zgodnie z DODO,
- **móc to wykazać.**

PRZEGLĄDY I UAKTUALNIANIE ŚRODKÓW BEZPIECZEŃSTWA

RODO (art 24) / DODO (art. 19)

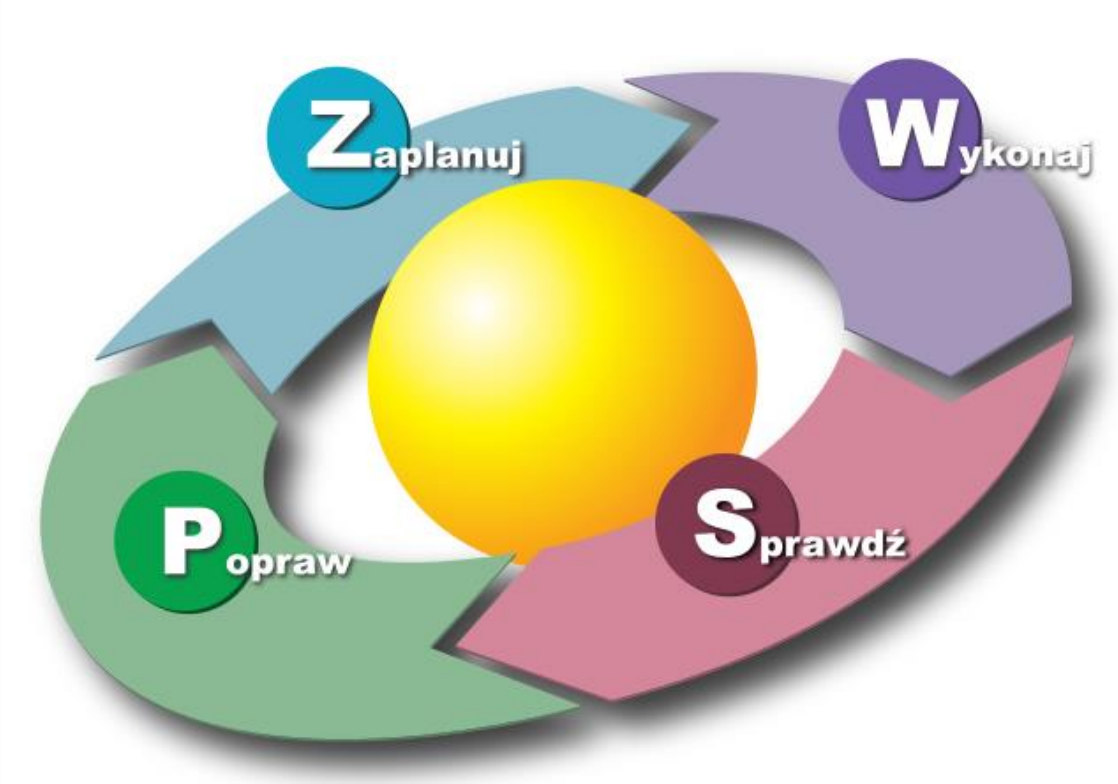
Odpowiednie środki techniczne i organizacyjne są w **razie potrzeby**:

- poddawane przeglądom,
- uaktualniane.

USTAWA Z 14 GRUDNIA 2018 R.

AD dokonuje **bieżącego przeglądu** środków, technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, pod kątem **potrzeby ich uaktualniania.**

PROCES ZARZĄDZANIA BEZPIECZEŃSTWEM



Urząd
Ochrony
Danych
Osobowych

KONTROLA DOSTĘPU DO SPRZĘTU

Uniemożliwienie osobom

nieuprawnionym dostępu do sprzętu

używanego do przetwarzania

Urząd
Ochrony
Danych
Osobowych

KONTROLA NOŚNIKÓW DANYCH

Zapobiegnięcie nieuprawnionemu

odczytywaniu, kopiowaniu,

zmienianiu lub usuwaniu nośników

danych

Urząd
Ochrony
Danych
Osobowych

KONTROLA PRZECHOWYWANIA

Zapobiegnięcie nieuprawnionemu

wprowadzaniu danych osobowych

oraz nieuprawnionemu oglądaniu,

zmienianiu lub usuwaniu

przechowywanych danych

osobowych

Urząd
Ochrony
Danych
Osobowych

KONTROLA UŻYTKOWNIKÓW

Zapobiegnięcie korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych.

Urząd Ochrony Danych Osobowych

KONTROLA DOSTĘPU DO DANYCH

Zapewnienie osobom, uprawnionym

do korzystania z systemu

zautomatyzowanego przetwarzania,

dostępu wyłącznie do danych

osobowych objętych posiadanym

przez siebie uprawnieniem

Urząd
Ochrony
Danych
Osobowych

KONTROLA PRZESYŁU DANYCH

Umożliwienie zweryfikowania i ustalenia podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione, za pomocą sprzętu do przesyłu danych

Urząd Ochrony Danych Osobowych

KONTROLA WPROWADZANIA DANYCH

Umożliwienie następczej weryfikacji

i ustalenia, które dane osobowe

zostały wprowadzone do systemów

zautomatyzowanego przetwarzania,

kiedy i przez kogo.

Urząd
Ochrony
Danych
Osobowych

KONTROLA TRANSPORTU

Zapobieżenie nieuprawnionemu

odczytywaniu, kopiowaniu,

zmienianiu lub usuwaniu danych

osobowych podczas ich

przekazywania lub podczas

przenoszenia nośników

Urząd
Ochrony
Danych
Osobowych

ODZYSKIWANIE

Zapewnienie przywrócenia

zainstalowanych systemów w razie

awarii

Urząd
Ochrony
Danych
Osobowych

NIEZAWODNOŚĆ I INTEGRALNOŚĆ

Zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu

Urząd Ochrony Danych Osobowych

ZABEZPIECZENIE DANYCH OSOBOWYCH

- DANE OSOBOWE W SPOCZYNKU
- DANE OSOBOWE W UŻYCIU
- DANE OSOBOWE W RUCHU

Urząd
Ochrony
Danych
Osobowych

POLITYKA OCHRONY

Administrator **opracowuje i wdraża** politykę ochrony danych, uwzględniając w niej sposób dokumentowania środków technicznych i organizacyjnych mających zapewnić, aby dane osobowe były przetwarzane zgodnie z prawem i rzetelnie.

Urząd
Ochrony
Danych
Osobowych

WYKAZ KATEGORII CZYNNOŚCI PRZETWARZANIA

1. Imię i nazwisko lub nazwę oraz dane kontaktowe:
   - administratora,
   - współadministratora,
   - inspektora ochrony danych,
   - **podmiotu przetwarzającego.**
2. Cele przetwarzania.
3. Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
4. Opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych.
5. **Informacje o stosowaniu profilowania - w przypadku gdy zostało ono zastosowane.**

WYKAZ KATEGORII CZYNNOŚCI PRZETWARZANIA

6. Kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej - w przypadku gdy przekazanie nastąpiło.
7. **Wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone.**
8. Planowane terminy usunięcia poszczególnych kategorii danych - jeżeli jest to możliwe.
9. Ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe.

EWIDENCJA OPERACJI PRZETWARZANIA PROWADZONYCH W ZAUTOMATYZOWANYCH SYSTEMACH PRZETWARZANIA (ART. 36)

<table>
<tr><th>Rodzaj operacji</th><th colspan="3">Rodzaj informacji.</th></tr>
<tr><td>Zbieranie</td><td></td><td rowspan="7">Data i godzina operacji</td><td rowspan="7">Uzasadnienie zasadności operacji (w ewidencji nie prowadzonej w sposób automatyczny)</td></tr>
<tr><td>Modyfikowanie</td><td></td></tr>
<tr><td>Przeglądanie</td><td>Tożsamość osoby, która przeglądała dane osobowe (w miarę możliwości).</td></tr>
<tr><td>Ujawnianie</td><td>Tożsamość osoby, która ujawniła dane osobowe (w miarę możliwości).</td></tr>
<tr><td>Przekazywanie</td><td>Tożsamość odbiorców (w miarę możliwości).</td></tr>
<tr><td>Łączenie</td><td></td></tr>
<tr><td>Usuwanie</td><td></td></tr>
</table>

EWIDENCJA OPERACJI PRZETWARZANIA PROWADZONYCH W ZAUTOMATYZOWANYCH SYSTEMACH PRZETWARZANIA (ART. 36)

Cele prowadzenia ewidencji:

- weryfikacja zgodności przetwarzania z prawem,
- monitorowanie własnej działalności,
- zapewnienie integralności i bezpieczeństwa danych osobowych,
- na potrzeby postępowania karnego.

Ewidencja jest udostępniana na żądanie Prezesowi UODO

Urząd Ochrony Danych Osobowych

OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH (ART. 37)

Jeżeli dany rodzaj przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele **może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności** osób fizycznych, administrator – **przed przetworzeniem danych osobowych** – dokonuje **oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.**

OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH (ART. 37)

Ocena zawiera:

- **ogólny** opis planowanych operacji przetwarzania danych osobowych,
- ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą,
- środki planowane w celu rozwiązania takiego ryzyka,
- zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych.

UPRZEDNIE KONSULTACJE(ART. 37)

- Ocena skutków planowanych operacji dla przetwarzania, wykaże, że przetwarzanie danych osobowych **powodowałoby wysokie ryzyko** naruszenia praw i wolności osób fizycznych **w razie niepodjęcia** przez administratora **środków w celu zminimalizowania tego ryzyka.**
- Dany rodzaj przetwarzania danych osobowych stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą.
- Operacja przetwarzania znajduje się w wykazie opublikowanym przez PUODO.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH (ART. 41)

- Upoważnienie do przetwarzania danych osobowych w ramach danej kategorii czynności przetwarzania.
- Zatwierdzony przez AD wniosek o nadanie **uprawnień do dostępu do danych** osobowych w ramach danej kategorii czynności.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH (ART. 41)

Wniosek zawiera:

- imię i nazwisko, stanowisko, miejsce zatrudnienia osoby, której wniosek dotyczy,
- zakres i czasookres dostępu do danych osobowych,
- rodzaj danych osobowych i sposób ich przetwarzania.

Załącznik do wniosku:

oświadczenie osoby, której wniosek dotyczy, o zobowiązaniu się do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

EWIDENCJA OSÓB UPOWAŻNIONYCH (ART. 42)

- imię i nazwisko osoby upoważnionej,
- datę udzielenia i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie teleinformatycznym.

EWIDENCJA OSÓB UPOWAŻNIONYCH (ART. 42)

Role ewidencji może pełnić:

wykaz osób uprawnionych, prowadzony na podstawie zatwierdzonych przez administratora lub podmiot przetwarzający wniosków o nadanie uprawnień do dostępu do zbioru danych.

Urząd
Ochrony
Danych
Osobowych

DZIĘKUJĘ ZA UWAGĘ

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