enterprise europe network

RODO a analiza ryzyka w MŚP

Seminarium z cyklu ”Europejskie Przedsiębiorstwo”

r. pr. Maciej Gawroński
apl. r. Patrycja Naklicka

www.een.org.pl

PARP Grupa PFR / Centrum Rozwoju MŚP

2008-2018 enterprise europe network Business Support on Your Doorstep

European Commission

Kim jesteśmy?
Gawroński & Partners

Nasz zespół to osoby z doświadczeniem w Komisji Nadzoru Finansowego, jako szefowie działów prawnych instytucji finansowych, prawnicy in-house największych polskich spółek publicznych, prawnicy kancelarii międzynarodowych i krajowych, specjaliści do spraw przestępstw gospodarczych w tym korupcji i współpracy z organami ścigania.

Maciej Gawroński

maciej.gawroński@gawronski.law

+48 609 602 566

- ekspert danych osobowych, IT, cyberbezpieczeństwa, własności intelektualnej, sporów
- ekspert Komisji Europejskiej ds. Kontraktów Cloud Computingowych
- konsultant Grupy Roboczej Artykułu 29 ds. transferów danych
- pomysłodawca bezpośredniej odpowiedzialności podprzetwarzających (art. 82 RODO), przenoszalności danych osobowych (art. 20 RODO), konsultował zasady podpowierzenia (art. 28.2 i 28.4 RODO)
- doradzał przy największym w Polsce i Centralnej Europie projekcie informatycznym w sektorze prywatnym jak i w setkach innych projektów IT
- główny autor treści modułu LEX Ochrona Danych Osobowych Wolters Kluwer, https://www.ochrona-danych-osobowych.lex.pl/ i publikacji RODO. Praktyczny przewodnik z wzorami (kwiecień 2018)
- reprezentował Polskę i klientów prywatnych w sporach o wartości miliardów euro

Patrycja Naklicka

patrycja.naklicka@gawronski.law

+48 506 256 421

- specjalizuje się w prawie nowych technologii, w tym IT oraz ochronie i bezpieczeństwie danych osobowych.
- doradza w zakresie ochrony danych na rzecz klientów z wielu sektorów gospodarki w tym: sektora energetycznego, telekomunikacyjnego, bankowego.
- wdraża złożony projekt zintegrowanego systemu informatycznego dla czołowego banku na rynku polskim.
- specjalizuje się w analizach zarządzania bezpieczeństwem informacji oraz zarządzaniem ryzyka przetwarzania danych osobowych. W ramach praktyki wraz z zespołem Kancelarii Gawroński & Partners opracowała autorską metodologię analizy ryzka przetwarzania danych osobowych.
- uczestniczyła w projektach z zakresu ochrony danych osobowych oraz projektów IT, w tym w projektach wdrożeniowych RODO (Ogólne Rozporządzenie EU o Ochronie Danych Osobowych).

RODO. Przewodnik ze wzorami

- najbardziej praktyczny komentarz dostępny na rynku
- tylko o obowiązkach administratorów i przetwarzających
- 460 stron, w tym wzory dokumentów
- Według publikacji twitterowych: „**To się czyta**”.

https://www.profinfo.pl/sklep/rodo-przewodnik-ze-wzorami-przedsprzedaz,72415.html

Program

1. ***Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych**
2. Podstawy prawne analizy ryzyka
3. Źródła metodyki analizy ryzyka
    1. Privacy Impact assessment (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Ogólne Rozporządzenie o Ochronie Danych Osobowych

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Ogólne Rozporządzenie o Ochronie Danych („**RODO**”)

Od **25 maja 2018 r.** RODO ma **bezpośrednie zastosowanie** w każdym państwie członkowskim UE

Porządek prawny po 25 maja 2018 roku:

1) **RODO** – podstawowe źródło praw i obowiązków związanych z przetwarzaniem danych osobowych;

2) **ustawa o ochronie danych osobowych z 10.05.2018 r.** (Dz.U. poz. 1000) – przepisy proceduralne, „infrastruktura RODO”;

3) **ustawa o ochronie danych osobowych z 1997 r**. – obowiązująca nadal w bardzo ograniczonym zakresie;

4) **ustawa „sektorowa”** - ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (projekt ustawy przyjęty przez Komitet Stały Rady Ministrów, planowana na listopad).

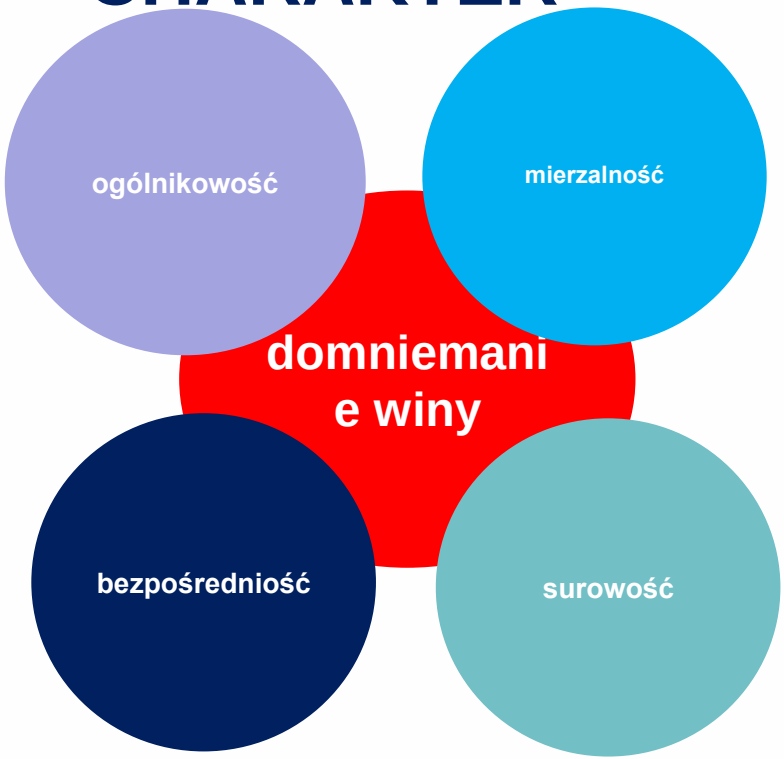
*__ustawa z 9.05.2018 r__. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. 2018 poz. 894).

Podejście do ochrony danych osobowych

RODO PERSPEKTYWA I – CHARAKTER

Nikt dotychczas nie odważył się wprowadzić regulacji, w której są tak wielkie kary za tak niejasne przepisy

- Wojciech Kapica, szef praktyki regulacyjnej Gawroński & Partners S.K.A.



Podejście do ochrony danych osobowych

RODO PERSPEKTYWA II – FILARY

- **Legalność** – to zasady do wprowadzenia
- **Prawa** – prawa jednostki to strumień pracy do obsłużenia
- **Bezpieczeństwo** – to procesy do wprowadzenia i utrzymywania

FUNDAMENT

- **Rozliczalność** – obowiązek wykazania zgodności (domniemanie winy)

Podejście do ochrony danych osobowych
RODO PERSPEKTYWA III – RYZYKO

Podejście przez ryzyko i na zasadzie ryzyka w połączeniu z …domniemaniem winy ☺

- ryzyko x 76, prawdopodobieństwo x 13

Motyw 75

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych

Motyw 76

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko

Ryzyko – definicja, znaczenie

RODO

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych

Normy ISO

Ryzyko „wpływ niepewności na cele”

W RODO chodzi **o ryzyko naruszenia praw lub wolności osób, których dane przetwarzamy**

Ryzyko naruszenia praw lub wolności

Prawa i wolności jednostek takie jak:

- zdrowie,
- wolność,
- bezpieczeństwo osobiste,
- prawo do prywatności,
- swoboda sumienia, wyznania,
- dobre imię, wizerunek,
- prawo do poszanowania życia prywatnego i rodzinnego,
- zakaz dyskryminacji,
- prawo do tajemnicy korespondencji,
- prawo do nietykalności mieszkania,
- oraz inne.

Istota zasady *risk based approach*

Risk based approach oznacza, że administrator i podmiot przetwarzający muszą sami określić środki i procedury zapewnienia zgodności z prawem i bezpieczeństwa przetwarzania danych osobowych.

Administrator i podmiot przetwarzający podejmują decyzję o przetwarzaniu na własne ryzyko.

Cel zasady *risk based approach*

Cel: Zapewnienie ochrony przetwarzania danych osobowych w sposób **racjonalny** (im większe ryzyko naruszenia praw i wolności – tym bardziej zaawansowane środki ochrony).

Wzrost ochrony w miarę wzrostu ryzyka

- Proaktywne podejście do zarządzania ryzykiem bezpieczeństwa danych
- Skuteczne przestrzeganie przepisów i zapewnienie „działającej" regulacji
- Dostosowanie środków ochrony przetwarzania danych osobowych odpowiednich do skali ryzyka
- Skoncentrowanie się na sytuacjach najwyższego ryzyka

Wyzwania stosowania podejścia *risk based approach*

- Ciężar doboru indywidualnych odpowiednich środków bezpieczeństwa spoczywa na administratorze i podmiocie przetwarzającym
- Zapewnienie większej „elastyczności” w doborze metod przetwarzania i środków zapewnienia bezpieczeństwa danych
- **Oszacowanie ryzyka w** celu doboru odpowiednich środków bezpieczeństwa - **przeprowadzenie analizy ryzyka**

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. **Podstawy prawne analizy ryzyka**
3. Źródła metodyki analizy ryzyka
    1. *Privacy Impact assessment* (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Motyw 75 RODO

Ryzyko naruszenia praw lub wolności osób, o **różnym prawdopodobieństwie** i **wadze**, może wynikać z przetwarzania danych osobowych mogącego prowadzić do **uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych.**

Ryzko naruszenia praw lub wolności

(prawdopodobieństwo x waga naruszenia)

skutek

(i) uszczerbek fizyczny lub (ii) szkód majątkowych lub (iii) niemajątkowych

Motyw 75 RODO c.d.

w szczególności:

- jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
- jeżeli 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 lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
- jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się - w celu tworzenia lub wykorzystywania profili osobistych; lub
- jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci;
- jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Motyw 75 RODO Podsumowanie

1) Ryzyko pozbawienie praw lub wolności;
2) Ryzyko pozbawienia kontroli nad danymi osobowymi;
3) Jeżeli przetwarzane są dane wrażliwe;
4) Profilowanie;
5) Osoby wymagające szczególnej opieki;
6) Przetwarzanie dużej ilości danych osobowych.

Motyw 85 RODO

Naruszenie ochrony danych osobowych może skutkować powstaniem **uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych**, takich jak

- utrata kontroli nad własnymi danymi osobowymi,
- ograniczenie praw,
- dyskryminacja,
- kradzież,
- sfałszowanie tożsamości,
- strata finansowa,
- nieuprawnione odwrócenie pseudonimizacji,
- naruszenie dobrego imienia,
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
- wszelkie inne znaczne szkody gospodarcze lub społeczne.

Motyw 76 RODO

Prawdopodobieństwo i **powagę ryzyka** naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych.

charakter – na czym polega przetwarzanie (opis operacji lub czynności przetwarzania, z tym że w ramach czynności przetwarzania możemy podejmować różne działania i te różne działania mogą wiązać się z różnymi ryzykami);

zakres – jakie dane, ile osób, jak bardzo rozproszone geograficznie jest przetwarzanie;

cel – po co administratorowi przetwarzanie;

kontekst – czym zajmuje się administrator (sektor, rola w łańcuchu dostawy, dla jakich sektorów/ klientów pracuje – po co przetwarzanie podmiotom danych) i okoliczności zewnętrzne.

Art. 24 ust. 1 RODO
Podejście od strony ryzyka

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w miarę potrzeby poddawane przeglądom i uaktualniane.

Art. 25 ust. 1 RODO (*privacy by design*)

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 zagrożenia wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne (....)

Art. 30 ust. 5 RODO
zwolnienie z Rejestrów

Obowiązki, o których mowa w ust. 1 i 2 , nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować **ryzyko** naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Art. 32 RODO
Bezpieczeństwo

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 zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Art. 35 ust. 1 RODO
Ocena skutków dla ochrony danych

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.

Podstawy prawne analizy ryzka a bezpieczeństwo przetwarzania w RODO

Atrybuty bezpieczeństwa informacji oraz stopnie ryzyka

Atrybuty bezpieczeństwa informacji C.I.A. a bezpieczeństwo przetwarzania w RODO

Tradycyjne rozumienie bezpieczeństwa opiera się na trzech podstawowych parametrach:

CIA

C – confidentiality – poufność

I – integrity – integralność

A – availability – dostępność

Przetwarzanie danych w RODO zgodnie z zasadami (art. 5 RODO) to przetwarzanie właśnie zgodnie z atrybutami bezpieczeństwa

C.I.A. (A)

(A) – accountability - rozliczalność

RYZYKO wg RODO = L x S

Ryzyko wg RODO to iloczyn:

(i) prawdopodobieństwa zagrożenia

(ii) powagi zagrożenia

Ryzyko wg ISO to:

„**wpływ niepewności na cele**”

Ryzyko jest czymś negatywnym co może niekorzystnie wpłynąć na osiągnięcie celu przez wywołanie niepożądanych skutków ubocznych (niezrealizowanie celu przetwarzania)

Stopnie ryzyka

RODO uznaje, że

istnieją różne stopnie ryzyka przetwarzania danych i powinniśmy zapewnić stopnie bezpieczeństwa odpowiednie do stopni ryzyka (*risk based approach*)

Stopnie ryzyka wg UODO:

1. pomijalny
2. niski
3. średni (może być bez)
4. wysoki
5. maksymalny

Stopnie ryzyka wg CNIL:

1. pomijalny
2. ograniczony
3. znaczący
4. maksymalny

Wnioski

Żeby zapewnić stopnie bezpieczeństwa adekwatne do stopni ryzyka należy przeprowadzić:

Analizę Ryzyka

Motyw 76 RODO
Ryzyko należy **oszacować na podstawie obiektywnej oceny**, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. **Źródła metodyki analizy ryzyka**
    1. **Privacy Impact assessment (PIA) CNIL**
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Źródła metodyki przeprowadzenia analizy ryzyka

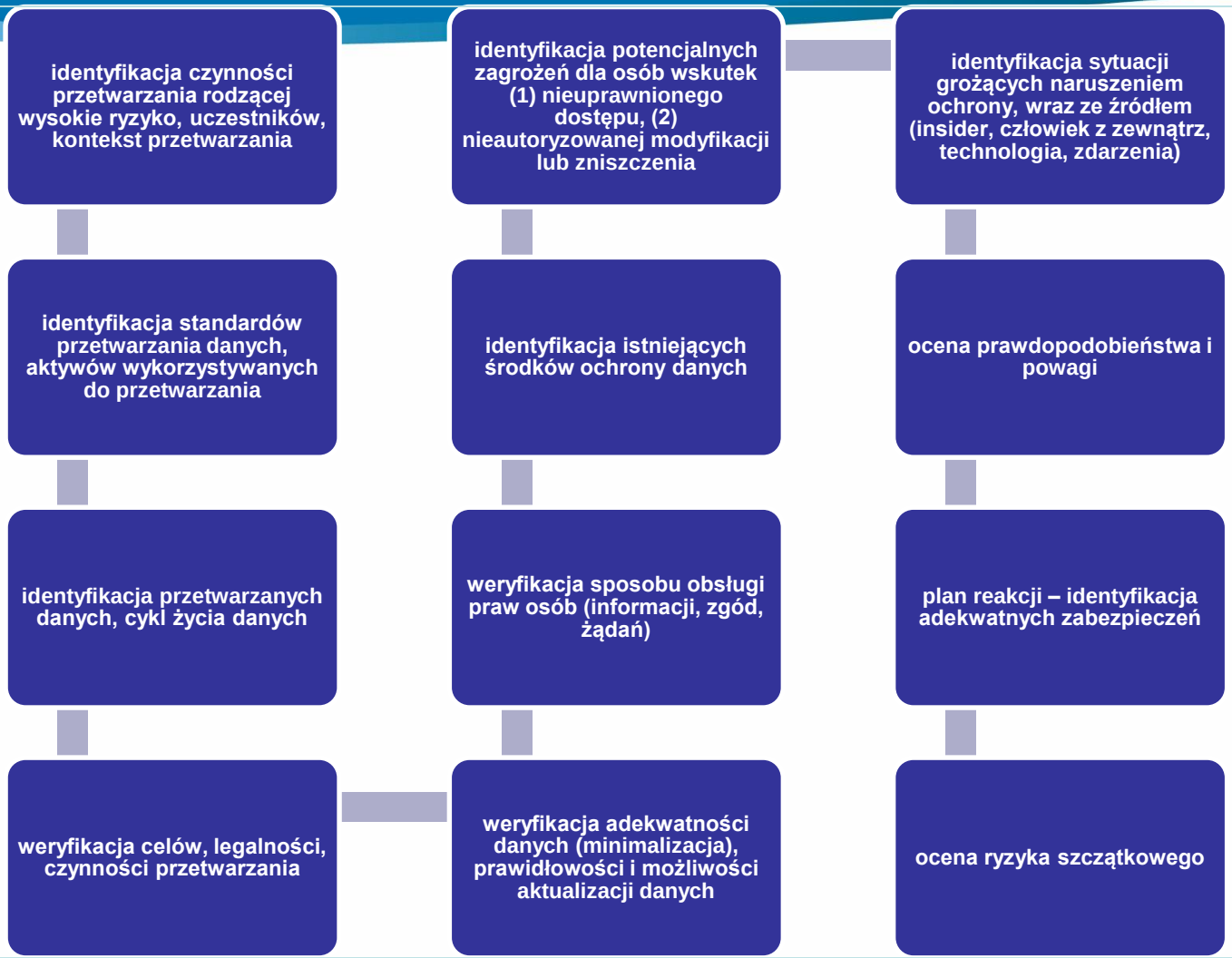
- na gruncie RODO nie została wskazana jedna określona metodyka przeprowadzania procesu analizy ryzyka;
- wybór metodyki powinien odpowiadać specyfice danego podmiotu (wielkość, struktura, możliwości organizacyjne, techniczne, finansowe);
- organizacja może skorzystać z jednej z dostępnych metodyk lub stworzyć własną na podstawie dostępnych źródeł i najlepszych opracowanych praktyk;
- analiza ryzyka przetwarzania danych osobowych jest częścią procesu zarządzania ryzykiem w organizacji i powinna być wpisana w proces zarządzania organizacją.

Privacy Impact assessment (PIA) CNIL

CNIL - francuski organ ochrony danych osobowych opracował ***PIA*** – narzędzie do przeprowadzenia DPIA – w polskiej wersji językowej (zatwierdzonej przez PUODO) można pobrać ze strony:

https://www.uodo.gov.pl/pl/123/213

Ocena skutków dla ochrony danych wg CNIL



Prezentacja kluczowych obszarów aplikacji wraz z omówieniem

część warsztatowa

enterprise europe network

Przerwa kawowa

Po przerwie zapraszamy na część II

www.een.org.pl

PARP Grupa PFR / Centrum Rozwoju MŚP

2008-2018 enterprise europe network Business Support on Your Doorstep

European Commission

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. **Źródła metodyki analizy ryzyka**
    1. Privacy Impact assessment (PIA) CNIL
    2. **Podejście oparte na ryzyku – materiały UODO**
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Podejście oparte na ryzyku – materiały UODO

Prezes Urzędu Ochrony Danych Osobowych (PUODO dawniej GIODO), przygotował dwuczęściowy poradnik:

1) Jak rozumieć podejście oparte na ryzyku według RODO?

2) Jak stosować podejście oparte na ryzyku?

Dostępne na stronie PUODO pod linkiem:

https://www.uodo.gov.pl/pl/123/208

Jak rozumieć podejście oparte na ryzyku wg RODO

Pierwsza część poradnika wskazuje:

- teoretyczne podejście do zasady *risk based approach.*
- co zasada *risk based approach* oznacza dla administratora i podmiotu przetwarzającego.
- wskazuje o jakie ryzyko (naruszenia praw i wolności osób), należy przeprowadzić analizę.

Pierwsza pomoc dla organizacji

Jak stosować podejście oparte na ryzyku?

Druga część przewodnika przedstawia proces analizy ryzyka rekomendowany przez UODO.

Analiza Ryzyka wg UODO (5 kroków)

1) Ustalenie kontekstu
2) Mechanizmy kontrolne
3) Szacowanie ryzyka
4) Postępowanie z ryzykiem – decyzja
5) Ogólna ocena ryzyka a DPIA

Analiza Ryzyka wg UODO

Krok 1: Ustalenie kontekstu:

a) Określenie **informacji i uwarunkowań** związanych z działaniem organizacji (profil organizacji)

b) Określenie **aktywów** (to co ma wartość dla organizacji) zaangażowanych w proces przetwarzania

c) Opis przetwarzanych danych i właścicieli tych aktywów

d) Szczegółowy opis stosowanych zabezpieczeń

e) Określenie kryteriów akceptacji ryzyka

Analiza Ryzyka wg UODO

Krok 2: Mechanizmy kontrolne

a) Identyfikacja wymagań dla procesów przetwarzania danych w kontekście konkretnych celów działalności administratora (zgodność z zasadami / cel / przesłanki przetwarzania)

b) Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ich wypełnienia (środki techniczne, organizacyjne, logiczne)

Analiza Ryzyka wg UODO

Krok 3: Szacowanie ryzyka

a) Identyfikacja zagrożeń (zagrożenie jako źródło potencjalnej szkody)

b) Identyfikacja podatności (sprzęt, oprogramowanie, sieć, personel, siedziba, organizacja)

c) Analiza i ocena następstw zmaterializowania się zagrożeń (1 i 2 = identyfikowanie następstw, jakie może spowodować zmaterializowanie się zagrożenia)

d) Szacowanie poziomu ryzyka (prawdopodobieństwa jego zajścia x szacowanie skutków jego zmaterializowania się)

e) Określenie listy zidentyfikowanych ryzyk (krok 2 porównujemy z krokiem 4)

Szacowanie poziomu ryzyka (prawdopodobieństwo)

I. Przykładowe prawdopodobieństwo wystąpienia zdarzenia wskazane przez UODO

Prawdopodobieństwo	Poziom	Opis
Prawie pewne	5	zdarzenie występuje co najmniej raz w tygodniu
Prawdopodobne	4	zdarzenie występuje co najmniej raz w miesiącu
Możliwe	3	zdarzenie występuje co najmniej raz na kwartał
Mało prawdopodobne	2	zdarzenie występuje co najmniej raz na pół roku
Rzadkie	1	zdarzenie nie występuje lub występuje raz w roku

Przy szacowaniu prawdopodobieństwa incydentu zwykle uwzględnia się następujące czynniki:

- statystyki dotyczące podobnych zdarzeń,
- atrakcyjność aktywu,
- czynniki środowiskowe,
- rodzaje podatności,
- a także istniejące zabezpieczenia.

Szacowanie poziomu ryzyka: (skutki)

Przykładowe skutki ze względu na finanse i reputację wskazane przez UODO

Skutek	Poziom	Opis	
		finanse	reputacja
Bardzo wysoki	5	powyżej 1 mln zł	negatywne opinie w mediach międzynarodowych
Wysoki	4	w zakresie 500 tys. – 1 mln zł	negatywne opinie w mediach krajowych
Średni	3	w zakresie 100 – 500 tys. zł	negatywne opinie w mediach lokalnych
Niski	2	w zakresie 5 – 100 tys. zł	negatywne opinie bez udziału mediów
Bardzo niski	1	poniżej 5 tys. zł	brak wpływu na reputację

Proponowana macierz ryzyka wg UODO

			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

Analiza Ryzyka wg UODO

Krok 4: Postępowanie z ryzykiem – decyzja

a) **modyfikowanie (redukcja) ryzyka** (polega na obniżeniu poziomu ryzyka)

b) **zachowanie (akceptacja) ryzyka** (nie robimy nic)

c) **unikanie ryzyka** (rezygnacja z danej czynności przetwarzania)

d) **dzielenie (przeniesienie) ryzyka** (polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę)

Analiza Ryzyka wg UODO

Krok 5: Określenie listy zidentyfikowanych ryzyk

Porównanie poziomu ryzyk wyliczonych w kroku 4 dla poszczególnych operacji przetwarzania z kryteriami akceptacji ryzyka określonymi w kontekście danego rodzaju operacji przetwarzania i wymaganiami wskazanymi w kroku 2.

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).

Raport z analizy ryzyka wg UODO

Nazwa zasobu	Poufność	Integralność	Dostępność	Wartość aktywów	Znane zagrożenia	Wartość zagrożenia	Podatność opis	Wartość podatności	Możliwość wystąpienia	Kontrola bieżąca	Wynik ryzyka	Zapobieganie ryzyku	Możliwość ponownego wystąpienia	Ryzyko szczątkowe
	Poziom ryzyka?	Poziom ryzyka?	Poziom ryzyka?			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Bardzo wysoki	Bardzo wysoki	Bardzo wysoki			Niski		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Poziom ryzyka?	Poziom ryzyka?	Poziom ryzyka?			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Wysoki	Wysoki	Wysoki			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Poziom ryzyka?	Poziom ryzyka?	Poziom ryzyka?			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Średni	Średni	Średni			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	
	Poziom ryzyka?	Poziom ryzyka?	Poziom ryzyka?			Poziom ryzyka?		Poziom ryzyka?	Poziom ryzyka?		Poziom ryzyka?		Poziom ryzyka?	

Kalkulator ryzyka ochrony danych

PARP Grupa PFR / Centrum Rozwoju MŚP

enterprise europe network 2008-2018 Business Support on Your Doorstep

European Commission

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. **Źródła metodyki analizy ryzyka**
    1. Privacy Impact assessment (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. **Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)**
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Szacowanie ryzyka oparte o normy ISO

- ISO 27005:2014 Zarządzanie ryzykiem w bezpieczeństwie informacji

Wytyczne dotyczące zarzadzania ryzykiem dla zapewnienia bezpieczeństwa informacji w organizacji, w szczególności wspierając wymagania dotyczące **systemu zarządzania bezpieczeństwem informacji (SZBI)**.

Jednak w Normie ISO 27005:2014 nie przedstawiono **żadnej określonej metody** zarządzania ryzykiem w bezpieczeństwie informacji.

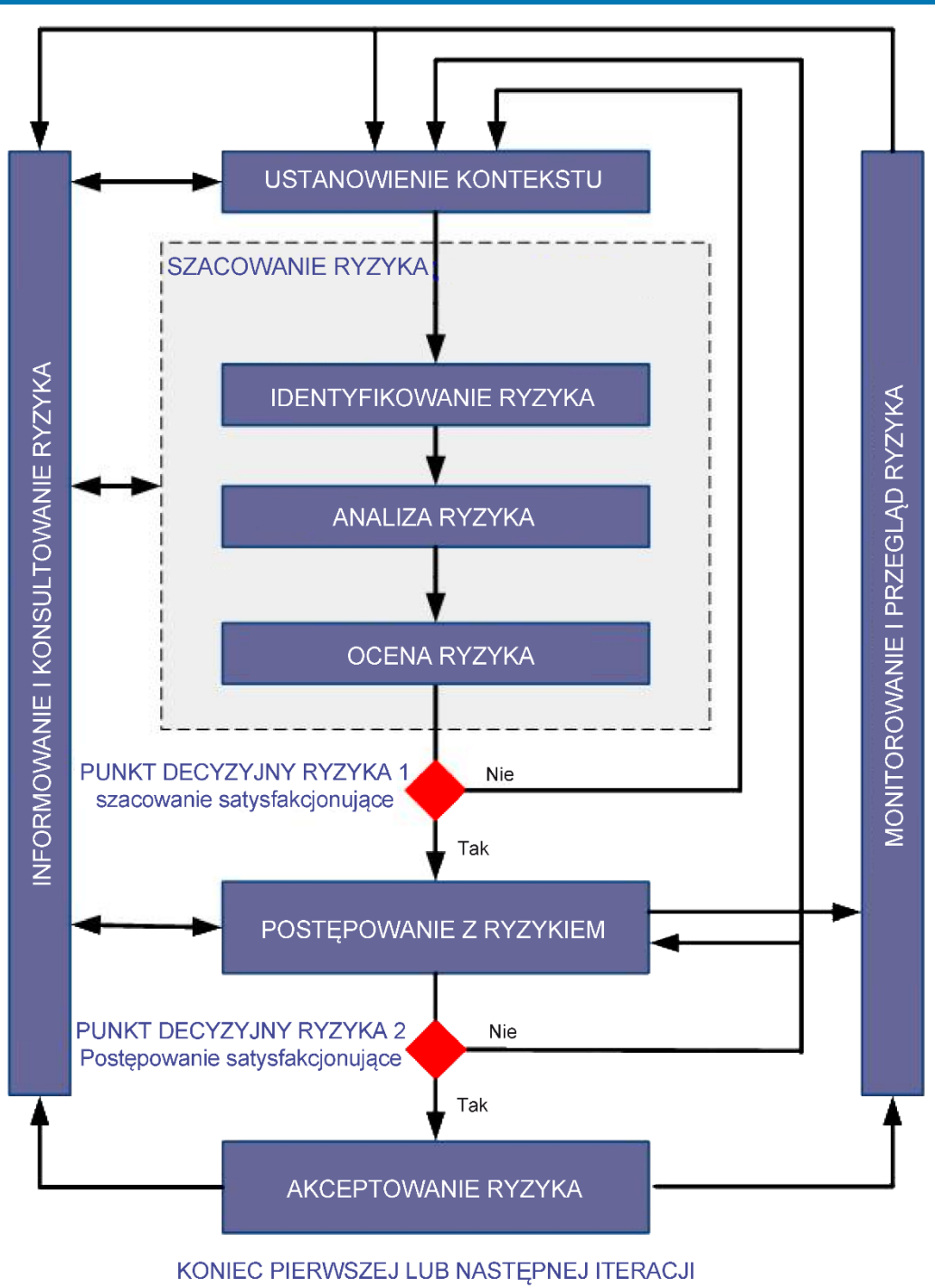
- ISO 29134:2017 Guidelines for privacy impact assessment

Wytyczne dotyczące oceny wpływu na prywatność. (PIA) jest instrumentem **oceny potencjalnego wpływu na prywatność** np. procesu, systemu informatycznego, programu, modułu oprogramowania, urządzenia lub innej inicjatywy, która przetwarza dane osobowe (PII)

Norma ISO 27005
Proces zarządzania ryzykiem

Przykładowy proces zarządzania bezpieczeństwem informacji wg. ISO 27005 w 6 krokach

1) Ustanowienie kontekstu
2) Identyfikowanie ryzyka
3) Analiza ryzyka
4) Ocena ryzyka
5) Postępowanie z ryzykiem
6) Akceptowanie ryzyka



Krok 1: Ustanowienie kontekstu

Należy określić podejście do zarządzania ryzykiem, odnoszące się do podstawowych kryteriów takich jak:

1. **Kryteria oceny ryzyk** (wartość biznesowa procesu analizowanego, krytyczność zaangażowanych aktywów, wymagania prawne, oczekiwania operacyjne i biznesowe);
2. **Kryteria skutków** (w kategoriach stopnia zniszczenia lub kosztów dla organizacji, straty biznesowe, zakłócenie planów i projektów organizacji);
3. **Kryteria akceptowania ryzyka** (kryteria akceptacji ryzyka zależą od polityki i celów organizacji oraz interesu uczestników). A w przypadku ustalania kryteriów akceptacji ryzyka przetwarzania danych osobowych – ogranicza nas RODO.

* Przy określaniu zarządzania ryzykiem ISO 27005 wskazuje, że zarządzanie ryzkiem należy zawęzić do pewnego zakresu: np. infrastruktury informatycznej, czy przetwarzania danych osobowych

Krok 2: Identyfikowanie ryzyka

Cel kroku 2: określenie co może się zdarzyć i spowodować potencjalną stratę, oraz uzyskanie wiedzy na temat tego jak / gdzie / dlaczego strata może się zdarzyć.

Identyfikowanie ryzyka to proces obejmujący:

I. Identyfikowanie aktywów

II. Identyfikowanie zagrożeń

III. Identyfikowanie istniejących zabezpieczeń

IV. Identyfikowanie podatności

V. Identyfikowanie następstw

Krok 2: Identyfikowanie ryzyka

I. Identyfikowanie aktywów

Jak zidentyfikować ryzyka? Najlepiej zidentyfikować ryzyka przez identyfikację aktywów wykorzystywanych w analizowanym zakresie.

Aktywa: to wszystko co służy do przeprowadzania procesu i ma wartość dla organizacji.

Poziom szczegółowości identyfikacji aktywów (także elementów aktywów) zależy od podejścia organizacji.

Krok 2: Identyfikowanie ryzyka

II. Identyfikowanie zagrożeń

Zagrożenie: potencjalna przyczyna uszkodzeń aktywów (a w konsekwencji uszkodzeń dla organizacji)

Źródła zagrożeń: mogą być różne: umyślne / przypadkowe/ naturalne

Należy zidentyfikować źródła/ typy i katalogi zagrożeń.

Rodzaj: zagrożenie

1. zniszczenie fizyczne: pożar / zalanie / zniszczenie
2. awaria techniczna: awaria urządzenia / niewłaściwe funkcjonowanie urządzeń
3. naruszenie bezpieczeństwa informacji: szpiegostwo zdalne / podsłuch

Więcej informacji o rodzajach zagrożeń można znaleźć w Załączniku C ISO 27005.

Krok 2: Identyfikowanie ryzyka

III. Identyfikowanie istniejących zabezpieczeń

Zaleca się zidentyfikowanie istniejących zabezpieczeń w celu sprawdzenia jak istniejące zabezpieczenia redukują **prawdopodobieństwo** zagrożenia i łatwość wykorzystania **podatności** lub **skutek incydentu**.

Zabezpieczenia: „*wszytko to co modyfikuje ryzko***” np.** środki ochrony technicznej, polityki, procesy, urządzenia, praktyki.

Krok 2: Identyfikowanie ryzyka

IV. Identyfikowanie podatności

Cel: identyfikacja podatności, które mogą spowodować szkodę dla aktywów lub organizacji

Przykładowe obszary podatności:

- organizacja
- procesy i procedury
- personel
- środowisko fizyczne
- konfiguracja systemów informatycznych
- sprzęt, oprogramowanie

Przykłady podatności: brak lub niewystarczające testowanie oprogramowania / niewystarczające utrzymanie / błędna instalacja nośników pamięci

Więcej informacji podatnościach oraz metody szacowania podatności można znaleźć w Załączniku D ISO 27005

Krok 2: Identyfikowanie ryzyka

V. Identyfikowanie następstw

Cel: określenie szkód lub następstw dla organizacji „co się może stać” jeżeli dane zagrożenie się zmaterializuje

Należy zidentyfikować *scenariusz incydentu.*
Scenariusz incydentu jest opisem sposobu, w jaki zagrożenie wykorzystuje określoną podatność w incydencie związanym z bezpieczeństwem informacji

Krok 3: Analiza ryzyka

Analiza ryzyka polega na przypisaniu wartości prawdopodobieństwu i następstwom ryzyka.

Analizę ryzyka można przeprowadzać na rożnym poziomie szczegółowości.

Główne etapy analizy ryzyka:

I. **Szacowanie następstw** (szacowanie skutków biznesowych, które mogłyby wynikać z możliwych lub rzeczywistych incydentów związanych z bezpieczeństwem informacji

II. **Szacowanie prawdopodobieństwa incydentu** (oszacowanie prawdopodobieństwa scenariuszy incydentów)

III. **Określenie poziomu ryzyka** (wielkość ryzka wyrażona przez kombinację następstw i prawdopodobieństwa)

Krok 4: Ocena ryzyka

Cel kroku 4: Subsumpcja **poziomów ryzyka** z **kryteriami oceny ryzyka** oraz **kryteriami akceptowania ryzyka**

Ocena ryzyka: proces porównania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia czy ryzko i/lub jego wielkość są akceptowane lub tolerowane

Wynik oceny ryzyka: decyzja o akceptacji ryzyka (szacowanie satysfakcjonujące) lub decyzja o konieczności podjęcia działań **postępowania z ryzykiem** (krok 5).

Krok 5: Postępowanie z ryzykiem

Cel kroku 5: wybranie dodatkowych zabezpieczeń w celu:

- **zmodyfikowania** (wdrożenie, usuniecie lub zmianę zabezpieczeń, tak aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne);
- **zachowania** (poziom ryzyka spełnia kryteria akceptowania ryzyka, to nie ma potrzeby wdrażania dodatkowych zabezpieczeń);
- **uniknięcia** (unikania działań lub warunków, które powodują powstanie określonych typów ryzyka);
- **dzielenia ryzyka** (dzieleniu określonych typów ryzyka z zewnętrznymi stronami).

*warianty postępowania z ryzykiem nie wykluczają się wzajemnie

Krok 5: Postępowanie z ryzykiem

Przy podjęciu decyzji o konieczności zmodyfikowania poziomu ryzyka Jak wybrać odpowiednie zabezpieczenia?

Należy brać pod uwagę:

- wynik szacowania ryzyka
- oczekiwany koszt wdrażania zabezpieczenia
- oczekiwane korzyści z wdrożonych

*zaleca się aby rozważyć mitygowanie ryzyka o niskim prawdopodobieństwie wystąpienia mogącego powodować poważne skutki.

Krok 6: Akceptowanie ryzyka

Przy założeniu, że poziom ryzyka jest akceptowalny dla organizacji.

Należy pamiętać, że przy ustalaniu poziomu akceptacji ryzyka przetwarzania danych osobowych – **nie możemy akceptować wysokiego ryzyka** przetwarzania danych.

Cel kroku 6: formalne udokumentowanie decyzji o zaakceptowaniu ryzyka oraz odpowiedzialności za decyzję.

Działania do podjęcia: przyjęcie formalnego raportu z przeprowadzonego procesu zarządzania bezpieczeństwem informacji.

I już jesteśmy bezpieczni

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. Źródła metodyki analizy ryzyka
    1. Privacy Impact assessment (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. **Metodyka analizy ryzyka oparta o normy ISO**
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Matryca Analizy Ryzyka wg G&P

Kancelaria G&P w ramach zebranych doświadczeń pracy z organizacjami przy opracowywaniu analizy ryzka wypracowała własną metodologię podejścia do analizy ryzyka praw i wolności osób fizycznych.

Matryca opiera się o założenia normy ISO 27005 oraz materiały przygotowane przez UODO jak i doświadczenia w zakresie zarządzania bezpieczeństwem informacji.

Matryca ma formę pliku Excel.

Najważniejsze elementy Matrycy Analizy Ryzyka wg G&P

Proces analizy ryzyka składa się z:

1) Identyfikacji ryzyka (wymagane RCPD organizacji)
2) Oceny ryzyka
3) Postępowania z ryzykiem
4) Oceny ryzyka szczątkowego
5) Oceny czy jest konieczność przeprowadzenia DPIA

zapraszamy do przeprowadzenia analizy ryzyka

(część warsztatowa na pliku Excel)

Program

1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. Źródła metodyki analizy ryzyka
    1. Privacy Impact assessment (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. **Uproszczona analiza ryzyka dla małych przedsiębiorstw**
6. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Uproszczona analiza ryzyka - podstawy

Ryzyko przetwarzania danych osobowych jest rozumiane jako ryzyko naruszenia praw lub wolności osób fizycznych

Ryzyko przetwarzania ma dwa wymiary:

a) ryzyko nieupoważnionego dostępu lub wykorzystania danych osobowych (**ryzyko naruszenia poufności**), oraz

b) ryzyko niemożności wykorzystania danych osobowych w sposób przewidziany (**ryzyko niedostępności danych i ryzyko wadliwości danych**).

Cel analizy ryzyka - *celem jest określenie wysokości (poziomu) ryzyka i w konsekwencji wskazanie rekomendowanych środków bezpieczeństwa technicznego i organizacyjnego właściwych dla ustalonego poziomu ryzyka.*

Założenia uproszczonej metodyki

Na potrzeby ustalenia poziomów ryzyka oraz zastosowania uproszczonej metodyki, brane są pod uwagi następujące czynniki:

1) **branża** (sektor) lub podsektor – przyjmuje się, że branża, w której dochodzi do przetwarzania danych osobowych, ma wpływ na ryzyko przetwarzania danych osobowych

2) **klientela** - klientela, czyli osoby lub podmioty, do których kierujemy ofertę usług lub produktów. Określa ona bezpośrednio kategorie osób i danych, które są przedmiotem przetwarzania

3) **skala przetwarzanych danych** - czyli liczba rekordów danych osobowych (liczba klientów, pacjentów, pracowników etc) przetwarzanych. Im więcej osób „przetwarzamy", ale też im więcej osób po naszej stronie ma dostęp do danych, tym większe prawdopodobieństwo np. wycieku danych

4) **wysokość przychodów** (obroty) - wysokość osiąganych przychodów jest pochodną skali prowadzonej działalności, a potencjalnie im wyższa skala działalności, tym większa liczba danych przetwarzamy

Założenia uproszczonej metodyki

dalsze założenia metodyki:

1) łącznie czynniki branży (podsektoru) i klienteli wskazują na **ogólne ryzyko prowadzonej działalności dla praw i wolności osób, których dane są przetwarzane,**

2) ogólny poziom ryzyka prowadzonej działalności jest zestawiany ze skalą działalności, **dając łączny poziom ryzyka dla naruszenia praw lub wolności osób fizycznych, przy przetwarzaniu danych osobowych,** który dodatkowo przez administratora przeszacowany wzwyż w przypadku generowania dużych przychodów (dużego obrotu).

Założenia uproszczonej metodyki

3) metodyka ustalania poziomów ryzyka jest określana dla czynności przetwarzania stanowiących **główny przedmiot działalności administratora** np. dla lekarzy – są to czynności przetwarzania właściwe dla lekarzy

4) przyjmuje się, że ryzyko naruszenia praw i wolności, dla czynności przetwarzania związanych z bieżącą działalnością organizacji (niestanowiących głównego przedmiotu działalności, core biznesu), tj. czynności przetwarzania z obszaru księgowości, prowadzenia kadr/hr lub bieżącej działalności, **jest potencjalnie takie samo dla każdego rodzaju organizacji**

zapraszamy do przeprowadzenia analizy ryzyka

(część warsztatowa)

Program

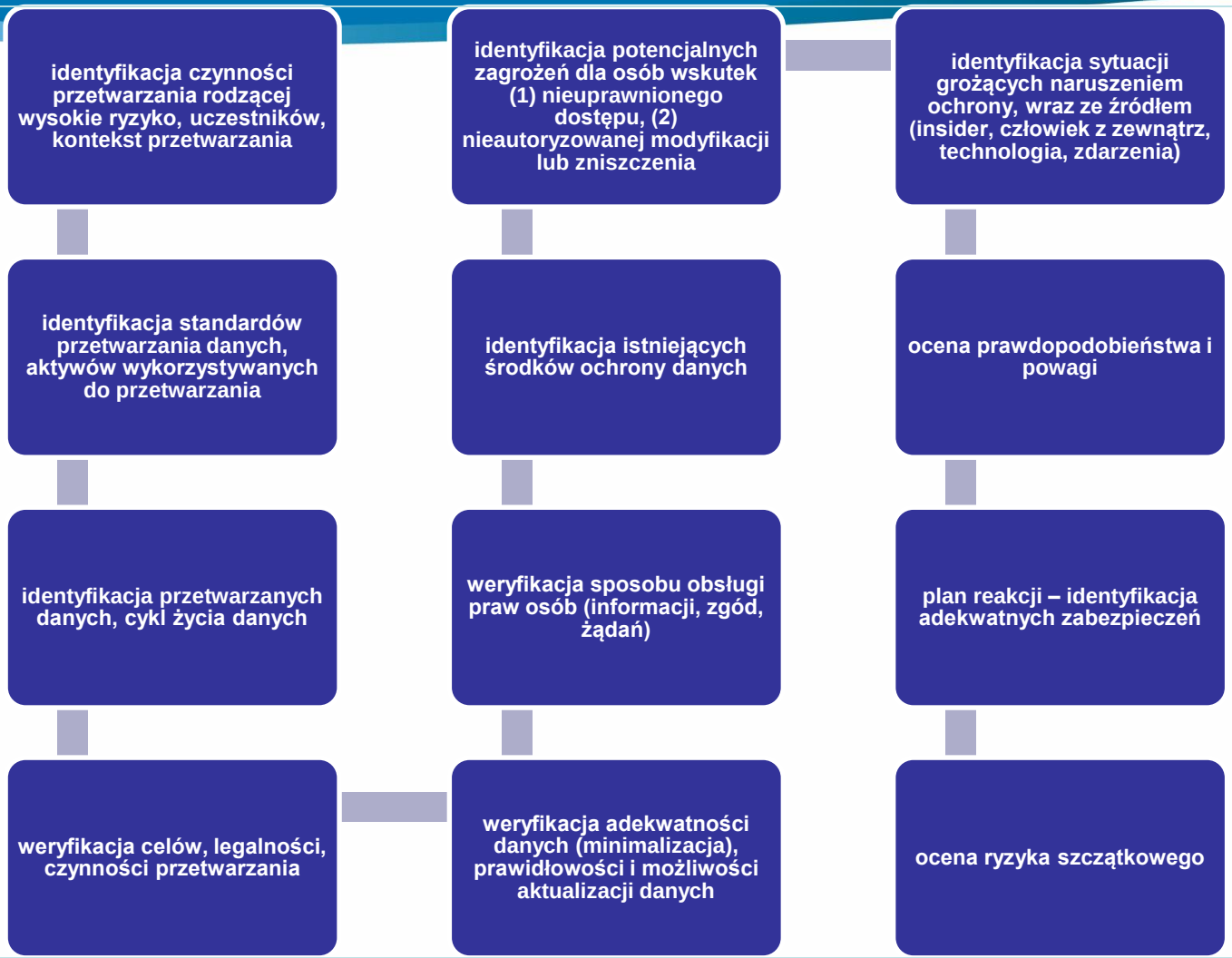
1. *Risk based approach* - podejście od strony ryzyka do przetwarzania i ochrony danych osobowych
2. Podstawy prawne analizy ryzyka
3. Źródła metodyki analizy ryzyka
    1. Privacy Impact assessment (PIA) CNIL
    2. Podejście oparte na ryzyku – materiały UODO
    3. Szacowanie ryzyka oparte o normy ISO (w tym: ISO 27005 i ISO 29134)
4. Metodyka analizy ryzyka oparta o normy ISO
5. Uproszczona analiza ryzyka dla małych przedsiębiorstw
6. **Ogólna ocena ryzyka a ocena skutków dla ochrony danych**

Ocena skutków dla ochrony danych (DPIA) Art. 35 ust. 1RODO

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.

Ocena skutków dla ochrony danych wg CNIL



DPIA w szczególności jest wymagane
Art. 35 ust. 3 RODO

a) **systematycznej, kompleksowej oceny czynników osobowych** odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) **przetwarzania na dużą skalę szczególnych kategorii danych osobowych**, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO;

c) **systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.**

Pierwszy wykaz rodzajów operacji wymagający przeprowadzenia DPIA

Art. 35 ust. 4 RODO

24 sierpnia 2018 r. w Monitorze Polskim został ogłoszony Komunikat PUODO z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających DPIA.

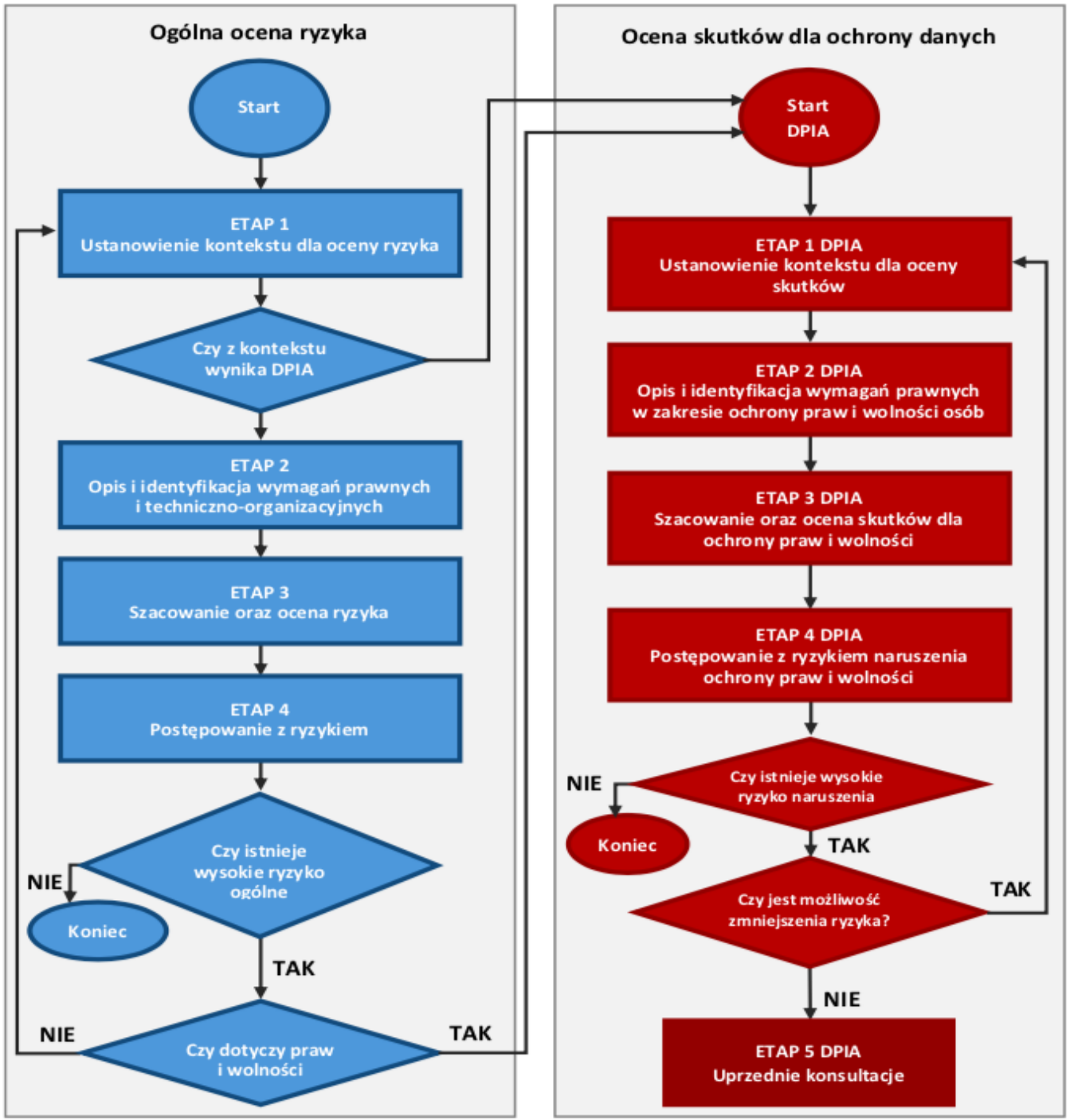
Ogłoszony wykaz **zawiera 9 kategorii rodzajów przetwarzania**, dla których obowiązkowe będzie dokonanie DPIA wraz z przykładami operacji, w których może wystąpić wysokie ryzyko naruszenia i przykładami potencjalnych obszarów obejmujących te operacje.

http://monitorpolski.gov.pl/MP/2018/827/

Kiedy należy przeprowadzić DPIA?

1) **poziom ryzyka został określony jako wysoki** w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania (dla planowanych i obecnych czynności przetwarzania)
2) rodzaj przetwarzania **został wskazany w przepisie prawa** (m.in. patrz art. 35 ust. 3 RODO)
3) dany rodzaj operacji przetwarzania **został wskazany w wykazie** podanym do publicznej wiadomości **przez PUODO**

Ogólna analiza ryzka a DPIA wg UODO



Gdy przetwarzanie powodowałoby wysokie ryzyko?

art. 36 ust. 1 RODO

Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby **administrator nie zastosował środków w celu zminimalizowania tego ryzyka?**

GDPR COMPLIANCE

To przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym!

enterprise europe network

Dziękujemy za uwagę

Maciej Gawroński
Patrycja Naklicka

PARP Grupa PFR / Centrum Rozwoju MŚP

2008-2018 enterprise europe network Business Support on Your Doorstep

European Commission

enterprise europe network

Zapraszamy do kontaktu

Gawroński & Partners s.k.a.
T: +48 22 243 49 53
E: info@gawronski.co
Al. Jana Pawła II 12
00-124 Warszawa

maciej.gawroński@gawronski.law
+48 609 602 566

www.een.org.pl

PARP Grupa PFR / Centrum Rozwoju MŚP

2008-2018 enterprise europe network Business Support on Your Doorstep

European Commission