GIODO
Generalny Inspektor Ochrony Danych Osobowych

Ryzyko w ochronie danych osobowych

Andrzej Kaczmarek
Dyrektor Departamentu Informatyki
Biuro Generalnego Inspektora Ochrony Danych Osobowych

Warszawa, 29 Stycznia 2018 r.

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

PLAN PREZENTACJI

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Pojęcie bezpieczeństwa, bezpieczeństwa informacji oraz bezpieczeństwa danych osobowych.
2. Źródła zagrożeń dla bezpieczeństwa informacji w tym bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów teleinformatycznych
3. Pojęcie ryzyka w zakresie bezpieczeństwa informacji oraz w zakresie ryzyka naruszenia praw i wolności osób fizycznych
4. Wytyczne i standardy odnoszące się do bezpieczeństwa informacji w SI
5. Jak przeprowadzać analizę ryzyka oraz analizę oceny skutków dla ochrony danych

Co to jest bezpieczeństwo?

Stan w którym jednostka […] nie odczuwa zagrożenia swego istnienia lub podstawowych interesów

Sytuacja, w której istnieje formalne, instytucjonalne, praktyczne gwarancje ochrony

Bezpieczeństwo informacji

Stan ochrony życiowo ważnych interesów społeczeństwa i państwa w środowisku imnformacyjnym od zagrożeń wewnętrznych i zewnętrznych (ANSI).

Zachowanie poufności, integralności i osiągalności informacji: PN-ISO/IEC 2000-1:2011
Dodatkowo można brać pod uwagę inne własności takie jak: autentyczność, rozliczalności niezaprzeczalność i niezawodność

Atrybuty bezpieczeństwa informacji wg normy PN-ISO/IEC 27000:2014

Atrybuty bezpieczeństwa: Nazwa - Definicja	
Poufność *(confidentiality)*	Właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom
Autentyczność *(Authenticity)*	Właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; dotyczy użytkowników, procesów, systemów, instytucji; autentyczność związana jest z badaniem, czy ktoś lub coś jest tym/czym za kogo/co się podaje.
Integralność danych *(data integrity)*	Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany
Integralność systemu *(system integrity)*	Właściwość polegająca na tym, że system realizuje swoja zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.

Atrybuty bezpieczeństwa informacji wg normy PN-ISO/IEC 27000:2014

Atrybuty bezpieczeństwa: Nazwa – Definicja c.d.	
Rozliczalność *(accountability)*	Właściwość zapewniająca, że działania podmiotu (np. użytkownika) mogą być jednoznacznie przyporządkowane tylko temu podmiotowi
Niezawodność *(reliability)*	Właściwość oznaczająca, spójne, zamierzone zachowanie i skutki.
Dostępność *(availability)*	Możliwość do wykorzystania na żądanie, w założonym czasie przez kogoś lub coś/co ma do tego prawo

System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji (SZBI) - z ang. ISMS (Information Security Management System) - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

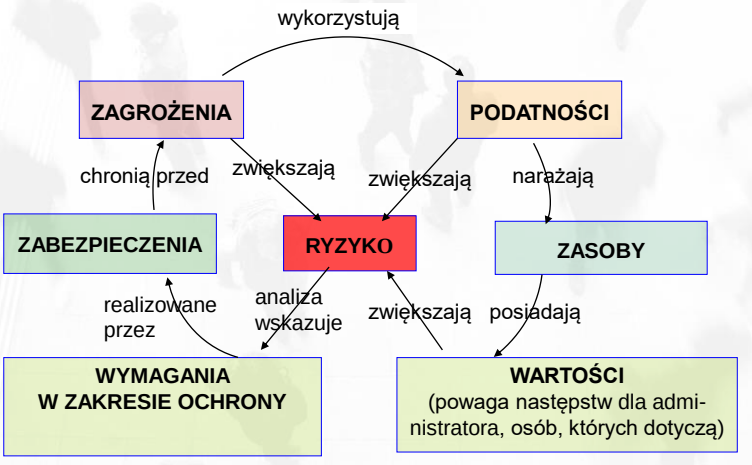
System zarządzania obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa)

Bezpieczeństwo informacji – proces zabezpieczania poufności, integralności i dostępności informacji

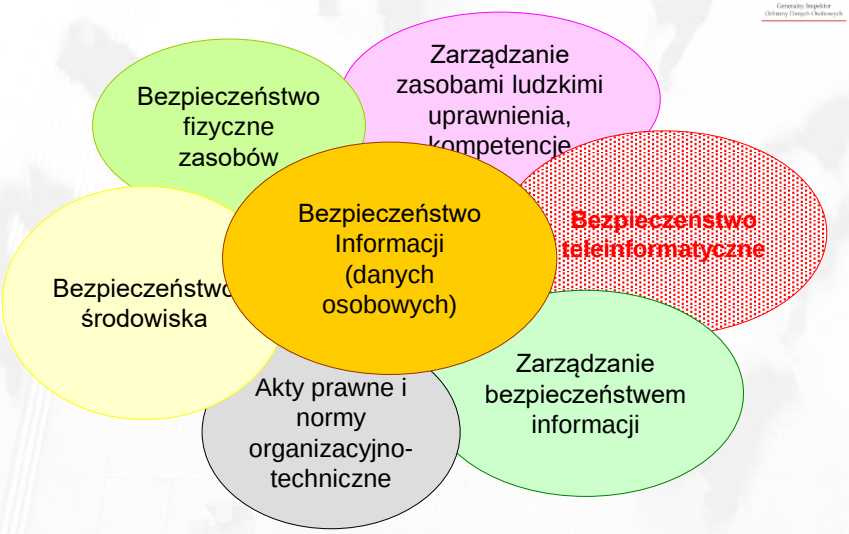
Inne pojęcia związane z bezpieczeństwem informacji

Inne pojęcia związane z bezpieczeństwem informacji - Definicje	
Zagrożenie *(Threat)*	Potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji [ISO/IEC 13335-1:2004]
Zasoby *(Assets)*	Wszystko, co ma wartość dla organizacji. [ISO/IEC 13335-1:2004]
Podatność *(Vulnerability)*	Słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń [ISO/IEC 13335-1:2004]
Ryzyko *(Risk)*	Kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji [ISO/IEC Guide 73:2002]
Zabezpieczenie *(Safeguard)*	Środki służące zarządzaniu ryzykiem, włączając polityki, procedury, zalecenia, praktyki lub struktury organizacyjne, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną.

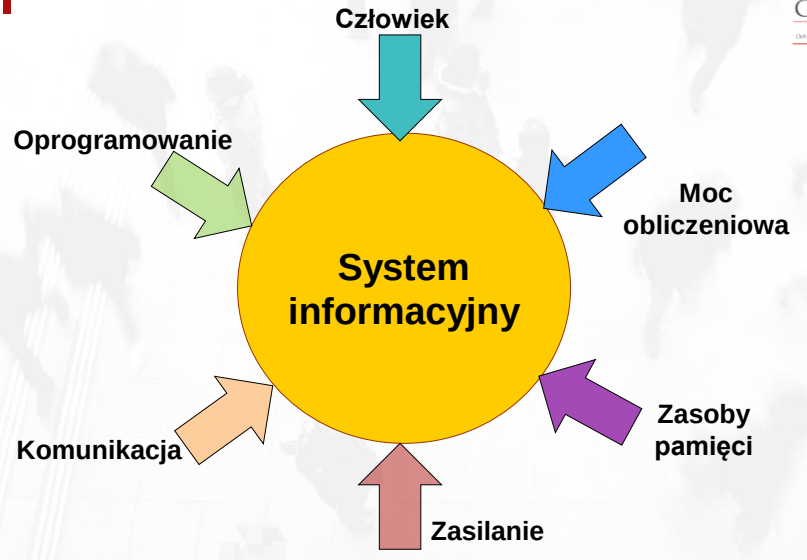
Model związków między elementami wpływającymi na bezpieczeństwo



Źródła zagrożeń dla bezpieczeństwa informacji, danych osobowych (I)



Źródła zagrożeń dla bezpieczeństwa informacji, danych osobowych (II)



Źródła zagrożeń związane z użyciem technologii teleinformatycznej i SI

GIODO

1. Jawność danych w fazie transmisji – podatność na ujawnienie, utratę integralności

- Protokół TCP/IP;
- protokół SMTP do obsługi poczty elektronicznej;
- protokół HTTP do przesyłania i udostępniania dokumentów hipertekstowych;
- Protokół SNMP służący do zdalnego sterowania komputerami, routerami i innymi urządzeniami w sieciach telekomunikacyjnych

- Protokół IPsec, IP v6
- protokół S/MIME - do bezpiecznego przesyłania poczty
- protokół HTTPs do bezpiecznego przesyłania i udostępniania dokumentów hipertekstowych;
- protokół SNMP v. 3 służący do bezpiecznego zarządzania komputerami, routerami i innymi urządzeniami w sieci.

Źródła zagrożeń związane z użyciem technologii teleinformatycznej i SI

GIODO

2. Korzystanie z sieci publicznych (poufność, integralność)

- Wspólne kablowe linie przesyłowe;
- Transmisja bezprzewodowa;
- Hotspoty: publicznie dostępne medium transmisji bezprzewodowej;
- Słabość zabezpieczeń kryptograficznych sieci bezprzewodowych.

Utrzymanie bezpieczeństwa systemu pracującego w środowisku sieciowym jest szczególnie trudne. Administrator odpowiedzialny za zabezpieczenie danych w takim środowisku jest - w porównaniu z atakującymi - na znacznie gorszej pozycji.

Żeby skutecznie zabezpieczyć system należy usunąć „wszystkie" jego słabości i podatności na znane rodzaje ataków, jak również ataki, które mogą pojawić się w najbliższej przyszłości, zaś aby skutecznie zaatakować - wystarczy znaleźć jedną słabość danego systemu i stosownie ją wykorzystać.

Źródła zagrożeń związane z użyciem technologii teleinformatycznej i SI

GIODO

3. Szkodliwe oprogramowanie (poufność, integralność, dostępność)

- Wirusy; Robaki; Trojany; Ransomware
- Backdoory; Rootkity;
- Keylogery; Spyware;
- Exploity;

Należy mieć na uwadze fakt, że:

Przy połączeniu systemu z siecią publiczną, jaką jest sieć Internet nad zabezpieczeniem systemu w sieci czuwa najczęściej jedna, a najwyżej kilka osób, podczas gdy nad złamaniem zastosowanych zabezpieczeń mogą pracować tysiące osób z różnych miejsc na całym świecie.

Źródła zagrożeń związane z użyciem technologii teleinformatycznej i SI

GIODO

4. Socjotechnika (poufność, integralność, dostępność)

Co to jest socjotechnika?

Jak stwierdził jeden z najbardziej znanych socjotechników, Kevin Mitnick, socjotechnika polega na „łamaniu" ludzi, a nie haseł.

- Rozmowa telefoniczna, podstęp;
- Phishing;
- Pfarming;

Jak chronić się przed atakami socjotechnicznymi?

Źródła zagrożeń związane z użyciem technologii teleinformatycznej i SI

5. Nowe narzędzia i technologie programistyczne

- Pliki *Cookies*;
- Technologia DPI (Głęboka Inspekcja Pakietów;
- Data maining,
- Rozpoznawanie obrazów, analiza intencji, nastrojów
- Standardowy język baz danych i wstrzykiwanie jego kodu do stron WWW (SQL injection);

- Zastosowania biometrii;
- Technologia RFID;
- Internet przedmiotów;
- Nawigacja drogowa.
- Geolokalizacja

Wymagania dotyczące bezpieczeństwa danych wynikające z u.o.d.o

Art. 36 u.o.d.o.

1. **Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (…).**
2. **Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.**

Art. 37 u.o.d.o.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Art. 38 u.o.d.o.

Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Wymagania dotyczące bezpieczeństwa danych wynikające z u.o.d.o / rozporządzenie wykonawcze

Art. 39a u.o.d.o.

Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych

Wymagania wskazane w załączniku do rozporządzenia

Wymagania dotyczące ochrony (załącznik do rozporządzenia)

Podstawowy

1) Zabezpieczenie obszaru przetwarzania;
2) Kontrola dostępu (indywidualne konto dla każdego użytkownika);
3) Zabezpieczenie przed szkodliwym oprogramowaniem i awarią zasilania;
4) Niepowtarzalność identyfikatora, odpowiednie parametry dotyczące hasła oraz obowiązek tworzenia kopi zapasowych;
5) Kryptograficzne zabezpieczenie komputerów przenośnych;
6) Odpowiednie procedury przenoszenia, likwidacji i napraw sprzętu;
7) Monitorowanie wdrożonych zabezpieczeń;

Podwyższony

8) Dodatkowa wymagania dotyczące hasła dla danych wrażliwych;
9) Dodatkowe zabezpieczenie danych wrażliwych opuszczających obszar przetwarzania (ochrona kryptograficzna);

Wysoki

10) Opis sposobu zabezpieczenia o którym mowa w punkcie 9 i jego ochrona;
11) Kontrola i zabezpieczenie przepływy danych na styku z siecią publiczną;
12) Kryptograficzna ochrona danych przesyłanych w sieci publicznej;

Wymagana określone w RODO

Obowiązki administratora. (Art. 24 rodo)

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych. (Art. 25 rodo)

1. Uwzględniając charakter, zakres, kontekst, cele i ryzyko administrator zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, minimalizacja danych i inne zabezpieczenia w celu skutecznej realizacji zasad ochrony danych, aby chronić prawa osób, których dane dotyczą.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Sugerowane w RODO środki bezpieczeństwa

1. Pseudonimizacja i szyfrowanie danych
   - rozdzielenie danych identyfikacyjnych od pozostałych, jak zorganizować ?
   - jak zapewnić ścisłą kontrola dostępu do danych identyfikacyjnych i sposobu ich połączenia z pozostałymi danymi ?
   - kiedy dane należy szyfrować ?
   - jaką zastosować metodę szyfrowania ?
   - kryptografię symetryczną (EAS, Twofish – jak długi klucz 128,192, 256 bitów ?)
   - kryptografię asymetryczną (RSA, DSA, Diffie-Hellmana – klucz 512 , 1024 - 4096)
   - a może wystarczy funkcja hashująca (skrótu); SHA-2, SHA-3, RIPMD-160?
   - wprowadzić zasady zarządzania kluczami kryptograficznymi
2. Zapewnienie zdolności do ciągłego zapewniania poufności, integralności, dostępności i odporności usług przetwarzania.
   - jakie zastosować rozwiązania dla zapewnienia ciągłości poufności i integralności?
   - czy dedykowana indywidualnie kontrola dostępu i suma kontrolna będą wystarczające?
   - czy niezbędne jest szyfrowania i podpis elektroniczny ? jak zarządzać kluczami?

Wymagania określone w RODO i związane z nimi ryzyko

GIODO

Kradzież baz danych osobowych
Brak dostępności
✓Ransomware
✓DDoS
Naruszenie integralności, poufności

→ **Ryzyko w bezpieczeństwie przetwarzania**

Żądanie
✓informacji od administratora
✓zaprzestania przetwarzania
✓usunięcia/przeniesienia danych
✓…….
Naruszenie ochrony danych

→ **Ryzyko nie wykonania obowiązków formalnych**

Uwzględnienie ryzyka przy projektowaniu i zarządzaniu bezpieczeństwem przetwarzania

Ocena wpływu przetwarzania na prawa i wolności podmiotów danych

→ **Ocena ryzyka / skutków naruszenia praw (DPIA)**

Ryzyka wynikające z nakładania się różnych zagrożeń - przykład

GIODO

Faktura
Standardowe
-numer faktury
-lista badań,
-cena
-dane pacjenta
-dane sprzedawcy
-numer zlecenia badań + kod

Paragon
Karta zlecenia badania
-numer zlecenia
-kod kreskowy
-lista badań

Szacowanie ryzyka a systemy zarządzania

Normy, dobre praktyki, kodeksy postępowania

- ✓ Bezpieczeństwo informacji PN-ISO/IEC 27001, PN-ISO/IEC 27002
- ✓ Jakość, zarządzanie jakością PN-ISO/IEC 9001:2015
- ✓ Ciągłość działania PN-ISO/IEC 22301:2014
- ✓ Właściwa organizacja przetwarzania (zasady, legalność, obowiązki informacyjne – RODO; ISO/IEC 29100:2011 Bezpieczeństwo informacji – Ramy prywatności

Zarządzanie ryzykiem

- ✓ Ryzyka i szanse ISO 31000, inne publikacje np. „Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk” *
- ✓ Zarządzanie ryzykiem w bezpieczeństwie informacji PN-ISO/IEC 27005:2011
- ✓ Ocena skutków przetwarzania ISO/IEC 29134:2017 Guidelines for privacy impact assessment
- ✓ Postępowanie z ryzykiem, konsultacje z organem nadzorczym

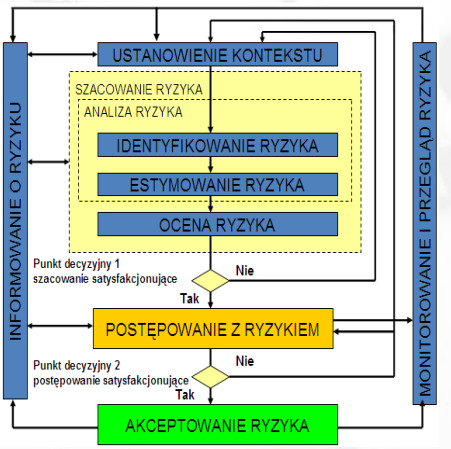
* Publikacja jest ogólnie dostępna, finansowana przez NCBIR w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”

Szacowanie ryzyka w bezpieczeństwie informacji

Identyfikacja ryzyka w BI (PDO)

- ✓ Identyfikacja aktywów
- ✓ Identyfikacja zagrożeń - ich prawdopodobieństwa wystąpienia
- ✓ Identyfikacja podatności (środowiska przetwarzania)
- ✓ Identyfikacja zabezpieczeń i ich skuteczności
- ✓ Identyfikacja następstw

Analiza ryzyka- PN-ISO/IEC 27005)



Proces zarządzania ryzykiem w bezpieczeństwie informacji wg PN-ISO/IEC 27005

Szacowanie ryzyka - ustanowienie kontekstu

Ustanowienie kontekstu to 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.

Informacje dotyczące:

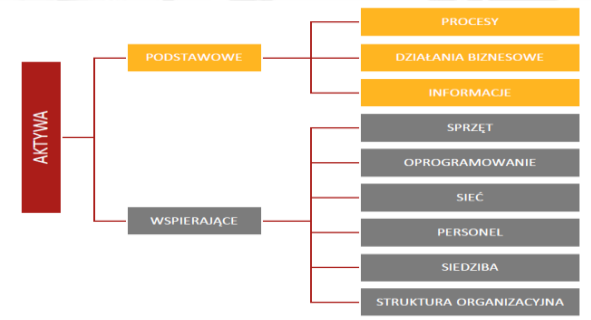
- ✓ **strukturę i rozmiary organizacji,**
- ✓ **strategie i stosowane polityki,**
- ✓ **system obiegu informacji, procesy, decyzje, rola przywództwa,**
- ✓ **informacje dotyczące środowiska technologicznego i organizacji,**
- ✓ **normy i kodeksy (kultura organizacyjna).**

Informacje dotyczące:

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

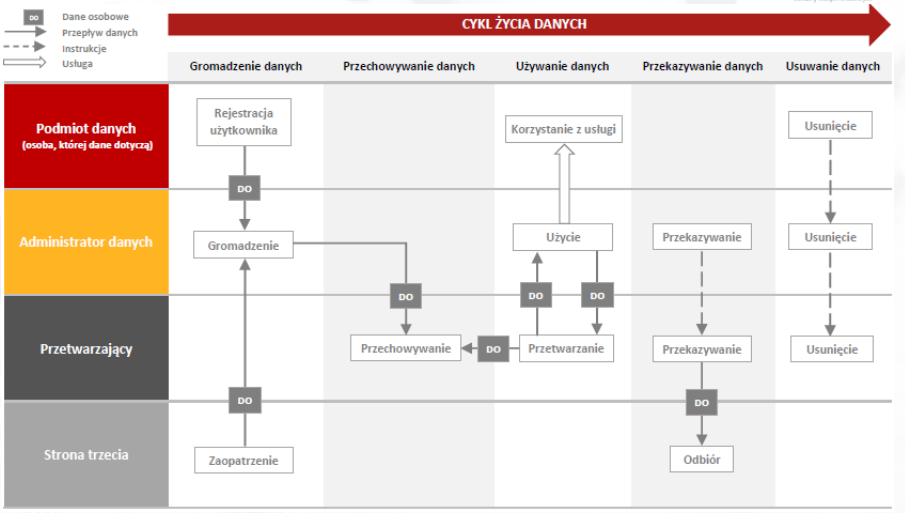
Kontekst – opis, identyfikacja i klasyfikacja

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

Kontekst – uwzględnienie całego cyklu przetwarzania



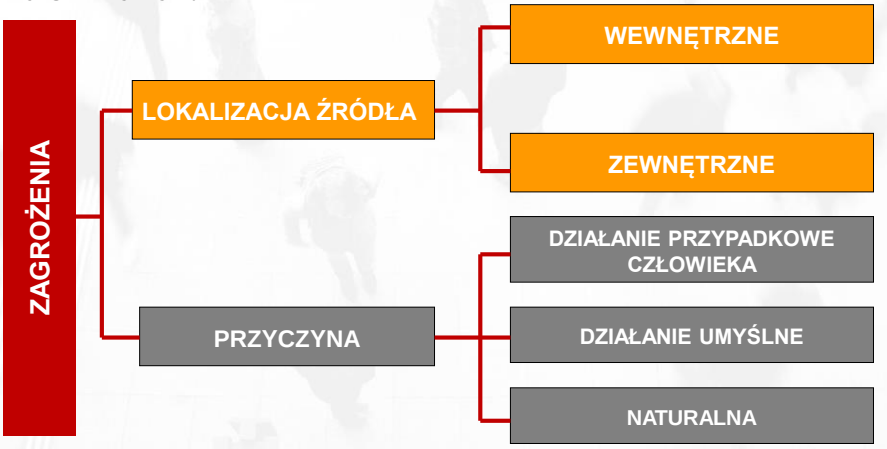
Kontekst – uwzględnienie zabezpieczeń i kontroli

W celu określania istniejących zabezpieczeń można wykorzystać:

- regulacje już funkcjonujące w organizacji (np. polityki, regulaminy i instrukcje),
- dokumentację wdrożonych rozwiązań technicznych i fizycznych.

Identyfikacja zagrożeń

Do identyfikacji zagrożeń wykorzystuje się różne klasyfikacje, np. zagrożenia można podzielić ze względu na lokalizację źródła zagrożenia oraz ze względu na jego przyczynę



Identyfikacja podatności na urzeczywistnienie zagrożeń

Dla poszczególnych aktywów można wyróżnić wiele podatności.

Przykładowe podatności wg normy PN-ISO/IEC 27005

Ocena skutku dla poszczególnych zagrożeń

Podczas doboru wartości przypisywanej skutkowi utraty poufności S_p należy przyjąć następujące zasady:

1) Jeżeli utrata poufności dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć **$S_p = 1$.**
2) Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć **$S_p = 2$.**
3) Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, wpływa w sposób znaczący na wizerunek urzędu i organu, który ten urząd obsługuje, jednak nie wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, jednak może wiązać się z odpowiedzialnością administracyjną, należy przyjąć **$S_p = 3$**.
4) Jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i może prowadzić do roszczeń odszkodowawczych ze strony tych osób, a także do odpowiedzialności karnej osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć **$S_p = 4$.**

Ocena skutku dla poszczególnych kategorii (atrybutów bezpieczeństwa)

Podczas doboru wartości przypisywanej skutkowi utraty integralności S_i należy przyjąć następujące zasady:

1) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest łatwo wykrywalna i przywrócenie integralności nie powoduje nadmiernych kosztów należy przyjąć **$S_i = 1$.**
2) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych, jednak istnieje możliwość skorygowania decyzji należy przyjąć **$S_i = 2$.**
3) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych i nie istnieje możliwość skorygowania decyzji należy przyjąć **$S_i = 3$**.
4) Jeżeli spowodowana zagrożeniem utrata integralności informacji może okazać się niewykrywalna należy przyjąć **$S_i = 4$.**

Ocena skutku dla poszczególnych kategorii (atrybutów bezpieczeństwa)

Podczas doboru wartości przypisywanej skutkowi utraty dostępności S_d należy przyjąć następujące zasady:

1) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany materializacją zagrożenia, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), a przywrócenie pełnego dostępu do informacji lub usług systemu nie wiąże się z dodatkowymi kosztami należy przyjąć **S_d = 1**.
2) Jeżeli okres czasu utraty dostępności informacji lub usług, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), ale przywrócenie dostępu do informacji wiąże się z dodatkowymi kosztami należy przyjąć **S_d = 2.**
3) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, znacząco nie mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO) należy przyjąć **S_d = 3.**
4) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, wielokrotnie przekracza czas założony w planie zapewnienia ciągłości działania (RTO) lub jeżeli spowodowana zagrożeniem utrata dostępności informacji jest nieodwracalna należy przyjąć **S_d = 4**.

Wyliczanie poziomu ryzyka

Poziom ryzyka można wyliczyć według następującego wzoru:

$$R_p = P \times (S_d + S_i + S_p)$$

Rp – pierwotny poziom ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,

Gdzie: ***P ϵ {0,1,2,3,4}***

***0** – zdarzenie nieprawdopodobne (zagrożenie nie występuje),*
***1** – zdarzenie prawie nieprawdopodobne,*
***2** – zdarzenie mało prawdopodobne,*
***3** – zdarzenie wysoce prawdopodobne,*
***4** – zdarzenie niemal pewne.*

Wyliczanie poziomu ryzyka

Poziom ryzyka można wyliczyć według następującego wzoru:

$$R_p = P \times (S_d + S_i + S_p)$$

Rp – pierwotny poziom ryzyka,
P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,
Gdzie: ***P є {0,1,2,3,4}***

***S_d** – wartość przypisana skutkowi dla dostępności informacji,*
***S_i** – wartość przypisana skutkowi dla integralności informacji,*
***S_p** – wartość przypisana skutkowi dla poufności informacji,*

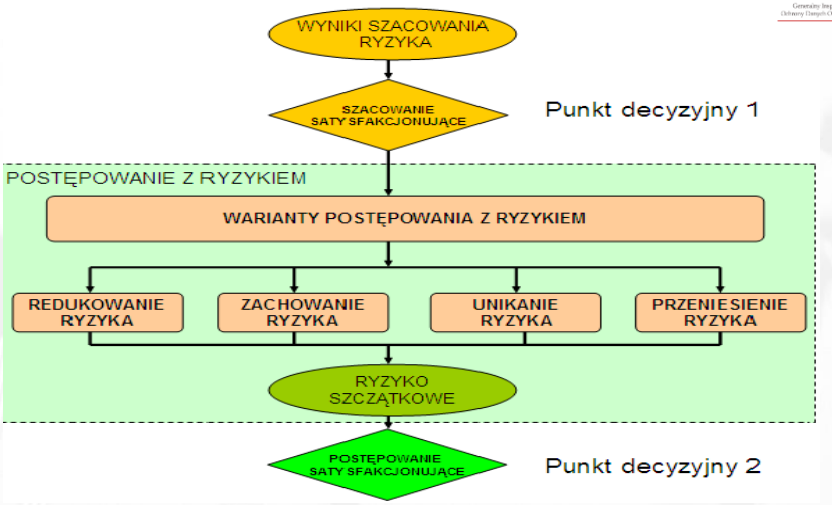
Gdzie: ***(S_d, S_i, S_p) є {0,1,2,3,4}***

0 – zdarzenie nie powoduje skutku (brak podatności),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

Przykład

Grupa aktywów	Rodzaj aktywu	Zagrożenie	Podatność	Prawdopo-dobieństwo	Skutek	Wartość ryzyka	Poziom ryzyka
Systemy, programy, aplikacje	Poczta MS Exchange 2016	Utrata poufności	Słabość protokołu. Brak szyfrowania, brak cert. ID.	3	Sp = 3 Si = 2 Sd = 2	3x7 = 21	Ryzyko średnie
Systemy, programy, aplikacje	Windows Xp	Utrata poufności, Integralności, dostępności	Brak odporności na zagrożenia, Brak aktualizacji	3	Sp = 3 Si = 3 Sd = 3	3x9 =27	Ryzyko wysokie
Systemy, programy, aplikacje	System obiegu dokume-ntów	Utrata dostępności, Nieuprawniony dostęp	Błąd konfiguracji. Złe uprawnienia.	2	Sp = 1 Si = 2 Sd = 2	2x5 = 10	Ryzyko niskie
Personel własny	Pracownicy, w tym administrat orzy SI.	Bezprawne ujawnienie., Bezprawne użycie danych	Brak doświadczenia. Brak świadomości. Brak wiedzy	2	Sp = 2 Si = 2 Sd = 2	2x6 - 12	Ryzyko średnie

Szacowanie ryzyka w bezpieczeństwie informacji



Postępowanie z ryzykiem wg PN- PN-ISO/IEC 27005

Uwzględnienie oceny skutków. Jak zrealizować?

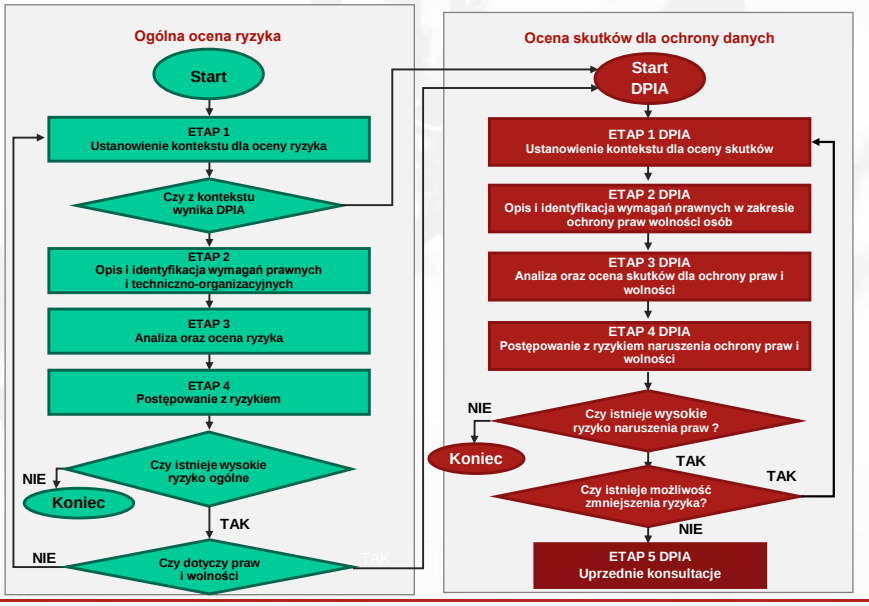
Wskazówki dotyczące oceny skutków dla ochrony danych – motyw 75 RODO

Ryzyko naruszenia praw lub wolności.

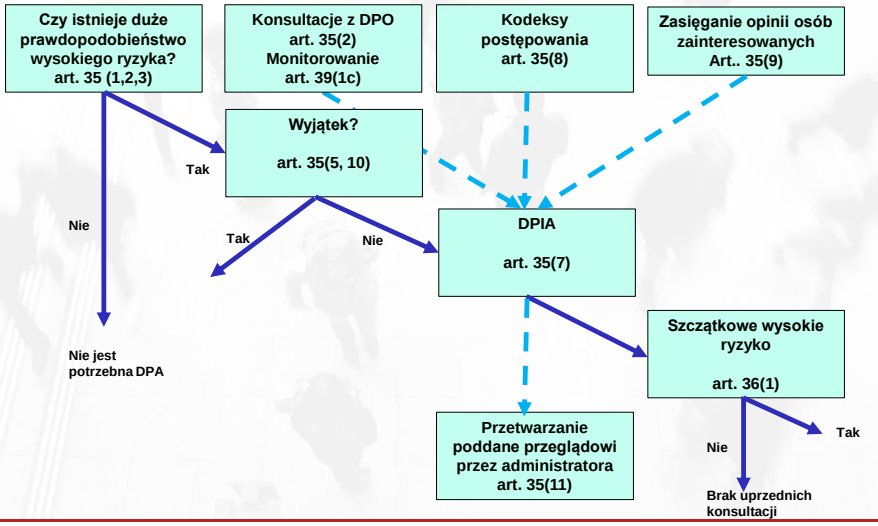
Dotyczy sytuacji gdy:

- 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 oceny skutków. Jak zrealizować?



Kiedy należy przeprowadzić ocenę skutków dla ochrony danych wg opinii Grupy Art. 29 ?



Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Art. 35 RODO wskazuje, że DPIA powinno być przeprowadzane jeżeli dane przetwarzane są w szczególności z użyciem nowych technologii i może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena taka jest wymagana w szczególności w przypadku:

1) 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;
2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art.. 10) lub
3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

Wytyczne wskazują, że DPIA nie jest wymagane, jeżeli:

- przetwarzanie „z dużym prawdopodobieństwem nie spowoduje wysokiego ryzyka naruszenia praw lub wolności osób fizycznych” (art. 35 ust. 1),
- charakter, zakres, kontekst i cele przetwarzania są bardzo podobne to przetwarzania, dla którego została dokonana DPIA (art. 35 ust. 1),
- 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).

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

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;

Uprzednie konsultacje

Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29

- 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);

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Polecana literatura:

•Wytyczne dotyczące oceny skutków dla ochrony danych (WP 248):
http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

•Wytyczne dotyczące inspektorów ochrony danych (WP 243)
http://www.giodo.gov.pl/pl/file/12390

•Zarządzanie ryzykiem. Przegląd wybranych metodyk; red. Dariusz Wróblewski, Wyd. CNBOP-PIB, Józefów 2015 https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf

Dziękuję za uwagę.

Dr inż. Andrzej Kaczmarek, CISA
Biuro Generalnego Inspektora Ochrony Danych Osobowych