Jak stworzyć sprawny system ochrony danych osobowych?

Łukasz Zegarek,
ekspert ds. ochrony danych osobowych

INFOR | WIDE AKADEMIA

Dlaczego stworzyć System ODO?

- obowiązek: ustawa, umowy
- bezpieczeństwo faktyczne
- pozytywny wizerunek
- oszczędności – zwłaszcza po 2018 roku! Zmiana przepisów UE

INFOR | WIDEO AKADEMIA

Podstawowe pojęcia związane z ochroną danych osobowych

INFOR | WIDE AKADEMIA

Dane osobowe (art. 6 UODO)

informacje określające cechy fizyczne, fizjologiczne, (…) społeczne i nie tylko

Katalog otwarty

Bez nadmiernych kosztów, czasu lub działań

Łatwa identyfikacja

Wszelkie informacje

Bardzo szerokie pojęcie

Cel

Czy celem jest identyfikacja?

Osoby fizyczne

Wyłącznie

INFOR | WIDEO AKADEMIA

Dane wrażliwe (art. 27 UODO)

Pochodzenie rasowe lub etniczne

Wyroki , orzeczenia o ukaraniu i mandatach karnych oraz inne wydane w postępowaniu sadowym lub administracyjnym

Przynależność wyznaniowa, partyjna lub związkowa

Nałogi, stan zdrowia, kod genetyczny lub życie seksualne

Przekonania religijne lub filozoficzne

Poglądy polityczne

INFOR | WIDEO AKADEMIA

V filarów ochrony danych osobowych

I Legalność przetwarzania

II Świadomość

III Zabezpieczenia

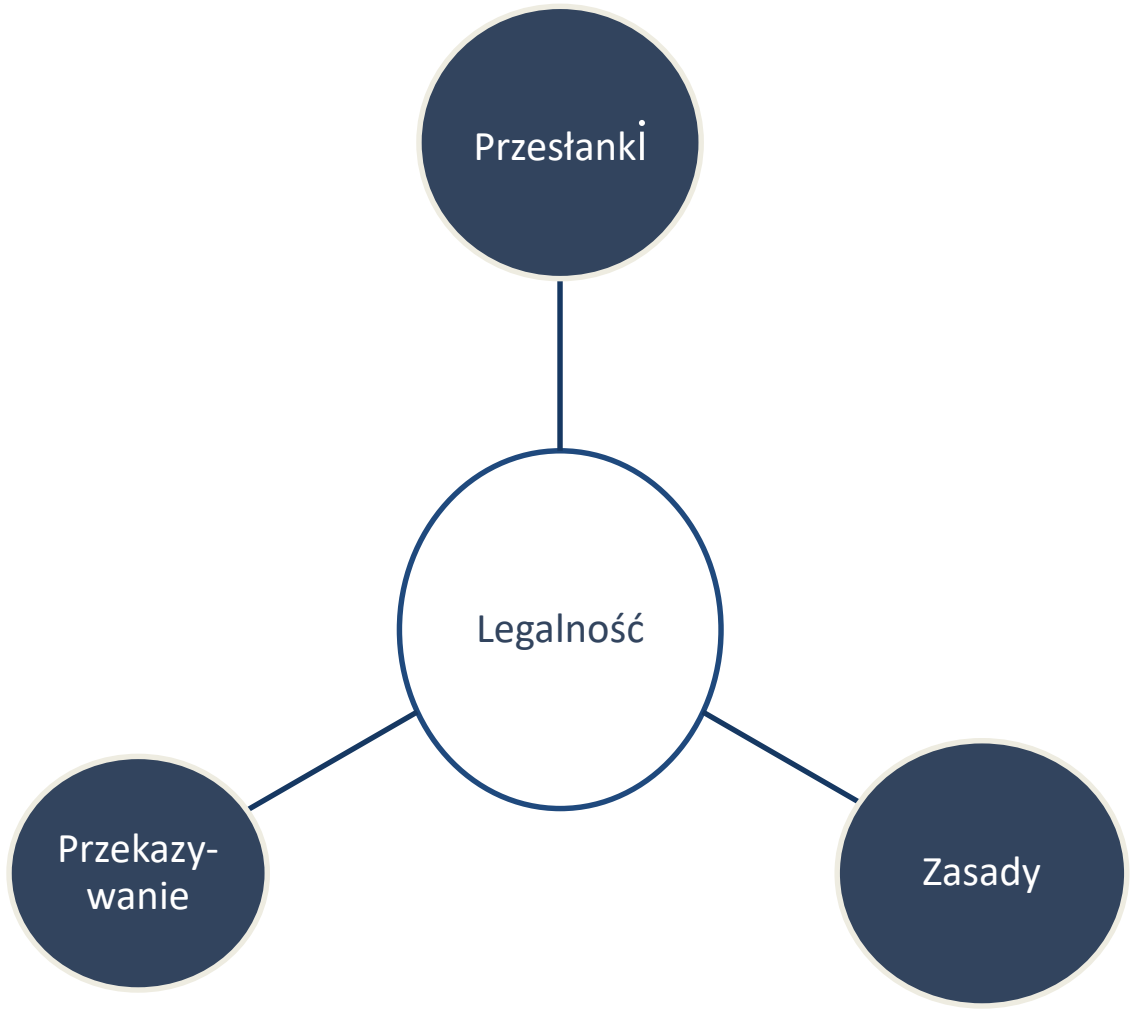
IV Rejestracja zbiorów do GIODO

V Obowiązek informacyjny

INFOR | WIDEO AKADEMIA

I Filar – Legalność przetwarzania

INFOR | WIDE AKADEMIA



INFOR | WIDE AKADEMIA

Zasady przetwarzania danych osobowych

Zasada adekwatności

- Adekwatność danych w stosunku do celów, w jakich są przetwarzane.

Zasada celowości

- Zbieranie danych dla oznaczonych celów.

Zasada ograniczenia czasowego

- Nie należy przechowywać danych dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Uwaga na CV!

INFOR | WIDEO AKADEMIA

Przesłanki legalności przetwarzania danych zwykłych (art. 23 uodo)

Zgoda

Przepis prawa

Realizacja umowy

Dobro publiczne

Prawnie uspr. cel

INFOR AKADEMIA

Przekazywanie danych

Przekazywanie danych = powierzenie / udostępnienie

- Powierzenie = wypożyczenie danych. Podmiot który dane otrzymał (tzw. Procesor) **nie staje** się ich ADO
- Udostępnienie = podzielenie się danymi. Podmiot który dane otrzymał **staje się** ich ADO i ponosi pełną odpowiedzialność

Przekazywanie poza granice Polski

- Bezpieczne – w ramach EOG. Wymogi jak przy przekazywaniu danych w Polsce. **Przykład**: Rumunia
- Do Państwa trzeciego – poza EOG. UWAGA! Dodatkowe warunki! **Przykład**: Rosja, Ukraina, USA, Chiny, Bangladesz

Przekazywanie danych

Co legalizuje powierzenie / udostępnienie

- Powierzenie – pisemna umowa powierzenia
- Udostępnienie – jedna z przesłanek legalności

Przykłady powierzenia / udostępnienia

- Powierzenie – outsourcingi: marketing, obsługa kadr/płac/księgowości, IT, ochrona, niszczenie/przechowywanie dokumentów
- Udostępnianie – policja, sąd, komornik, bank, ubezpieczenie, usługi medyczne, benefity

II Filar – Świadomość

INFOR | WIDE AKADEMIA

Czy szkolić?

Obowiązek:

- zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

- nadzorowania przestrzegania zasad określonych w dokumentacji

INFOR | WIDEO AKADEMIA

Wnioski

Dostęp do danych = upoważnienie

- **Każdy** pracownik posiadający dostęp do zbioru danych osobowych musi posiadać upoważnienie

Upoważnienie = szkolenie

- **Każdy** pracownik posiadający upoważnienie, musi zostać przeszkolony
- Szczególnie rekomendowane przeszkolenie pracowników: marketingu, kadr, płac, księgowości, IT

INFOR | WIDEO AKADEMIA

III Filar – Zabezpieczenia

INFOR | WIDE AKADEMIA

Zabezpieczenia fizyczne

Szafy zamykane na klucz	Drzwi zamykane na klucz	Monitoring
Ochrona	Kraty w oknach	SKD

INFOR | WIDEO AKADEMIA

Zabezpieczenia techniczne

1 użytkownik = 1 login i 1 hasło	Zmiana haseł co 30 dni	Hasła min. 8 znaków w tym 2 znaki specjalne
Kopie zapasowe	Systemy firewall i anti-vir	… Rozporządzenie MSWiA z 2004 r.

INFOR | WIDEO AKADEMIA

Zabezpieczenia organizacyjne

Stworzenie Polityki Bezpieczeństwa

Stworzenie Instrukcji Zarządzania Systemami Informatycznymi

Nadawanie i ewidencjonowanie upoważnień

Stworzenie struktury SODO

INFOR | WIDEO AKADEMIA

IV Filar – Rejestracja zbiorów do GIODO

INFOR | WIDE AKADEMIA

Obowiązek rejestracyjny

O czym pamiętać?

- Większość zbiorów danych osobowych powinna zostać zarejestrowana na www.egiodo.giodo.gov.pl

INFOR | WIDEO AKADEMIA

V Filar – Obowiązek Informacyjny

INFOR | WIDE AKADEMIA

Obowiązek informacyjny – art. 24 UODO

- adres i pełna nazwa ADO
- cel zbierania danych
- odbiorcy danych (lub kategorie odbiorców)
- prawo dostępu do treści danych oraz możliwość ich poprawiania
- dobrowolność albo obowiązek podania danych

INFOR | WIDEO AKADEMIA

Obowiązek informacyjny w praktyce

Kiedy zachować szczególną uwagę?

- Udostępnianie danych osobowych poza Spółkę
- Monitoring
- Akcje marketingowe
- Ciche rekrutacje

Kiedy jesteśmy zwolnieni z obowiązku informacyjnego?

- Kiedy osoba której dane dotyczą posiada już wszystkie te informacje
- Jeśli powierzamy dane osobowe

INFOR | WIDEO AKADEMIA