Wprowadzenie do RODO

Dr Jarosław Greser

1 Nowa filozofia przepisów o ochronie danych osobowych

2 Nowe struktury na poziomie urzędów

3 Nowe struktury na poziomie zarządzania danymi osobowymi w organizacji

4 Jak przygotować procedury (ocena ryzyka)

Nowa filozofia przepisów o ochronie danych osobowych

Było

Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.
w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. WE L 281).

Będzie

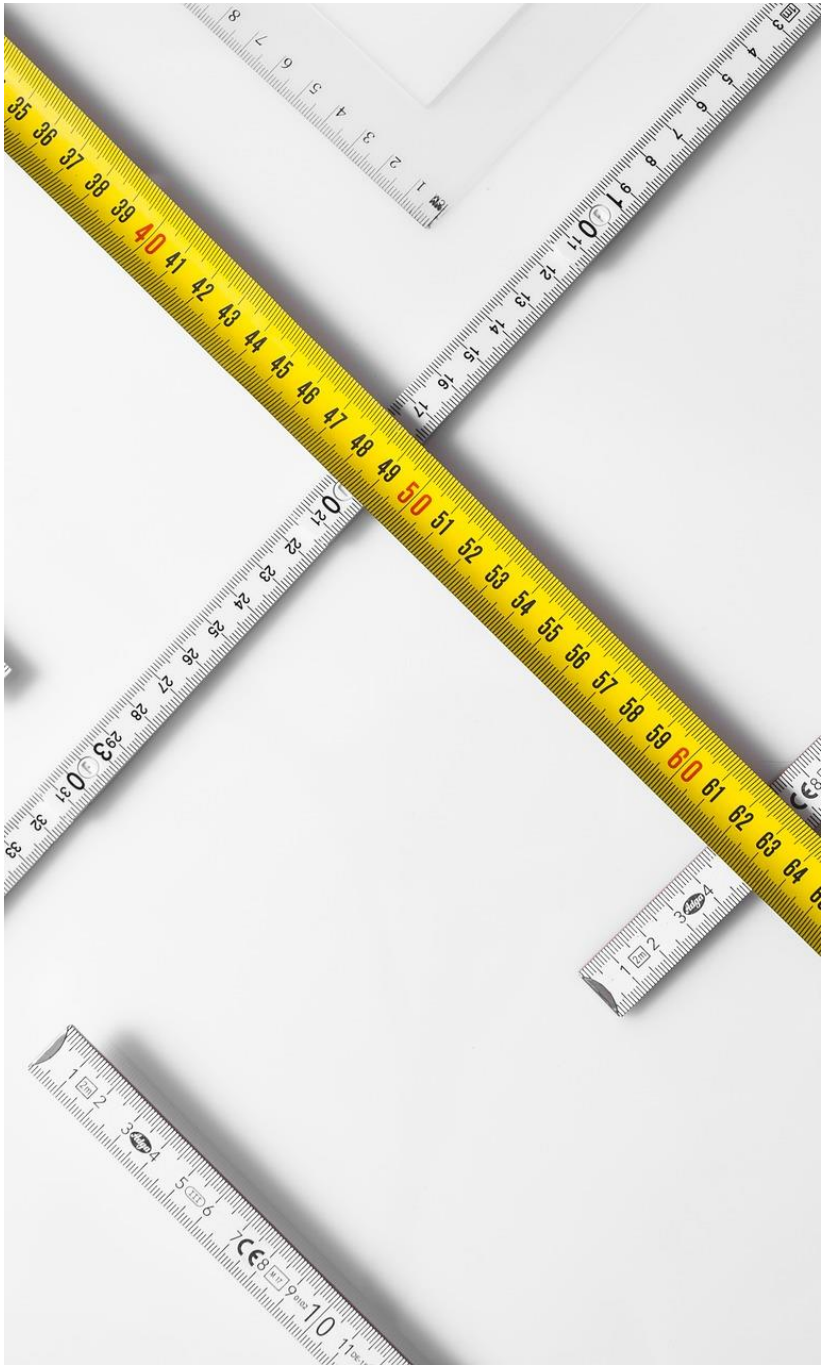
Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w skrócie: RODO).

Czym jest RODO?

Akt prawny stosowany bezpośrednio – wywołuje natychmiastowe skutki prawne od momentu wejścia w życie na poziomie zarówno Unii Europejskiej, jak i państw członkowskich.

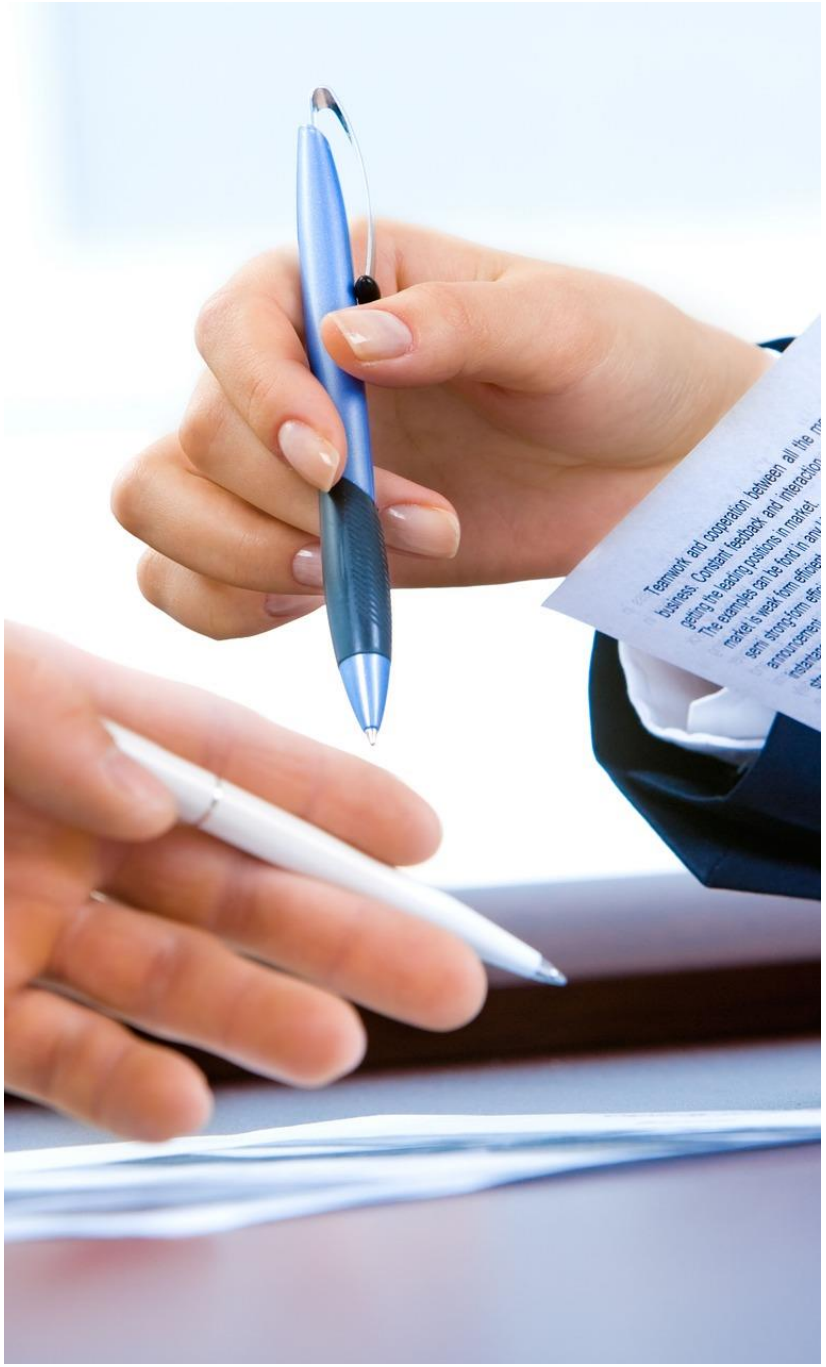
Ma pierwszeństwo
w wypadku kolizji
z prawem krajowym
(art. 91 ust. 3
Konstytucji).


Filozofia RODO



RODO odchodzi
od sztywno
wyznaczonych zasad
postępowania
na rzecz podejścia
opartego na ryzyku
(*risk based approach).*

Co to oznacza w praktyce?



W uproszczeniu:

po wejściu w życie RODO nie ma listy obowiązkowych dokumentów, procedur.

Organizacja musi sama je wymyśleć i wdrożyć.

Jeśli analiza przeprowadzona w organizacji potwierdzi, że przyjęte już w organizacji systemy ochrony czy dokumenty są wystarczające do ochrony przetwarzanych danych, z powodzeniem można je zaadaptować do wymogów RODO.

Nowe struktury na poziomie urzędów

1

Likwidacja Generalnego Inspektora Ochrony Danych Osobowych.

2

Nowy organ – Prezes Urzędu Ochrony Danych Osobowych.

3

Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. Jest również organem nadzorczym.

Nowe struktury na poziomie zarządzania danymi osobowymi w organizacji

1

Likwidacja stanowiska Administratora Bezpieczeństwa Informacji.

2

Osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, pełnią funkcję inspektora ochrony danych do dnia 1 września 2018 r.

3

Administrator lub podmiot przetwarzający zawiadamiają Prezesa Urzędu o wyznaczeniu inspektora ochrony danych osobowych, albo że administrator bezpieczeństwa informacji nie pełni funkcji inspektora ochrony danych.

4

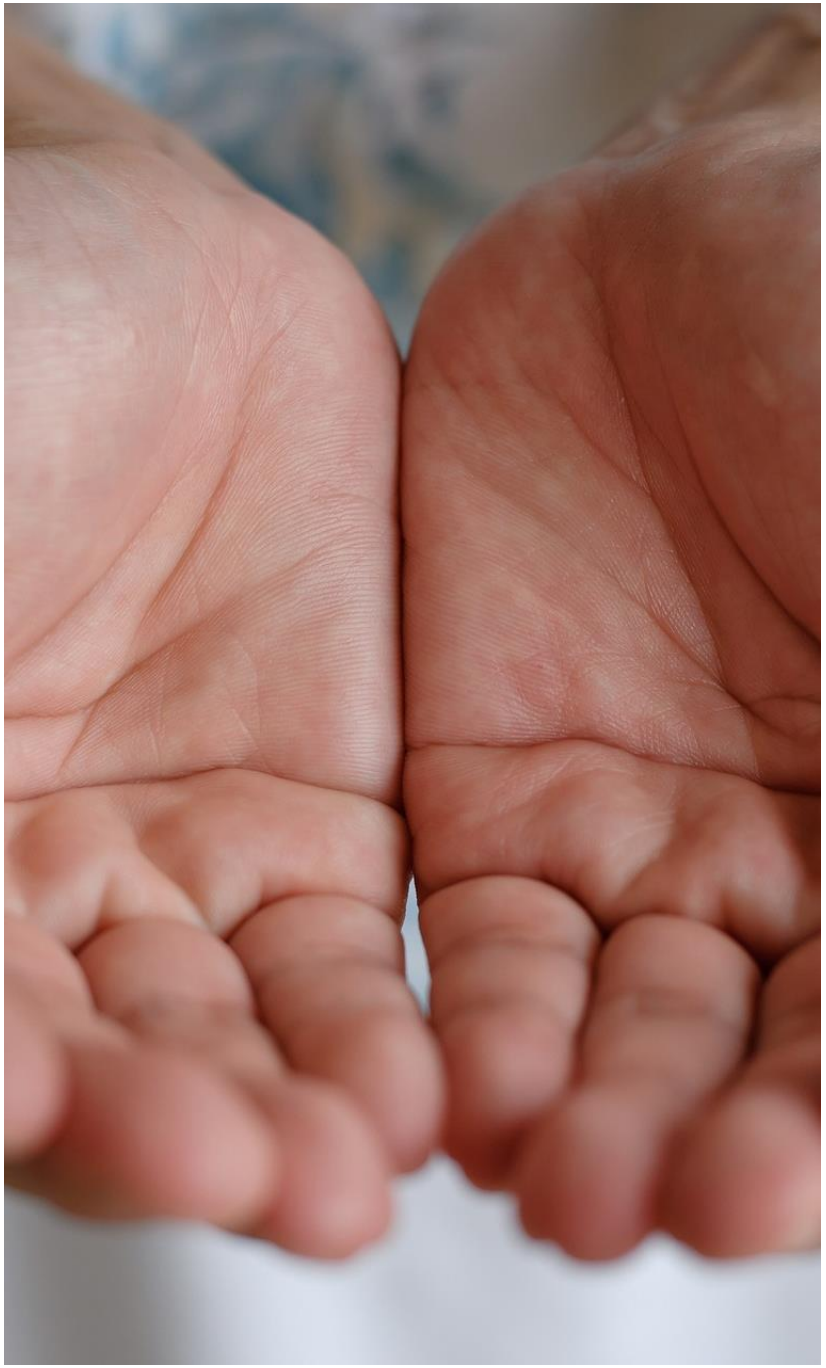
Rejestracja zbiorów danych osobowych zostanie zlikwidowana.

- 5

Dane zgromadzone w rejestrze GIODO Prezes Urzędu przechowuje przez okres
3 lat od dnia wejścia w życie niniejszej ustawy.

Jak przygotować procedury?

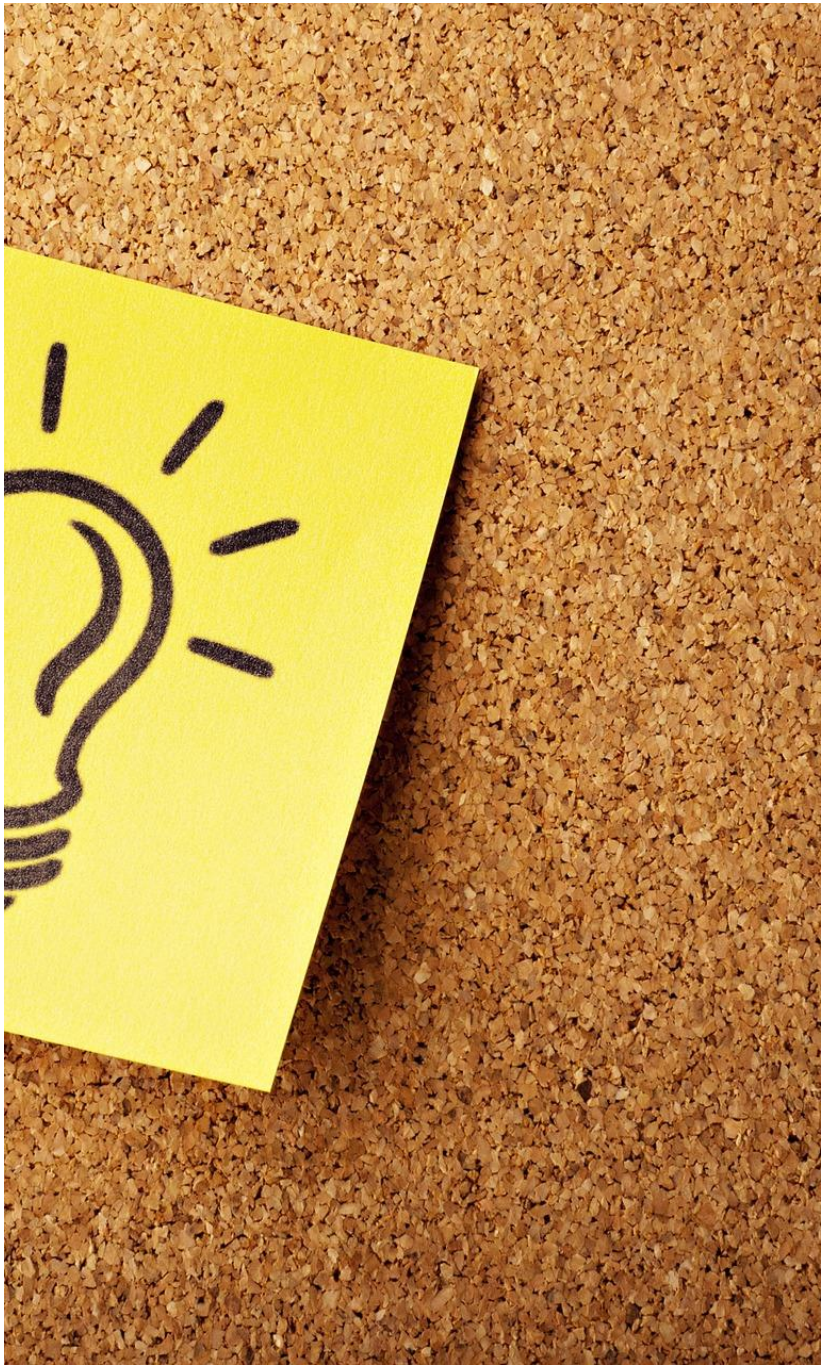
Analiza ryzyka zastępuje obligatoryjną listę dokumentów i procedur.



Wielkość organizacji lub prowadzenie działalności gospodarczej nie mają znaczenia dla zwolnienia fundacji czy stowarzyszenia z tego obowiązku.

Nie jest wymagana żadna szczególna forma.

Dozwolone jest korzystanie z dowolnej metodologii, o ile da się wykazać, że pozwala ona na rzetelną ocenę ryzyka.



Przykładowa metodologia:

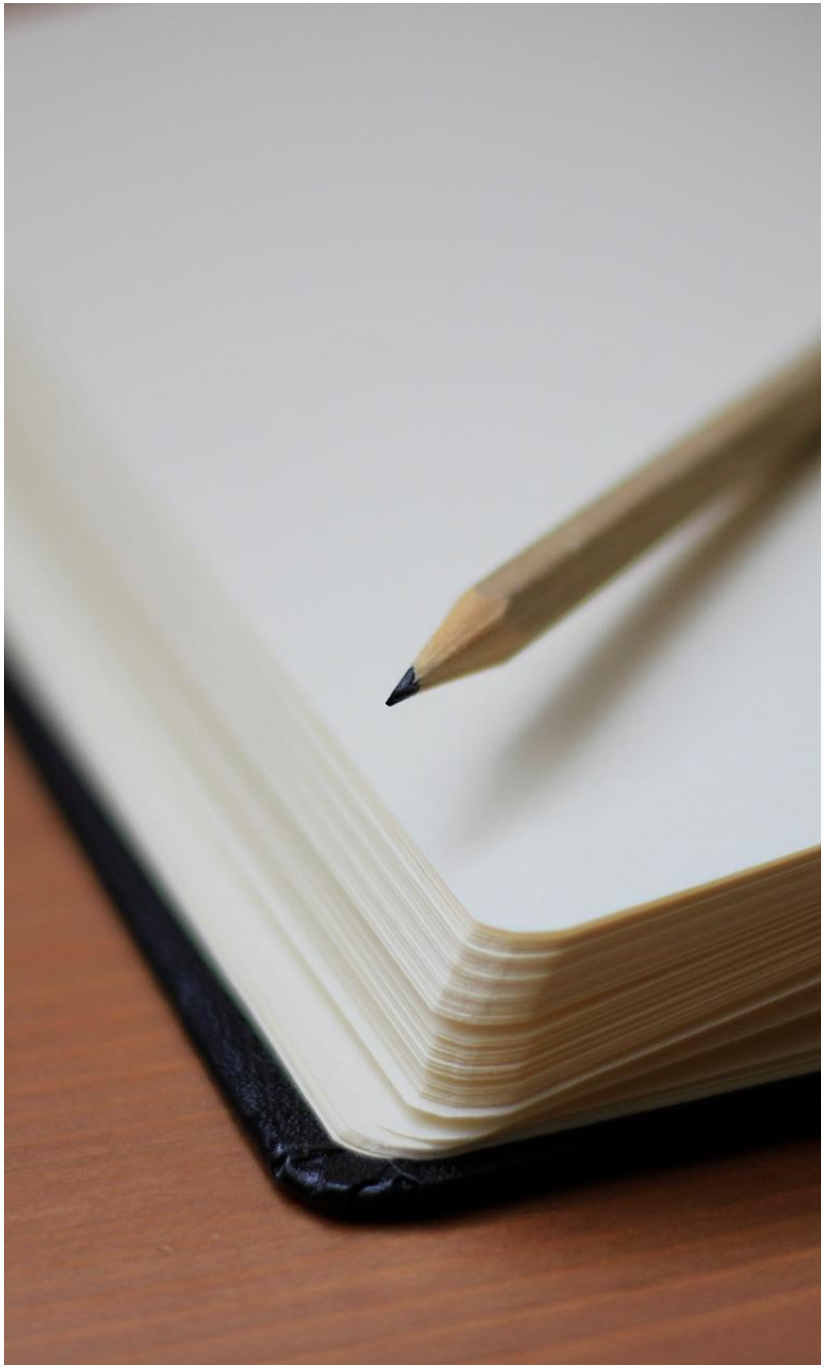
ISO/IEC 27002 – Praktyczne zasady zabezpieczania informacji.

Wskazówki GIODO

Cztery etapy oceny ryzyka:

1. kontekst dla oceny ryzyka,
2. opis i identyfikacja wymagań prawnych i techniczno-organizacyjnych,
3. szacowanie i ocena ryzyka,
4. postępowanie z ryzkiem.

„Jak stosować podejście oparte na ryzyku, część 2”
(https://giodo.gov.pl/pl/p/opinie-wytyczne-wskazówki)



- Efekt – odpowiednie środki techniczne i organizacyjne.
- Analiza ryzyka powinna mieć formę pisemną.
- Tryb stworzenia i przyjęcia zależy od wewnętrznych uregulowań w organizacji.

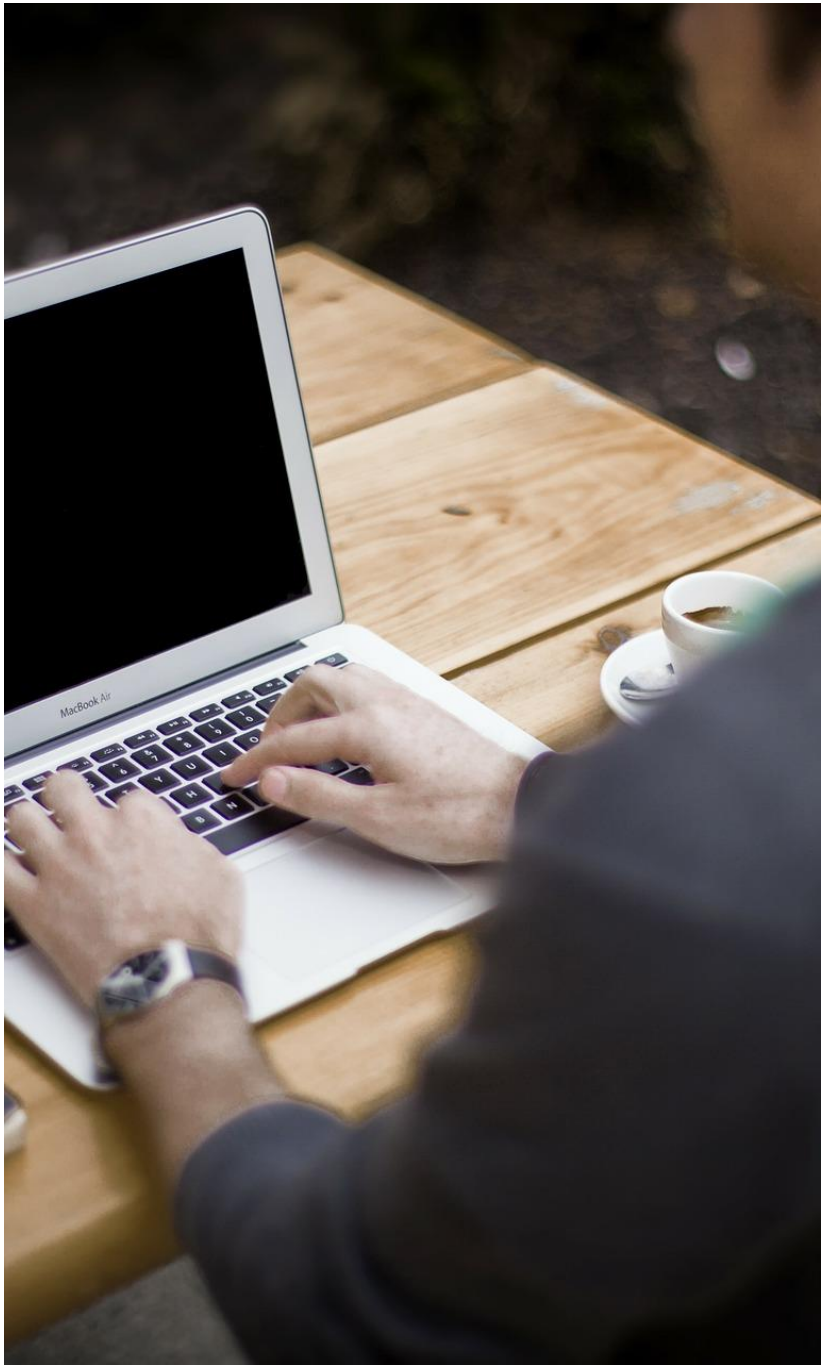
Kontekst
dla oceny ryzyka

Kontekst obejmuje charakter, zakres i cele przetwarzania danych osobowych.

Przykład:

Stowarzyszenie zbiera dane w celu wsparcia osób niepełnosprawnych
vs. oferowania produktów, od sprzedaży których uzyskuje prowizje.

Opis i identyfikacja wymagań



Przy pomocy jakich środków te dane są przetwarzane?

Przykład: Google Docs – przetwarzanie danych w chmurze.

Czy dane te są przetwarzane zgodnie z prawem?

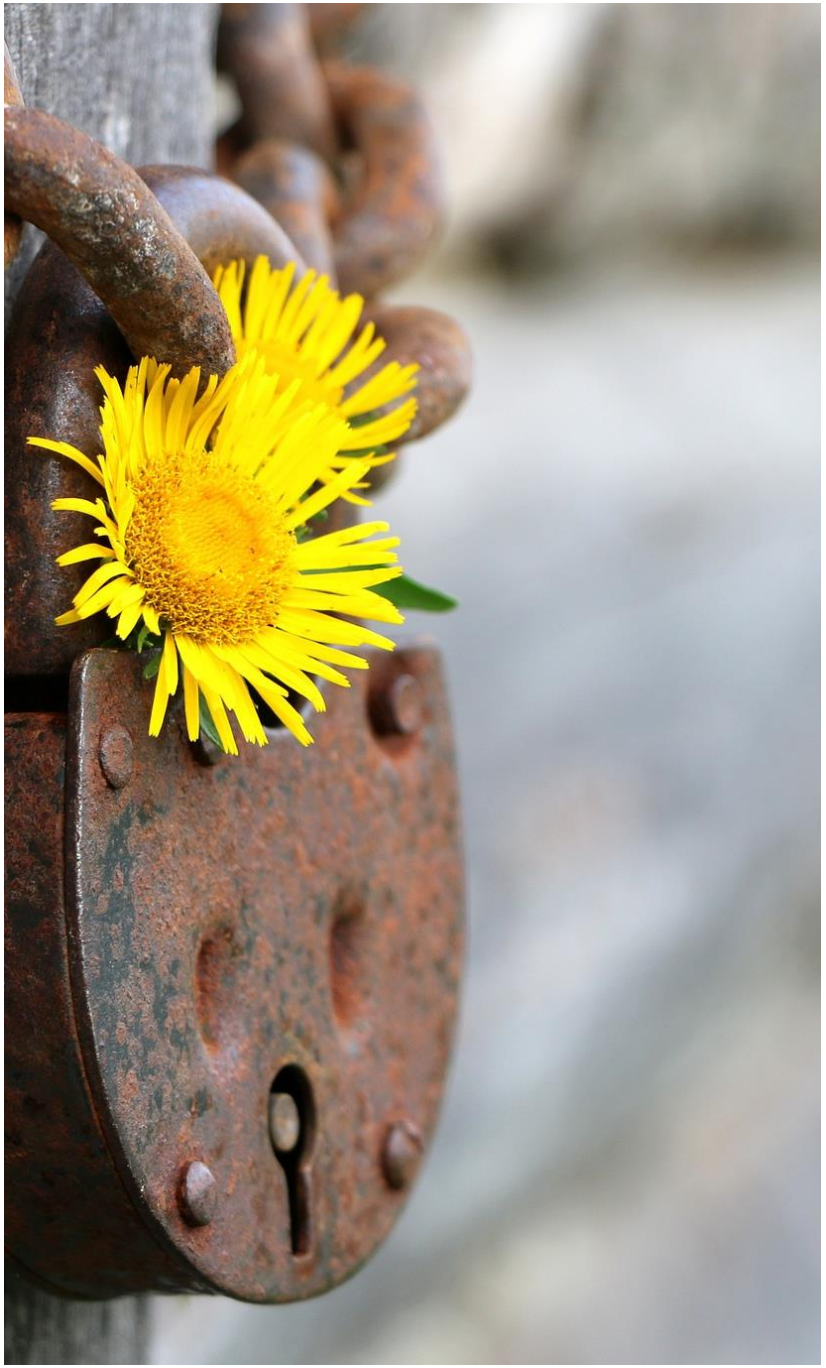
Przykład: skontrolowanie czy zgody na przetwarzanie danych osobowych były zebrane prawidłowo.

Szacowanie i ocena ryzyka

Oszacowanie prawdopodobieństwa wystąpienia zdarzenia naruszającego prawa osób, których dane są przetwarzane oraz określenie istotności efektów takiego zdarzenia.

Przykład: zgubienie pen drive'a z danymi osobowymi – prawdopodobieństwo niskie, efekt zdarzenia – duże zagrożenie naruszenia praw i wolności osób, których dane dotyczą.

Wybór formy postępowania z ryzykiem



- Obniżenie poziomu ryzyka
- Unikanie ryzyka
- Akceptacja ryzyka

Przykład: sporządzenie klauzul umownych zakazujących kopiowania danych na dyski przenośne, konfiguracja systemu uniemożliwiająca zapis takich danych.

Wskazówki GIODO

Art. 32 ust. 1 wskazuje działania, które mogą być podjęte dla minimalizowania ryzyka. Są to:

1. pseudonimizacja i szyfrowanie danych osobowych;

Wskazówki GIODO

Art. 32 ust. 1 wskazuje działania, które mogą być podjęte dla minimalizowania ryzyka. Są to:

1. pseudonimizacja i szyfrowanie danych osobowych;
2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (np. zasilanie awaryjne serwerów);

Wskazówki GIODO

Art. 32 ust. 1 wskazuje działania, które mogą być podjęte dla minimalizowania ryzyka. Są to:

1. pseudonimizacja i szyfrowanie danych osobowych;
2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (np. zasilanie awaryjne serwerów);
3. zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego /technicznego (np. posiadanie kopii zapasowych);

Wskazówki GIODO

Art. 32 ust. 1 wskazuje działania, które mogą być podjęte dla minimalizowania ryzyka. Są to:

1. pseudonimizacja i szyfrowanie danych osobowych;
2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (np. zasilanie awaryjne serwerów);
3. zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego /technicznego (np. posiadanie kopii zapasowych);
4. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (np. robienie niezapowiedzianych testów bezpieczeństwa).

Wybierając środki minimalizacji ryzyka trzeba uwzględnić:

- stan wiedzy technicznej

  (Przykład: rozwiązania o charakterze innowacyjnym muszą podlegać szczególnie wnikliwej ocenie)

- koszt wdrażania

  (Przykład: jest to przesłanka subiektywna w zakresie realnych możliwości organizacji)

Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA)

Jeśli analiza przeprowadzona w organizacji potwierdzi, że przyjęte systemy ochrony czy dokumenty są wystarczające do ochrony przetwarzanych danych, z powodzeniem można je zaadaptować wymogów RODO.

Pomocne narzędzia

Nowa filozofia w ochronie danych osobowych: Od Oceny Ryzyka Do Spójnej Strategii W Organizacji, opracowała Katarzyna Szymielewicz, Fundacja Panoptykon, 2017

Jak stosować podejście oparte na ryzyku, cz. 1 i cz. 2, Generalny Inspektor Ochrony Danych Osobowych, 2017