Urząd Ochrony Danych Osobowych

Analiza ryzyka a ocena skutków dla ochrony danych

Michał Mazur

Zespół Współpracy z Administratorami Danych
Urząd Ochrony Danych Osobowych

Warszawa, 19.12.2018 r.

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

Bezpieczeństwo odpowiednie do ryzyka
Analiza ryzyka i ocena skutków dla ochrony danych

Urząd Ochrony Danych Osobowych

UODO - Analiza ryzyka

Art. 36 UODO

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (…).

+ Art. 39a - rozporządzenie wykonawcze

Ustawodawca „wyręczał" administratora

RODO - Analiza ryzyka

Art. 24 i 32 RODO

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator (i podmiot przetwarzający) wdrażają odpowiednie środki techniczne i organizacyjne (…)

Administrator i podmiot prz. oceniają sami

Postać „kwalifikowana" analizy ryzyka
Ocena skutków dla ochrony danych

Art. 35 RODO

- ✓ **Przed rozpoczęciem przetwarzania**
- ✓ **Gdy ryzyko jest wysokie**

Art. 36 RODO

Uprzednie konsultacje z organem nadzorczym

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- **stan wiedzy technicznej,**
- **koszt wdrażania**
- **oraz charakter,**
- **zakres,**
- **kontekst**
- **i cele przetwarzania**
- **oraz ryzyko naruszenia praw lub wolności osób fizycznych**
- **o różnym prawdopodobieństwie wystąpienia**
- **i wadze,**
- **administrator i podmiot przetwarzający wdrażają**
- **odpowiednie środki techniczne i organizacyjne**

w tym między innymi (…)

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Adm. zarówno przy określaniu sposób przetwarzania, jak i w jego czasie wdraża odpowiednie środki techniczne i organizacyjne

Uwzględniając:

Patrz też art. 25

- **stan wiedzy technicznej**
- Standardy i normy (np. z serii ISO/IEC 27001) – które ulegają ciągłym przeglądom i zmianom uwarunkowanym postępem technologicznym. Normy te bazują na podstawowych wartościach informacji tj. poufności, integralności i dostępności.
- Analizy i materiały opracowywane przez zaufane podmioty (opracowania innych organów nadzorczych, opracowania Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, czy zalecenia konfiguracyjne, przewodniki zabezpieczeń dostępne na cert.gov.pl).
- Korzystanie z wiedzy specjalistów
- Rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych publikowane przez Prezesa UODO (art. 53 ust. 1 pkt. 4 ustawy o ochronie danych osobowych)

Przykład: Obecnie w kryptografii przyjmuje się, że od wielu lat szyfrowanie DES (w swojej podstawowej formie) obecnie nie zapewnia wysokiego poziomu bezpieczeństwa z uwagi na długość klucza i o wiele większą moc obliczeniową dzisiejszych komputerów.

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- stan wiedzy technicznej,
- **koszt wdrażania,**

- **Wyrok NSA 4 marca 2002 r. (II SA 3144/01)**
  Żadne względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych.
- Administrator sygnalizował „trudności w utworzeniu dwóch odrębnych zbiorów - aktualnych i archiwalnych oraz niewielki wpływ tej kosztownej i długotrwałej operacji na polepszenie ochrony danych osobowych osób fizycznych”.

- **Istnieje korelacja pomiędzy akceptowalnymi kosztami a ryzykiem.**
  Im większe jest stwierdzane ryzyko, tym większe mogą być adekwatne koszty wdrożenia środków technicznych i organizacyjnych zapewniających odpowiedni poziom ochrony.

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- **stan wiedzy technicznej,**
- **koszt wdrażania,**
- **oraz charakter,**

Planowane operacje przetwarzania (art. 4 pkt 2 RODO) jak i rodzaj danych osobowych, które będą przetwarzane, np. czy przetwarzane będą szczególne kategorie danych, np. dane dotyczące zdrowia.

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- stan wiedzy technicznej,
- koszt wdrażania,
- oraz charakter,
- **zakres**

Wszystkie aspekty ilościowe przetwarzania:

- zakres kategorii danych
- ilość przetwarzanych danych
- liczba podmiotów, których dotyczy przetwarzanie danych

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- stan wiedzy technicznej,
- koszt wdrażania,
- oraz charakter,
- zakres,
- **kontekst**

Wszelkie okoliczności prawne i faktyczne przetwarzania
(więcej o kontekście również przy ocenie skutków dla ochrony danych)

Należy oceniać intensywność ingerencji w prywatność danego procesu przetwarzania danych, np. związanego z monitoringiem, przyjęte rozwiązania techniczne, okoliczności i sposób wykorzystywania założonego rozwiązania i relacji do pozostałych elementów ocennych, w tym celu przetwarzania, a także przesłanek legalizacyjnych. Istotny może być również czas przetwarzania.

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- stan wiedzy technicznej,
- koszt wdrażania,
- oraz charakter,
- zakres,
- kontekst
- **i cele przetwarzania**

Bezpośrednio związane z realizacją zasady ograniczenia celu (art. 5 ust. 1 lit. b),

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- stan wiedzy technicznej,
- koszt wdrażania,
- oraz charakter,
- zakres,
- kontekst
- i cele przetwarzania
- **oraz ryzyko naruszenia praw lub wolności osób fizycznych**

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- (…)
- **oraz ryzyko naruszenia praw lub wolności osób fizycznych**

Pomocnymi w wyjaśnieniach mogą być motywy:

Motyw 75 (naruszenie praw lub wolności):

- Sytuacje zagrożenia dla praw lub wolności osób, których dane dotyczą:
  - Szkoda,
  - Utrata praw lub kontroli,
  - Dane szczególnej kategorii,
  - Profilowanie,
  - Osoby wymagające szczególnej opieki (w szczególności dzieci),
  - Duża skala

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 2 RODO i motyw 83

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności:

- Ryzyko związane z przetwarzaniem danych osobowych:
  - Przypadkowe lub niezgodne z prawem zniszczenie,
  - Utracenie,
  - Zmodyfikowanie,
  - Nieuprawnione ujawnienie,
  - Nieuprawniony dostęp do danych osobowych:

  przesyłanych, przechowywanych lub w inny sposób przetwarzanych i mogących w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych (motyw 75)

Bezpieczeństwo odpowiednie do ryzyka

Urząd Ochrony Danych Osobowych

Art. 32 ust 1 RODO

Uwzględniając:

- **stan wiedzy technicznej,**
- **koszt wdrażania**
- **oraz charakter,**
- **zakres,**
- **kontekst**
- **i cele przetwarzania**
- **oraz ryzyko naruszenia praw lub wolności osób fizycznych**
- **o różnym prawdopodobieństwie wystąpienia**
- **i wadze,**
- **administrator i podmiot przetwarzający wdrażają**
- **odpowiednie środki techniczne i organizacyjne**

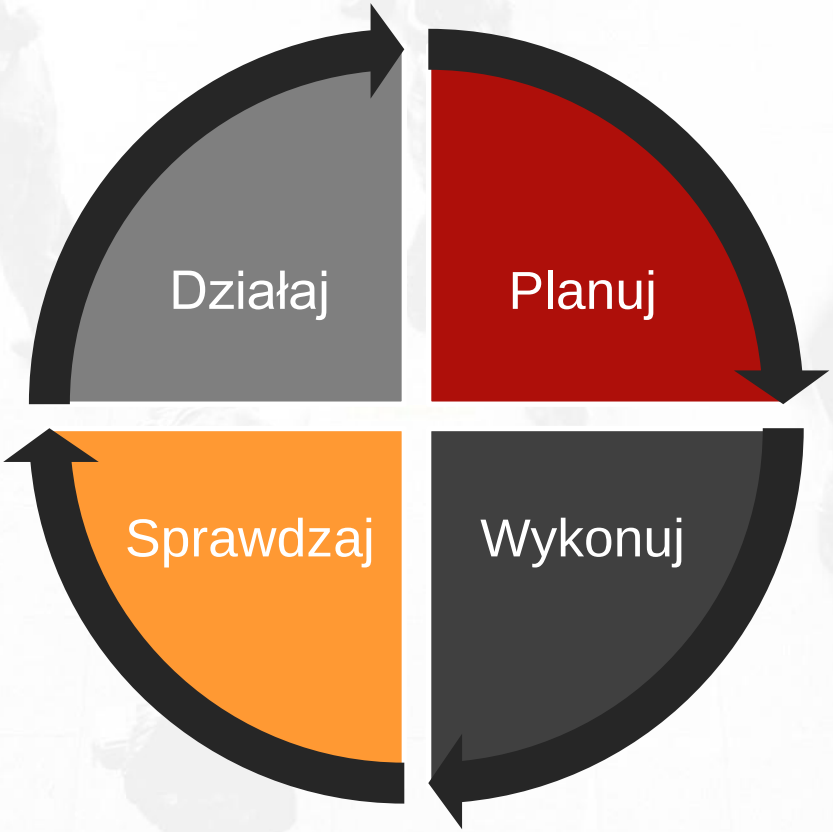
w tym między innymi (…)

Środki bezpieczeństwa w RODO

Urząd Ochrony Danych Osobowych

- Pseudonimizacja i szyfrowanie danych osobowych
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odproności systemów przetwarzania i usług (cyberbezpieczeństwo)
- Zdolność do szybkiego przywrócenia dostępności danych danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego – ciągłość działania
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Ochrona danych osobowych to proces…

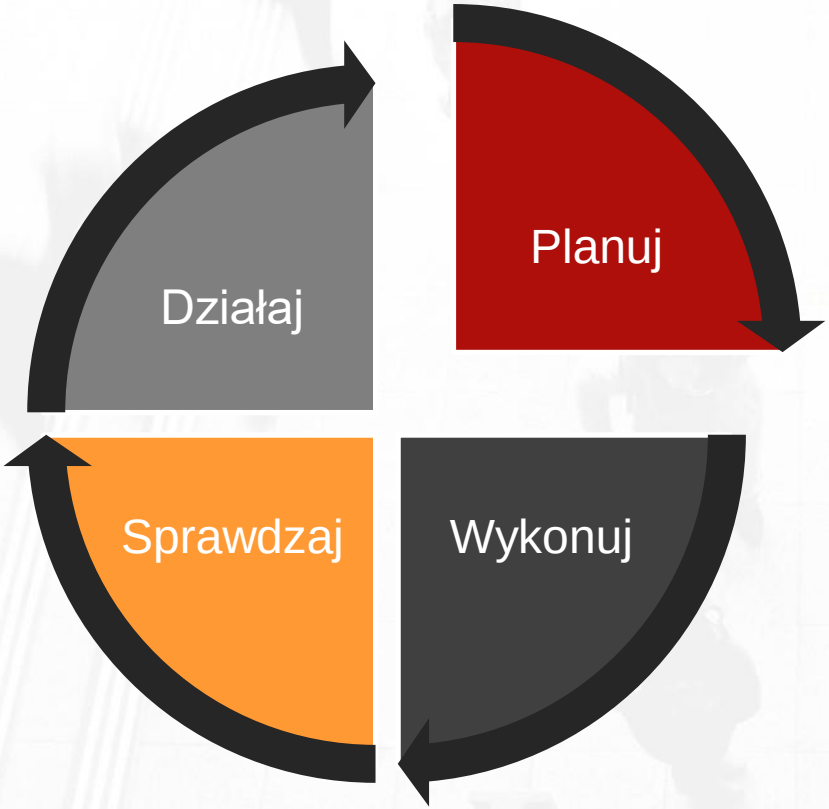


Dąż do doskonałości - cykl Deminga

Jak stosować podejście oparte na ryzyku

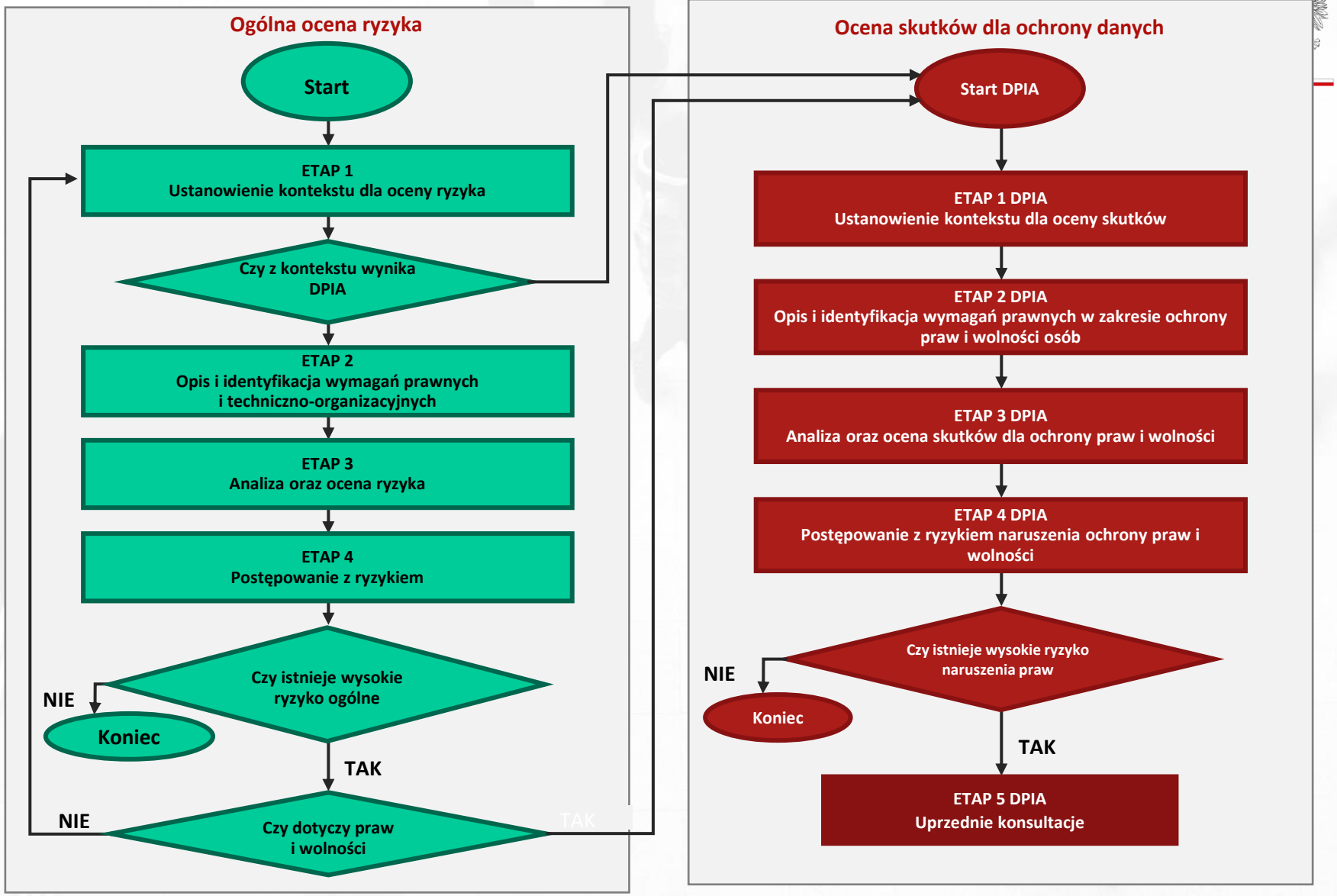
Urząd Ochrony Danych Osobowych

Zarówno ogólna ocena ryzyka, jak i ocena skutków dla ochrony danych polega na wielokrotnym (cyklicznym) powtarzaniu 4 podstawowych etapów:



1. **kontekst,**
2. **mechanizmy kontrolne,**
3. **szacowanie ryzyka,**
4. **postępowanie z ryzykiem**

Uwzględnienie oceny skutków. Jak zrealizować?



Ocena ryzyka

1. Ustanowienie kontekstu

Urząd Ochrony Danych Osobowych

1.1. Określenie wszystkich informacji i uwarunkowań związanych z działaniem organizacji, w tym posiadanych aktywów i zadań realizowanych przez konkretną organizację.

W odniesieniu do aktywów informacyjnych, w tym danych osobowych, powinny to być informacje obejmujące zakres, charakter i cele przetwarzania, a także potencjalne zagrożenia związane z ich nieuprawnionym ujawnieniem, utratą lub zniszczeniem. Informacje te najogólniej należy podzielić na wewnętrzne i zewnętrzne.

WEWNĘTRZNE - Informacje dotyczące:

- ✓ **struktury i rozmiaru organizacji,**
- ✓ **strategii i stosowanej polityki,**
- ✓ **systemu obiegu informacji, procesów, decyzji, roli przywództwa,**
- ✓ **Środowiska technologicznego,**
- ✓ **norm i standardów (kultura organizacyjna)**

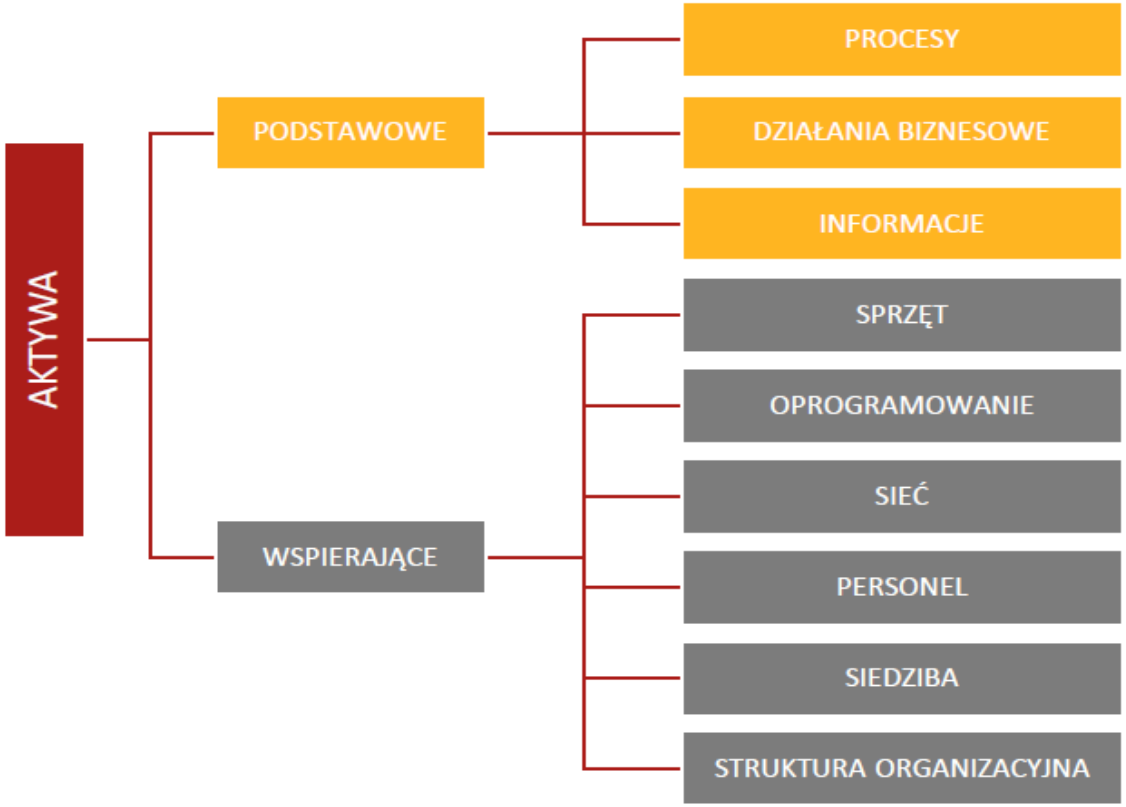
ZEWNĘTRZNE - Informacje dotyczące:

- ✓ **środowiska prawnego,**
- ✓ **środowiska społecznego i politycznego,**
- ✓ **korzystania z usług zewnętrznych,**
- ✓ **zasięgu terytorialnym i sposobu wymiany informacji.**

1. Ustanowienie kontekstu

1.2. Szczegółowy opis przetwarzanych danych i ich klasyfikacja

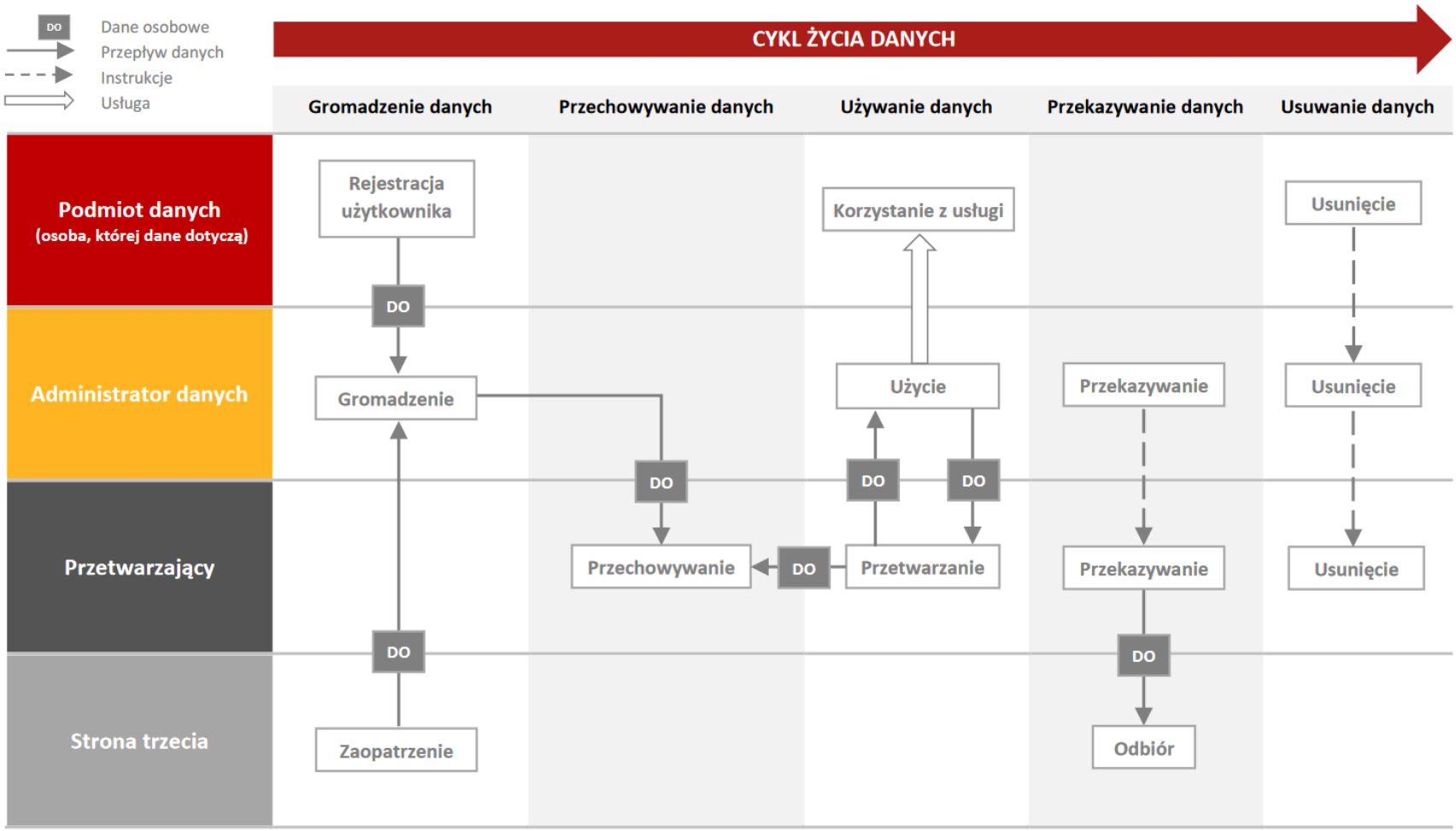
Należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych. Identyfikacja i klasyfikacja aktywów w danej organizacji powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie szacowania ryzyka.



Podział aktywów wg PN-ISO/IEC 27005

1. Ustanowienie kontekstu

1.2. Szczegółowy opis przetwarzanych danych i ich klasyfikacja



Przykładowy przepływ danych w organizacji

2. Mechanizmy kontrolne

Identyfikacja wymagań dla procesów przetwarzania danychw kontekście konkretnych celów działalności administratora

Należy określić:

- Konkretny cel przetwarzania,
- Odpowiednią do tego celu podstawę prawną przetwarzania danych (39 – 56 RODO)
- Wymagania dotyczące przejrzystości informacji udzielanych osobom, których dane dotyczą, na temat przetwarzania ich danych osobowych oraz ułatwiania im wykonywania ich praw
- Zakres danych niezbędny do realizacji celów przetwarzania
- Źródła i sposób pozyskiwania danych oraz przepływ danych w czasie ich przetwarzania
- Wymagania w zakresie jakości przetwarzanych danych oraz weryfikacji tej jakości
- Czas przez jaki dane będą przetwarzane oraz wymagania dotyczące sposobu ich usunięcia po czasie, kiedy będą już znane (jeśli cel przetwarzania został osiągnięty)

2. Mechanizmy kontrolne

Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ichwypełnienia

Należy określić:

- **Ogólne ryzyko naruszenia ochrony przetwarzanych danych**

Przykłady:

- rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (KNF 2013)
- Rozporządzenie MSWiA w sprawie sposobu utrwalania przebiegu imprezy masowej

- **Rozpoznanie czy w procesie przetwarzania występują elementy, które wymagają przeprowadzenia oceny skutków (z art. 35) i ew. konsultacji z organem nadzorczym (art. 36).**

2. Mechanizmy kontrolne

Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ich wypełnienia

Należy określić:

- **Zabezpieczenia organizacyjne** (zarządzanie personelem, **incydentami,** udziałem stron trzecich – podmiotów przetwarzających)
- **Środki kontroli logicznej** (anonimizacja, pseudonimizacja, środki kontroli dostępu, środki wspierające weryfikację danych na etapie ich wprowadzania itp.
- **Środki ochrony fizycznej** (dokumentacji papierowej, zagrożenia ze strony żywiołów itp.)

3. Szacowanie ryzyka

Identyfikacja zagrożeń

Urząd Ochrony Danych Osobowych

Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać. Uwzględnia się dwa podstawowe parametry:

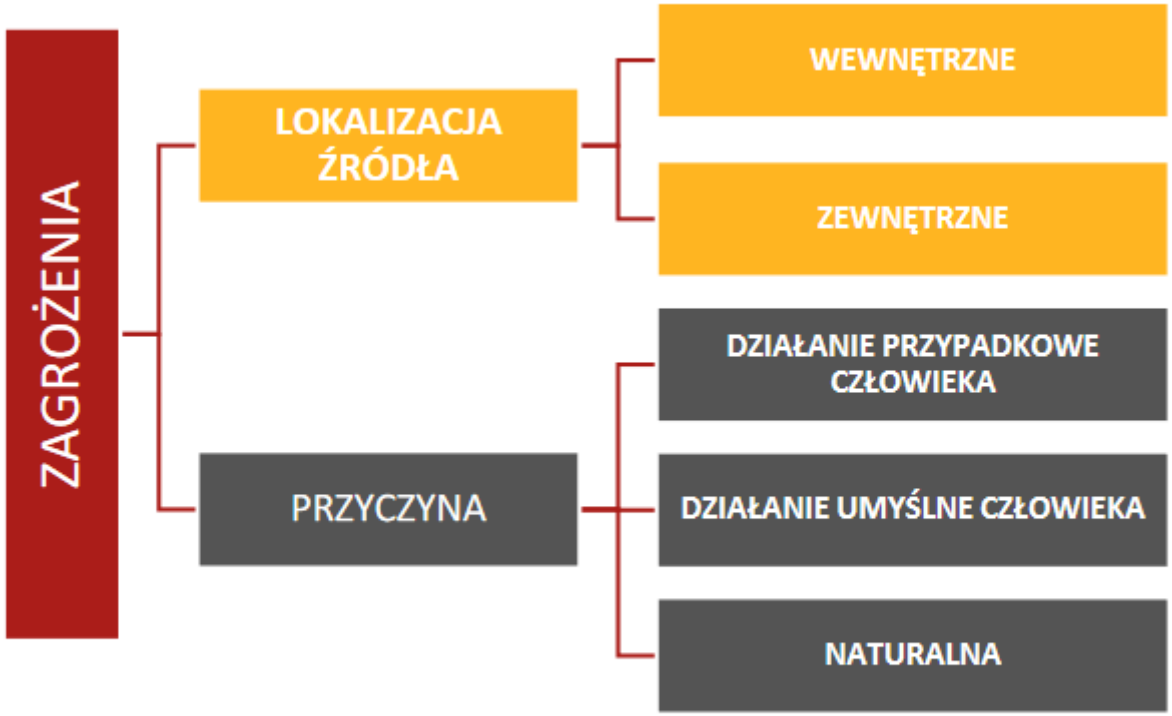
- **prawdopodobieństwo oraz**
- **mierzalne skutki zaistnienia takiego zdarzenia.**

Co do zasady wykorzystuje się w takich przypadkach jedną z poniższych metod:

1. **Ilościowa analiza ryzyka**
2. **Jakościowa analiza ryzyka**

3. Szacowanie ryzyka

Identyfikacja zagrożeń



Rysunek 6. Przykładowe kryteria podziału zagrożeń[4]

Katalog zagrożeń CERT.GOV.PL

RODZAJ	TYP			
1.1 - OPROGRAMOWANIE ZŁOŚLIWE	1.1.1 – wirus	1.1.2 - ransomware	1.1.3 - klient botnetu	
1.2 - PRZEŁAMANIE ZABEZPIECZEŃ	1.2.1 - włamanie na konto	1.2.2 - włamanie do systemu/aplikacji	1.2.3 - włamanie do infrastruktury	
1.3 - PUBLIKACJE W SIECI INTERNET	1.3.1 - treści szkodliwe	1.3.2 - dezinformacja	1.3.3 – groźby karalne	
	1.3.4 – kradzież tożsamości / podszywanie się	1.3.5 – publikacja danych wrażliwych		
1.4 - GROMADZENIE INFORMACJI	1.4.1 - skanowanie	1.4.2 - inżynieria społeczna	1.4.3 - sniffing	1.4.4 - SPAM
1.5 - SABOTAŻ KOMPUTEROWY	1.5.1 - nieuprawniona zmiana danych	1.5.2 – nieuprawniony dostęp do danych		
	1.5.3 - atak odmowy dostępu (np. DDoS, DoS)	1.5.4 – zniszczenie zasobu		
1.6 - CZYNNIK LUDZKI I ZDARZENIA LOSOWE	1.6.1 - naruszenie polityki bezpieczeństwa	1.6.3 -zaniedbanie		
	1.6.4 – prace techniczne	1.6.5 - awaria		
1.7 - PODATNOŚCI	1.7.1 – ujawnienie podatności	1.7.2 - błędna konfiguracja		
1.8 - CYBERTERRORYZM	1.8.1 –zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni			

3. Szacowanie ryzyka

3.2. Identyfikacja występujących podatności

Rysunek 8. Przykładowe podatności wg normy PN-ISO/IEC 27005

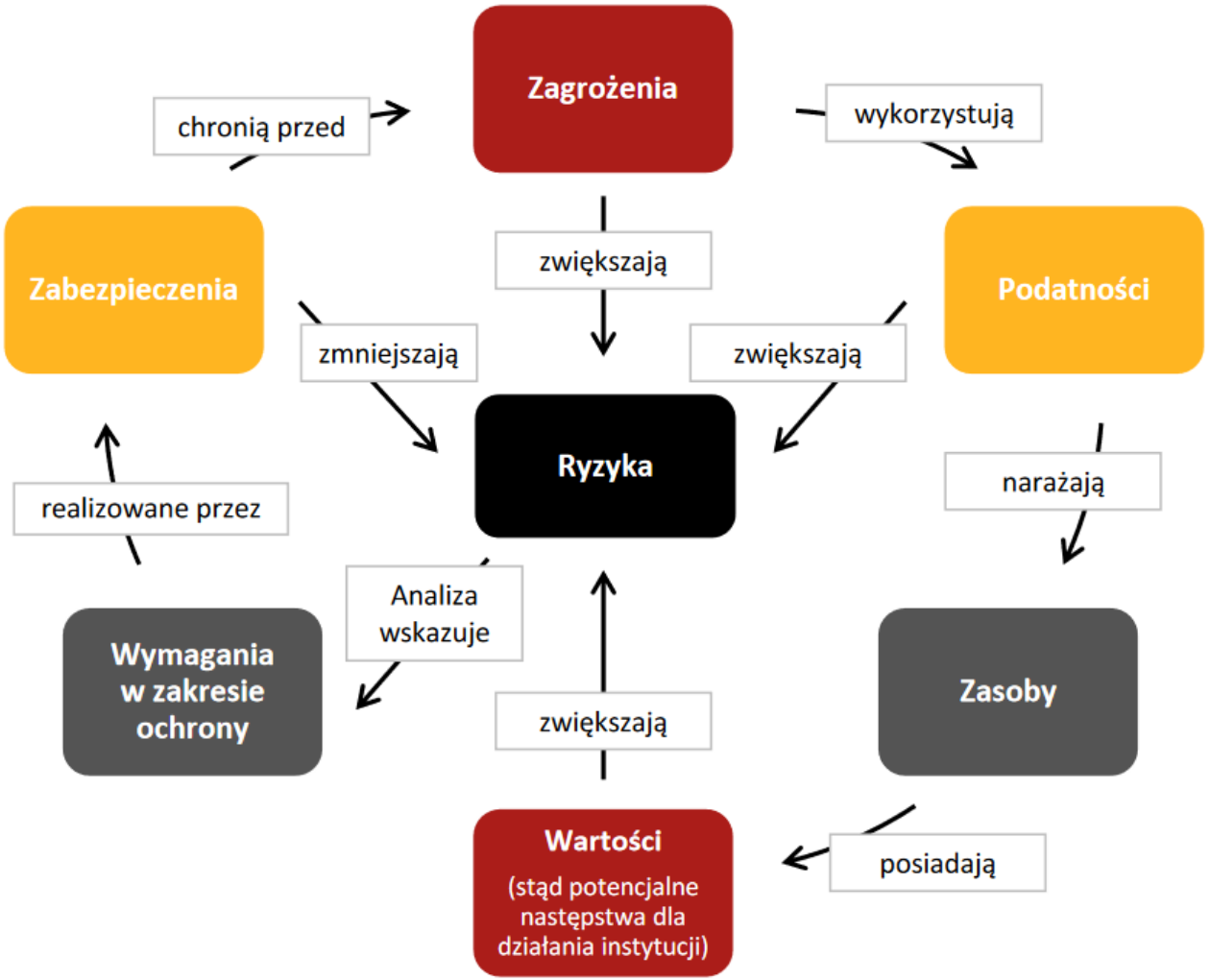
Urząd Ochrony Danych Osobowych

Bardzo często, dobrym źródłem informacji o zagrożeniach i podatnościach jest analiza zdarzeń, które już dotychczas miały miejsce u administratora czy podmiotu przetwarzającego.

Zalecany jest przegląd dostępnych archiwów bądź informacji medialnych na temat zdarzeń jakie miały miejsce u konkurentów bądź „trendach" w zakresie zagrożeń do danych procesów przetwarzania. Ponadto dobrym źródłem są analizy ekspertów czy komunikaty organów nadzorczych bądź innych instytucji specjalizujących się w danej dziedzinie (np. CERTy, Komisja Nadzoru Finansowego, Ministerstwa).

3. Szacowanie ryzyka

3.3. Analiza i ocena następstw zmaterializowania się zagrożeń



3. Szacowanie ryzyka

3.4. Szacowanie poziomu

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	W	W

	Poziom ryzyka	Opis działania
	Niski **(N)**	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
	Średni **(Ś)**	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
	Wysoki **(W)**	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
	Krytyczny **(K)**	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Tabela 3. Przykładowa macierz ryzyka

3. Szacowanie ryzyka

3.5. Określenie listy zidentyfikowanych ryzyk

Rodzaj operacji przetwarzania danych	Zidentyfikowane zagrożenia	Poziom ryzyka	Decyzja	Uzasadnienie akceptacji wyliczonego poziomu ryzyka
Przykład: Przechowywanie elektronicznej dokumentacji medycznej	Utrata danych w przypadku awarii nośnika danych.	Wysoki	Zastosować dodatkowe środki bezpieczeństwa w postaci systemu kopii zapasowych.	Brak akceptacji. Dane mogą być niezbędne do ratowania zdrowia i życia. Utrata zaufania pacjentów do podmiotu przetwarzającego (świadczącego usługi medyczne).

4. Postępowanie z ryzykiem - decyzja

Rysunek 10. Rodzaje postępowania z ryzykiem wg normy ISO/IEC 27005

Urząd Ochrony Danych Osobowych

Ocena skutków dla ochrony danych

…to proces budowania i wykazywania zgodności

Ocena skutków dla ochrony danych

Urząd Ochrony Danych Osobowych

Opinia GR art 29 – DPIA jako ważne narzędzie rozliczalności

DPIA jest procesem mającym opisać przetwarzanie, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu wynikającym z przetwarzania danych osobowych ryzykiem naruszenia praw lub wolności osób fizycznych poprzez ocenę ryzyka i ustalenie środków mających mu zaradzić.

Dokonanie oceny pozwala wykazać, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

Ocena skutków dla ochrony danych

Urząd Ochrony Danych Osobowych

Art. 35 ust 1

1. DPIA dotyczy **planowanych** operacji przetwarzania (np. nowa usługa, rozpoczęcie działalności)
2. Należy rozważyć czy przeprowadzić DPIA w przypadku wykorzystania nowych technologii
3. Należy wziąć pod uwagę: charakter, zakres, kontekst i cele przetwarzania a to z kolei pozwoli ustalić **czy dane przetwarzanie będzie wysoce ryzykowne dla praw lub wolności osób fizycznych.**

Kryteria zawarte w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

- Swoboda w wyborze metodyki przeprowadzenia oceny.
- Metodyka ta powinna być zgodna z **kryteriami określonymi w załączniku nr 2 do Wytycznych GR Art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679. (WP 248).**
- Kryteria można wykorzystać do wykazania, że konkretna metodyka oceny skutków dla ochrony danych spełnia standardy przewidziane w RODO.
- Pomocne informacje w poradniku GIODO: *Jak rozumieć i stosować podejście oparte na ryzyku?*,
- Wskazana jest ścisła współpraca pomiędzy administratorem, inspektorem ochrony danych oraz podmiotem przetwarzającym na każdym z etapów dokonywania oceny skutków dla ochrony danych.

Adresaci obowiązku

Urząd Ochrony Danych Osobowych

Adresatem obowiązku prowadzenia oceny skutków jest **administrator.** Natomiast **nie jest wykluczony udział w ocenie skutków podmiotu przetwarzającego**, który w razie potrzeby i na żądanie administratora powinien wspierać go w zapewnieniu przestrzegania tego obowiązku.

Ponadto, jeżeli w strukturze danego administratora został wyznaczony inspektor ochrony danych osobowych, zgodnie z art. 39 ust. 1 lit. c także on bierze udział w ocenie skutków, udzielając na żądanie administratora zaleceń w tym zakresie i monitorując jej wykonanie.

Uwzględnienie oceny skutków. Jak zrealizować?

Urząd Ochrony Danych

Wskazówki dotyczące oceny skutków dla ochrony danych – motyw 75 RODO

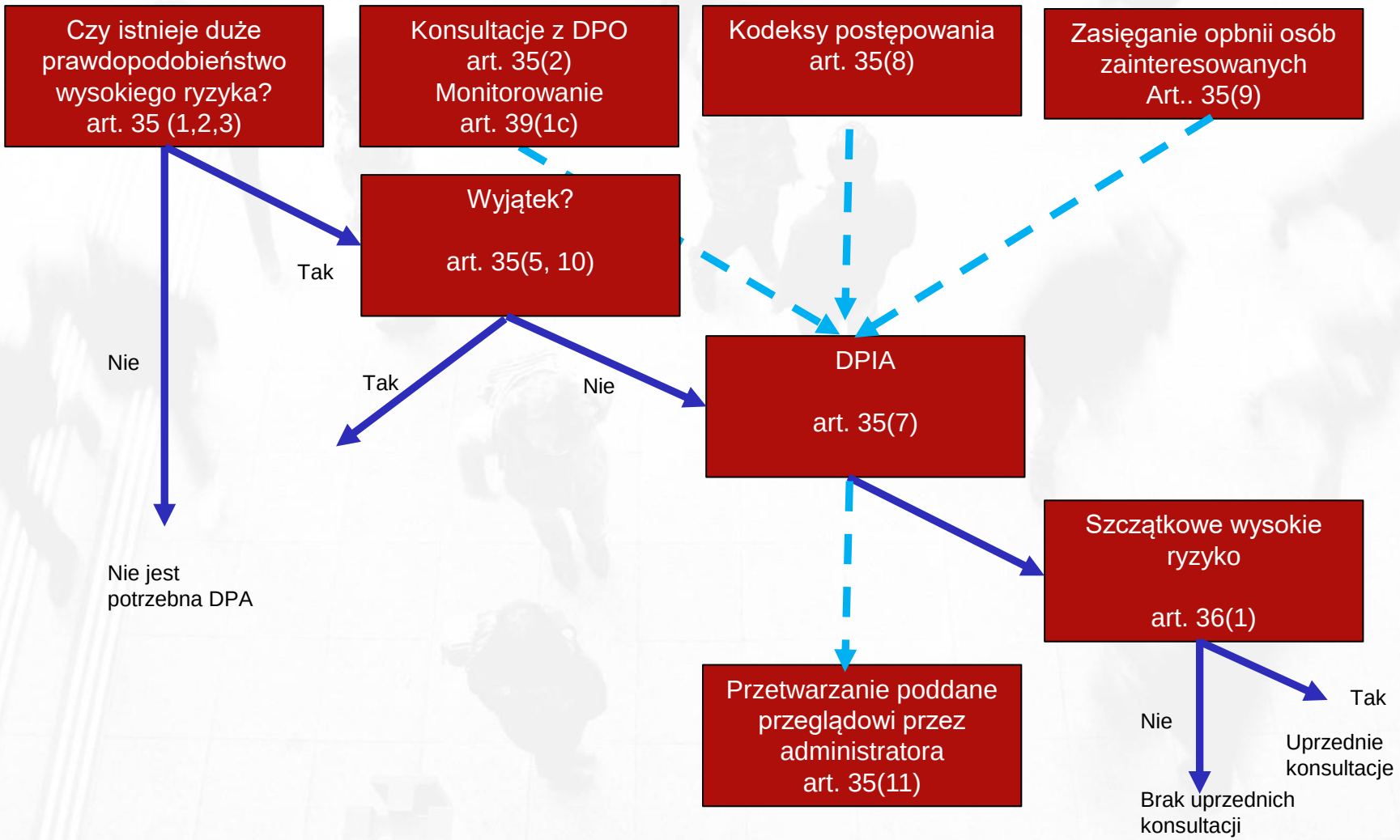
Ryzyko naruszenia praw lub wolności.

Dotyczy sytuacji gdy:

- Przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą
- Osoby mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
- Przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia, seksualności lub wyroków skazujących
- Oeniane są czynniki osobowe, np dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
- Przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych



Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

DPIA nie jest wymagane, jeżeli:

- przetwarzanie „**z dużym prawdopodobieństwem nie spowoduje wysokiego ryzyka naruszenia praw lub wolności osób fizycznych**”,
- charakter, zakres, kontekst i cele przetwarzania są **bardzo podobne do przetwarzania, dla którego została dokonana ocena**,
- gdy operacja przetwarzania ma podstawę prawną w prawie UE lub państwie członkowskiego i prawo reguluje określoną operację przetwarzania uwzględniając DPIA (zgodnie ze standardami RODO, DPIA w takich przypadkach jest wymagana w ramach ustanowienia tej podstawy prawnej (artykuł 35 ust. 10);
- gdy przetwarzanie uwzględnione jest w opcjonalnym wykazie (ustanowionym przez organ nadzorczy) operacji przetwarzania niepodlegających wymogowi dokonania DPIA (art. 35 ust. 5).

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Jak „szybko” zweryfikować czy muszę dokonać oceny skutków dla ochrony danych?

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 1 - Ewaluacja lub ocena, w tym profilowanie i przewidywanie, szczególnie „*aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą*”. Np.:

- Bank oceniający zdolność kredytowa na podstawie analizy danych z BIK.
- Określenie preferencji użytkownika w oparciu o odwiedzane strony internetowe.

Kryterium 2 - Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki. Np::

- System odcinkowej kontroli prędkości - system wylicza średnią prędkość i przekazuje dane do wystawienia mandatu.
- Automatyczne zatwierdzanie lub odrzucanie wniosku kredytowego.

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 3 - Systematyczne monitorowanie, tj. przetwarzanie wykorzystywane do obserwacji, monitorowania i kontroli osób, których dane dotyczą, w tym dane zbierane poprzez „*systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie*”.

- Rejestrowanie obrazu dla określonego miejsca, np. osób wchodzących i wychodzących z restauracji, hotelu;
- Rozpoznawanie osób z wykorzystaniem systemu rozpoznawania wizerunku i rejestrowanie ich w bazie klientów (rozpoznanie może być wykonane bez wiedzy osób ich dotyczących).

Kryterium 4 - Dane wrażliwe, w tym dane obejmujące szczególne kategorie danych określonych w artykule 9 i 10.

- Rejestr dokumentacji medycznej prowadzony przez szpital;
- Prywatny detektyw przechowujący dane dotyczące działań przestępczych;
- Przetwarzanie danych biometrycznych, np. system kontroli wejścia na stadion;

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 5 - Dane przetwarzane na dużą skalę
(„duża skala – motyw 91), należy wziąć pod uwagę:

a) liczbę osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;

b) zakres przetwarzanych danych osobowych;

c) okres, przez jaki dane są przetwarzane;

d) zakres geograficzny przetwarzania danych osobowych.

- Rejestrowanie danych dotyczących zużycia energii przez liczniki inteligentne z częstotliwością co 15 minut;
- Przetwarzanie danych lokalizacyjnych w określonym przedziale czasu, np. w godzinach pracy;
- Przetwarzanie danych osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem kart miejskich;

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 6 - Dokonano porównania lub połączenia zestawów danych: na przykład pochodzących z dwóch lub większej liczby operacji przetwarzania prowadzonych w różnych celach i/lub przez różnych administratorów danych w sposób, który wykracza poza racjonalne oczekiwania osoby, której dane dotyczą.

- Zastosowanie technologii BigData.

Kryterium 7 - Dane dotyczące osób wymagających szczególnej opieki, tj. jeżeli przetwarzanie tego rodzaju danych może wymagać DPIA ze względu na zwiększony brak równowagi sił między osobą, której dane dotyczą, a administratorem danych, co oznacza, że osoba może nie być w stanie wyrazić zgody na przetwarzanie jej danych lub sprzeciwić się takiemu przetwarzaniu.

- Przetwarzanie danych pracowników, uczniów;
- Przetwarzanie danych osobowych osób chorych psychicznie, osób ubiegających się o azyl, pacjentów;

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 8 - Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych.

- Zastosowanie biometrii uniemożliwiającej zmiany wzorca biometrycznego w przypadku utraty poufności (źródła danej biometrycznej nie da się zmienić tak jak hasła);
- Zastosowanie biometrii wielomodalnej na przykład połączenie wykorzystania odcisków palców i rozpoznawania twarzy do usprawnienia fizycznej kontroli dostępu;
- Zastosowanie tej samej metody biometrycznej w różnych systemach uwierzytelniania (przyszłe konsekwencje łączenia danych z różnych źródeł);
- Internet przedmiotów i usługi geolokalizacyjne (przetwarzanie fotografii z metadanymi dotyczącymi lokalizacji).

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Kryterium 9 - Gdy przetwarzanie samo w sobie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy” (artykuł 22 i motyw 91). Dotyczy to przetwarzania prowadzonego w miejscu publicznym, którego przechodzący ludzie nie mogą uniknąć, lub przetwarzania, którego celem jest umożliwienie, zmiana lub odmowa dostępu osób, których dane dotyczą, do usługi lub zawarcia umowy.

- Monitorowanie otoczenia bankomatu, czy monitorowanie wejścia do urzędu;
- Sprawdzanie przez bank klientów w bazie informacji kredytowej;
- Sprawdzanie klientów w bazie informacji gospodarczej.

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

WP 248 rev. 01 – przykłady, strona 13 i 14 Inny przykład:

Przetwarzanie	**Kryteria**	**OSOD?**
Usługa budująca profil żywieniowy użytkownika i informująca (reklamująca) o posiłkach w pobliskich restauracjach w zależności od lokalizacji użytkownika dostarczanej przez inną usługę (gromadzącą dane np. na potrzeby nawigacji samochodowej).	1. Profilowanie 5. Duża skala 6. Połączenie zestawów danych	**TAK**

Co do zasady, wg wytycznych 2 kryteria kwalifikują do przeprowadzenia OSOD. Przy czym należy pamiętać by dla indywidualnych przypadków wziąć pod uwagę cały kontekst planowanego przetwarzania.

Dla powyższego przykładu zalecana byłaby lektura innych wytycznych – **WP251 rev. 01** (wytyczne w sprawie profilowania), **WP203** (wytyczne w sprawie ograniczonego celu)

OCENA WSTĘPNA
Kryteria w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

Uznałem/łam, że spełniam kryteria, co dalej?

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

GR Art. 29 proponuje następujące **kryteria, które administratorzy danych mogą wykorzystać do oceny, czy DPIA lub metodologia przeprowadzania DPIA są wystarczająco obszerne, aby zapewnić zgodność z RODO:**

- Zapewniony jest systematyczny opis planowanych operacji przetwarzania (artykuł 35 ust. 7):
  - charakter, zakres, kontekst i cele przetwarzania są uwzględnione;
  - dokumentowane dane osobowe, odbiorcy oraz okres przechowywania danych osobowych;
  - dostarczony jest funkcjonalny opis operacji przetwarzania;
  - zidentyfikowane są aktywa, na których opierają się dane osobowe (sprzęt, oprogramowanie, sieci, ludzie, dokumenty papierowe lub papierowe kanały transmisji);
  - uwzględnia się zgodność z zatwierdzonymi kodeksami postępowania;

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Urząd Ochrony Danych Osobowych

- Zarządzenie ryzykiem naruszenia praw lub wolności osób (artykuł 35 ust. 7):
  - Uwzględnienie źródła, charakteru, specyfiki i powagi tego ryzyka (porównaj motyw 84); lub dokładniej, w odniesieniu do każdego ryzyka (nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych) z punktu widzenia osób, których dane dotyczą:
    - uwzględniono źródło ryzyka (motyw 90);
    - potencjalne skutki dla praw lub wolności osób, których dane dotyczą, są identyfikowane w przypadku nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
    - zagrożenia, które mogłyby prowadzić do nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
    - oszacowano prawdopodobieństwo i powagę tego ryzyka (motyw 90);
  - ustalono środki planowane w celu zaradzenia ryzyku (artykuł 35 ust. 7 lit. d i Motyw 90);
- zaangażowanie zainteresowanych stron:
  - zasięgnięto konsultacji DPO (artykuł 35 ust. 2);
  - zasięgnięto opinii osób, których dane dotyczą lub ich przedstawicieli (artykuł 35 ust. 9);

Urząd Ochrony Danych Osobowych

Dyskusja
i wymiana dobrych praktyk

Urząd
Ochrony
Danych
Osobowych

Dziękuję za uwagę

Michał Mazur

m_mazur@uodo.gov.pl