FBI Polska
FUNDACJA BEZPIECZEŃSTWA INFORMACJI POLSKA

Wydanie 1.0

Metodyka zarządzania ryzykiem w ochronie danych osobowych

Warszawa 2018

METRYKA DOKUMENTU

Prawa własności	Fundacja Bezpieczeństwa Informacji Polska
Podstawa opracowania	Rozprawa doktorska mgr Kamila Pszczółkowskiego pt. *"Metodyka zarządzania ryzykiem w ochronie danych osobowych"*
Licencja wykorzystania	Dokument oparty o licencje Creative Commons typu CC BY-NC-ND Licencja ta pozwala na pobieranie utworu i dzielenie się nim z innymi, tak długo jak autorstwo zostaje uznane, a utwór nie jest modyfikowany lub wykorzystywany komercyjnie. Rozpowszechnianie utworu w celach komercyjnych jest możliwe po zyskaniu zgody Fundacji Bezpieczeństwa Informacji Polska.
Kontakt	Wszelkie pytania, uwagi lub propozycje doskonalenia metodyki proszę zgłaszać do na adres e-mail: kamil.pszczolkowski@fbipolska.pl
Wersja	1.0
Liczba stron	57

HISTORIA ZMIAN DOKUMENTU

Do wydania	Data zmiany	Opis zmiany

Spis treści

Terminy i definicje

Akceptowanie ryzyka	Decyzja, aby zaakceptować ryzyko [źródło PKN-ISO Guide 73].
Czynności przetwarzania	Zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
Analiza ryzyka	Systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka [źródło PKN-ISO Guide 73].
Bezpieczeństwo danych osobowych	Zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania.
Dostępność	Właściwość bycia dostępnym i użytecznym na zadanie autoryzowanego podmiotu [źródło ISO/IEC 27000].
Działanie korygujące	Działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanej sytuacji [źródło ISO 9000].
Działanie zapobiegawcze	Działanie w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanej [źródło ISO 9000].
Grupa zasobów	Zbiór zasobów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność.
Incydent związany z bezpieczeństwem danych osobowych	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo naruszenia praw lub wolności osób fizycznych.
Informowanie o ryzyku	Wymiana lub dzielenie się informacjami o ryzyku między decydentami, a innymi uczestnikami [źródło PKN-ISO Guide 73].
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności zasobów [źródło ISO/IEC 27000].
Kryteria ryzyka	Odniesienia, względem których szacowana jest istotność ryzyka [źródło PKN-ISO Guide 73].
Monitorowanie ryzyka	Ciągłe sprawdzanie, nadzorowanie, krytyczne obserwowanie lub określanie stanu prowadzone w celu zidentyfikowania zmian w zakresie wymaganego lub oczekiwanego poziomu skuteczności [źródło PN-ISO 31000].
Ocena ryzyka	Proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka [źródło PKN-ISO Guide 73].
Podatność	Słabość zasobu lub zabezpieczenia, która może być wykorzystana przez zagrożenie [źródło ISO/IEC 27000].
Postępowanie z ryzykiem	Proces wyboru i wdrażania środków modyfikujących ryzyko [źródło PKN-ISO Guide 73].

Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom [źródło ISO/IEC 27000].
Przegląd	Działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności przedmiotu rozważań do osiągnięcia ustalonych celów [źródło PN-ISO 31000].
RODO	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.
Ryzyko	Kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji [źródło PKN-ISO Guide 73].
Ryzyko bezpieczeństwa danych osobowych	Potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, powodując w ten sposób szkodę oraz w rezultacie negatywne / niepożądane konsekwencje.
Ryzyko akceptowalne	Poziom ryzyka niepowodujący lub ograniczający wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
Ryzyko szczątkowe	Ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem [źródło PN-ISO 31000].
Skuteczność	Stopień, w jakim zaplanowane działania są realizowane, a zaplanowane rezultaty osiągnięte [źródło ISO 9000].
Skutek	Konsekwencje urzeczywistnienia się zagrożenia naruszenia praw lub wolności osób fizycznych lub bezpieczeństwa informacji.
Szacowanie ryzyka	Całościowy proces analizy i oceny ryzyka [źródło PKN-ISO Guide 73].
Właściciel zasobu	Osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo zasobów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do zasobu.
Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną [źródło ISO/IEC 27000].
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać naruszenie praw lub wolności osób fizycznych.
Zarzadzanie ryzykiem	Skoordynowane działania, mające na celu kierowanie i zarządzanie organizacją z uwzględnieniem ryzyka [źródło PKN-ISO Guide 73].
Zasada "need to know"	Zasada wiedzy koniecznej, tzn. udzielenie tylko informacji potrzebnych do realizacji powierzonych zadań.

Zasoby	Wszystko, co ma wartość dla każdego, kto zajmuje się przetwarzaniem informacji umożliwiających identyfikację osoby fizycznej [źródło ISO/IEC 29134:2017].
Zdarzenie	Wystąpienie szczególnego zbioru okoliczności [źródło PKN-ISO Guide 73].
Zdarzenie związane z bezpieczeństwem danych osobowych	Określony stan, który wskazuje na możliwe naruszenie bezpieczeństwa danych osobowych, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem danych osobowych.

1. Wprowadzenie

Niniejsza metodyka została opracowana na podstawie rozprawy doktorskiej mgr Kamila Pszczółkowskiego pt. „*Metodyka zarządzania ryzykiem w ochronie danych osobowych*”, na zlecenie Fundacji Bezpieczeństwa Informacji Polska.

Celem Fundacji jest podejmowanie działań na rzecz wspierania bezpieczeństwa informacyjnego i cyberprzestrzeni w Polsce, budowanie świadomości w zakresie bezpieczeństwa oraz świadomego wykorzystania Internetu, przegląd skuteczności i efektowności stosowanych zabezpieczeń, w tym projektowanie i propagowanie nowych rozwiązań organizacyjnych i technicznych powodujących wzrost bezpieczeństwa w kraju.

Prezentowana metodyka jest zgodna z:

a) Rozporządzeniem 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 (w skrócie RODO);

b) Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW;

c) Wytyczne Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218 w sprawie oceny oddziaływania na ochronę danych i określenia czy przetwarzanie "może prowadzić do wysokiego ryzyka" w rozumieniu rozporządzenia 2016/679.

2. Założenie funkcjonowania procesu zarządzania ryzykiem

Zarządzanie ochroną danych osobowych oparte na ryzyku ma na celu:

a) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
b) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
c) ocenę czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zarządzanie ryzykiem w ochronie danych osobowych jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie.

Stosowana przez organizację metodyka zarządzania ryzykiem ma zapewnić porównywalne i powtarzalne rezultaty, poprzez zastosowanie standaryzacji skal oceny oraz sposobu przeprowadzania analizy, niezależnie od tego, kto będzie przeprowadzał analizę i ocenę ryzyka danych osobowych w organizacji.

Zgodnie z dobrymi praktykami oraz opinią Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218, zaleca się by zarządzanie ryzykiem w ochronie danych osobowych zapewniało:

a) zidentyfikowanie operacji przetwarzania danych osobowych o wysokim ryzyku naruszenia praw lub wolności osób fizycznych;
b) oszacowanie ryzyka z punktu widzenia ich skutków urzeczywistnienia ryzyka naruszenia praw lub wolności osób fizycznych oraz prawdopodobieństwa ich wystąpienia;
c) postępowanie z ryzykiem w celu zredukowania ryzyka;
d) informowanie o ryzyku interesariuszy i konsultacje eksperckie;
e) monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem.

Ocena skutków powinna być uruchamiana na etapie projektowania czynności przetwarzania, nawet jeśli niektóre czynności przetwarzania są wciąż nieznane. Konieczne może być powtórzenie poszczególnych etapów oceny skutków w miarę postępu procesu projektowania, ponieważ wybór niektórych środków technicznych lub organizacyjnych może mieć wpływ na wagę lub prawdopodobieństwo wystąpienia zagrożeń związanych z przetwarzaniem danych osobowych.

Wymaganie aktualizacji przeprowadzonej oceny skutków dla ochrony danych osobowych po rozpoczęciu procesu przetwarzania nie jest ważnym powodem odłożenia lub braku realizacji oceny na etapie projektowania rozwiązania. W niektórych przypadkach ocena skutków będzie procesem ciągłym, na przykład, gdy proces przetwarzania jest dynamiczny i podlega ciągłym zmianom.

Warto podkreślić, że ocena skutków dla ochrony danych w rozumieniu RODO jest narzędziem do zarządzania ryzykiem w kontekście ochrony praw lub wolności osób fizycznych, których dane dotyczą. Natomiast w zarządzaniu ryzykiem bezpieczeństwa informacji skupiamy się na ryzykach i konsekwencjach dla organizacji, a nie na osobach fizycznych. Konteksty te nie wykluczają się wzajemnie jednakże należy o nich pamiętać przy wykonywaniu oceny ryzyka.

Aktualnie tematyka zarządzania ryzykiem w ochronie danych osobowych jest nowym obszarem, gdzie brakuje opracowań i praktycznych wskazówek dotyczących sposobu realizacji i oceny ryzyka.

3. Proces zarządzania ryzykiem w ochronie danych osobowych

Poniższy diagram nr 1 prezentuje proces zarządzania ryzykiem w ochronie danych osobowych.

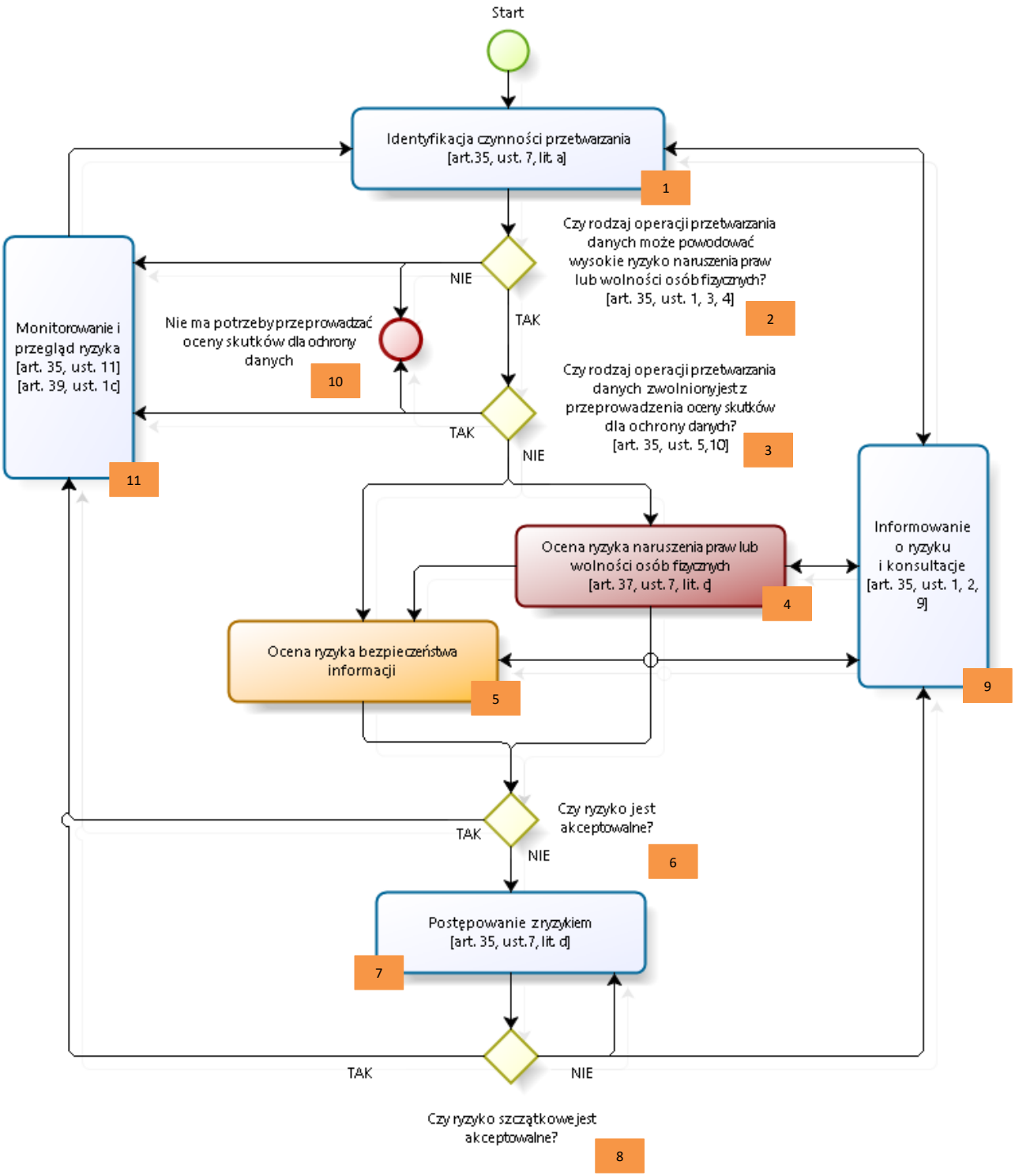

Diagram 1. Proces zarządzania ryzykiem w ochronie danych osobowych
Źródło: Opracowanie własne

3.1. Opis procesu zarządzania ryzykiem

Poniżej zostały opisane działania wynikające z realizacji procesu zarządzania ryzykiem w ochronie danych osobowych. Na diagramie nr 1, kolorem pomarańczowym zostały zaznaczone poszczególne kroki realizacji działań.

Krok	Działanie	Opis działania
1.	Identyfikacja czynności przetwarzania	Realizacja działania została opisana w rozdziale 4 niniejszego dokumentu.
2.	Ocena, czy rodzaj czynności przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych	Po przeprowadzeniu identyfikacja czynności przetwarzania (krok nr 1). Należy odpowiedzieć na pytanie na zasadzie TAK/NIE, czy dany rodzaj operacji przetwarzania danych w ramach zidentyfikowanego czynności przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? W przypadku pozytywnej odpowiedzi (TAK), przechodzimy do realizacji kroku nr 3. W przypadku negatywnej odpowiedzi (NIE), przechodzimy do realizacji kroku nr 10.
3.	Ocena, czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych	Po realizacji kroku nr 2. Należy odpowiedzieć na pytanie na zasadzie TAK/NIE, czy dany rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych? W przypadku pozytywnej odpowiedzi (TAK), przechodzimy do realizacji kroku nr 10. W przypadku negatywnej odpowiedzi (NIE), przechodzimy do realizacji kroku nr 4.
4.	Ocena ryzyka naruszenia praw lub wolności osób fizycznych	Należy dokonać oceny ryzyka naruszenia praw lub wolności osób fizycznych, w ramach której należy przeprowadzić: a) Identyfikację zagrożeń naruszenia praw lub wolności osób fizycznych (realizacja działania została opisana w rozdziale 5.1 niniejszego dokumentu); b) Ocena skutków urzeczywistnienia się zagrożeń (realizacja działania została opisana w rozdziale 5.2 niniejszego dokumentu); c) Ocenę prawdopodobieństwa urzeczywistnienia się zagrożenia (realizacja działania została opisana w rozdziale 5.3 niniejszego dokumentu); d) Ocenę powagi ryzyka naruszenia praw lub wolności osób fizycznych (realizacja działania została opisana w rozdziale 5.4 niniejszego dokumentu). Równolegle realizując działania powyższego kroku, realizujemy krok nr 9.
5	Ocena ryzyka bezpieczeństwa informacji	Poniższe działanie nie jest wymaga z punkty zapewnienia zgodności RODO, jednakże umożliwia definiowanie adekwatnych zabezpieczeń względem zasobów uczestniczących w przetwarzaniu danych osobowych.

Krok	Działanie	Opis działania
		Należy dokonać oceny bezpieczeństwa informacji, w ramach której należy przeprowadzić: a) Identyfikację zagrożeń bezpieczeństwa informacji (realizacja działania została opisana w rozdziale 6.1 niniejszego dokumentu); b) Identyfikacja podatności zasobów (realizacja działania została opisana w rozdziale 6.2 niniejszego dokumentu); c) Określenie istotności aktywów uczestniczących w przetwarzaniu danych osobowych (realizacja działania została opisana w rozdziale 6.3.1 niniejszego dokumentu); d) Określenie powagi podatności dla zasobów (realizacja działania została opisana w rozdziale 6.3.2 niniejszego dokumentu); e) Ocena skutków urzeczywistnienia się zagrożeń bezpieczeństwa informacji (realizacja działania została opisana w rozdziale 6.4 niniejszego dokumentu); f) Ocenę prawdopodobieństwa urzeczywistnienia się zagrożenia bezpieczeństwa informacji (realizacja działania została opisana w rozdziale 6.5 niniejszego dokumentu); g) Ocenę powagi ryzyka bezpieczeństwa informacji (realizacja działania została opisana w rozdziale 6.6 niniejszego dokumentu). Równolegle realizując działania powyższego kroku, realizujemy krok nr 9.
6.	Ocena, czy ryzyko jest akceptowalne	Po przeprowadzeniu kroku 4 i 5. Należy ocenić, na zasadzie TAK/NIE, czy ryzyko związane z naruszeniem praw lub wolności osób fizycznych i bezpieczeństwa informacji (jeśli było oceniane) jest akceptowalne (patrz rozdział 5.4 i 6.6)? W przypadku pozytywnej odpowiedzi (TAK) przechodzimy do realizacji kroku nr 11. W przypadku negatywnej odpowiedzi (NIE), przechodzimy do realizacji kroku nr 7.
7.	Postępowania z ryzykiem	Po realizacji kroku nr 6. Należy przeprowadzić postępowanie z ryzykiem. Realizacja działania została opisana w rozdziale 7 niniejszego dokumentu. Równolegle realizując działania powyższego kroku, realizujemy krok nr 9. W wyniku zakończenia realizacji działań kroku nr 7 przechodzimy do kroku nr 8.
8.	Ocena, czy ryzyko szczątkowe jest akceptowalne	Po przeprowadzeniu kroku 7. Należy ocenić, na zasadzie TAK/NIE, czy ryzyko szczątkowe związane z naruszeniem praw lub wolności osób fizycznych i bezpieczeństwa informacji (jeśli było ocenianie) jest akceptowalne oraz

Krok	Działanie	Opis działania
		czy wysokie ryzyko naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji zostało zminimalizowane do akceptowalnego (patrz rozdział 5.5 i 6.6)? W przypadku pozytywnej odpowiedzi (TAK) przechodzimy do realizacji kroku nr 11. W przypadku negatywnej odpowiedzi (NIE), przechodzimy do realizacji kroku nr 9.
9.	Informowanie o ryzyku lub/i przeprowadzenie konsultacji	Na każdym kroku procesu zarządzania ryzykiem ochrony danych osobowych można realizować proces informowania o ryzyku oraz prowadzenia konsultacji w interesariuszami, w tym konsultacje z organem nadzorczym (jeśli są wymagane). Realizacja działania została opisana w rozdziale 9 niniejszego dokumentu. W wyniku zakończenia realizacji działań kroku nr 9 przechodzimy do realizacji kroku nr 1, 4, 5 lub 7 (w zależności do kontekstu realizacji niniejszego kroku).
10.	Nie ma potrzeby przeprowadzenia oceny skutków dla ochrony danych osobowych	Dla wskazanych rodzajów operacji przetwarzania danych nie ma potrzeby przeprowadzenia oceny skutków dla ochrony danych osobowych. Taką decyzję należy uzasadnić w celach dowodowych i na potrzeby przyszłego przeglądu zasadności. W wyniku zakończenia realizacji działań kroku nr 10 przechodzimy do realizacji kroku nr 11.
11.	Monitorowanie i przegląd ryzyka	Monitorowanie i przegląd mechanizmów ochrony danych osobowych powinien być realizowany na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych. Realizacja działania została opisana w rozdziale 8 niniejszego dokumentu. W wyniku zakończenia realizacji działań kroku nr 11 przechodzimy do realizacji kroku nr 1.

Tabela 1. Opis procesu zarządzania ryzykiem
Źródło: Opracowanie własne

3.2. Efekty przeprowadzenia oceny ryzyka

Efekty przeprowadzenia oceny ryzyka mogą (ale nie muszą) skutkować realizacją między innymi następujących działań łącznie lub każdego z osobna.

Efekty przeprowadzenia oceny ryzyka	Opis działania
Podjęcie działań korygujących lub zapobiegawczych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba ustanowienia/zmodyfikowania lub zmiany dotychczasowych stosowanych zabezpieczeń organizacyjnych lub/i technicznych w organizacji.
Poinformowanie lub/i podjęcie konsultacji z organem nadzorczym	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba poinformowania o ryzyku lub potrzeba przeprowadzenia konsultacji dot. postępowania z ryzykiem z organem nadzorczym kontrolującymi działalność organizacji lub/i organem nadzorczym odpowiedzialnym za ochronę danych osobowych.
Poinformowanie lub/i podjęcie konsultacji z Administratorami danych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba poinformowania o ryzyku lub potrzeba przeprowadzenia konsultacji dot. postępowania z ryzykiem z Administratorami danych, który powierzyli organizacji przetwarzanie danych osobowych.
Zasięgnięcia opinii podmiotów, którym planowane jest lub powierzono przetwarzanie danych osobowych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba zasięgnięcia opinii dot. ryzyka podmiotów, którym planowane jest lub powierzono przetwarzanie danych osobowych.
Przeprowadzenie kontroli lub/i audytów wewnętrznych, zewnętrznych (w tym testów penetracyjnych) w organizacji lub podmiotom, którym planowane jest lub jest już powierzone przetwarzania danych osobowych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba przeprowadzić weryfikację adekwatności i skuteczności stosowanych zabezpieczeń w organizacji lub/i u podmiotów, którym planowane jest lub jest już powierzone przetwarzania danych osobowych.
Potwierdzenie aktualności czynności i zasobów wykorzystywanych do realizacji operacji przetwarzania danych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba przeprowadzenia przeglądu identyfikowanych zadań i zasobów wykorzystywanych do realizacji czynności przetwarzania danych.
Unikanie przetwarzania	W przeprowadzonej oceny ryzyka może zaistnieć potrzeba zaprzestania przetwarzania danych osobowych lub realizacji danych czynności przetwarzania.
Przeniesienie przetwarzania danych osobowych	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba przeniesienia utrzymywanych zasobów lub/i realizowanych czynnościami przetwarzania danych osobowych na zewnętrzny podmiot przetwarzający.
Zdefiniowanie wymagań bezpieczeństwa dla systemów informatycznych lub usług IT	W wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba zdefiniowania wymagań bezpieczeństwa ochrony danych osobowych przez zaprojektowanie, nabycie lub istotną modyfikację funkcjonującego systemu lub usługi IT oraz wymagań bezpieczeństwa dla odbioru systemów informatycznych lub usług IT.

Tabela 2. Efekty przeprowadzenia szacowania ryzyka
Źródło: Opracowanie własne

4. Identyfikacja czynności przetwarzania danych osobowych

Identyfikacja czynności przetwarzania danych osobowych realizowanych przez organizację stanowi punkt wyjścia do przeprowadzenia oceny ryzyka naruszenia praw lub wolności osób fizycznych oraz oceny ryzyka bezpieczeństwa informacji (jeśli będzie przeprowadzana).

W ramach realizacji działania należy zidentyfikować i zinwentaryzować:

a) główne świadczone usług i zadania realizowane przez organizację, w których przetwarzane są dane osobowe;
b) zasoby wykorzystywane do realizacji zidentyfikowanych zasoby, w szczególności: systemy IT, lokalizacje, nośniki, sieć, personel (przykładowy katalog zasobów stanowi załącznik nr 3);
c) odbiorców danych, którym ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
d) właścicieli zidentyfikowanych zadań.

Identyfikacja czynności przetwarzania powinna być udokumentowana, na bieżąco utrzymywana oraz okresowo, nie rzadziej niż raz na rok, przeglądana w celu potwierdzenia jej aktualności.

Do identyfikacji czynności przetwarzania warto posłużyć się rejestrem czynności przetwarzania opracowywanym i utrzymywanym w ramach zapewnia zgodności z art. 30 RODO.

5. Ocena ryzyka naruszenia praw lub wolności osób fizycznych

Ocenę ryzyka naruszenia praw lub wolności osób fizycznych można przeprowadzić w oparciu o:

a) tylko zidentyfikowane czynności przetwarzania (identyfikacja świadczonych usług i zadań opisana w rozdziale 4); lub
b) zidentyfikowanie czynności przetwarzania oraz wszystkie zidentyfikowane zasoby zaangażowane w przetwarzanie danych osobowych (przykładowy katalog zasobów znajduje się w załączniku nr 4) – podejście rekomendowane; lub
c) zidentyfikowanie czynności przetwarzania oraz zidentyfikowane zasoby bezpośrednio powiązane, czynnościami przetwarzania dla których ryzyko jest wysokie.

Zastosowane podeście do przeprowadzenia oceny ryzyka należy udokumentować.

Poniższy diagram prezentuje proces przeprowadzenia oceny ryzyka naruszenia praw lub wolności osób fizycznych.

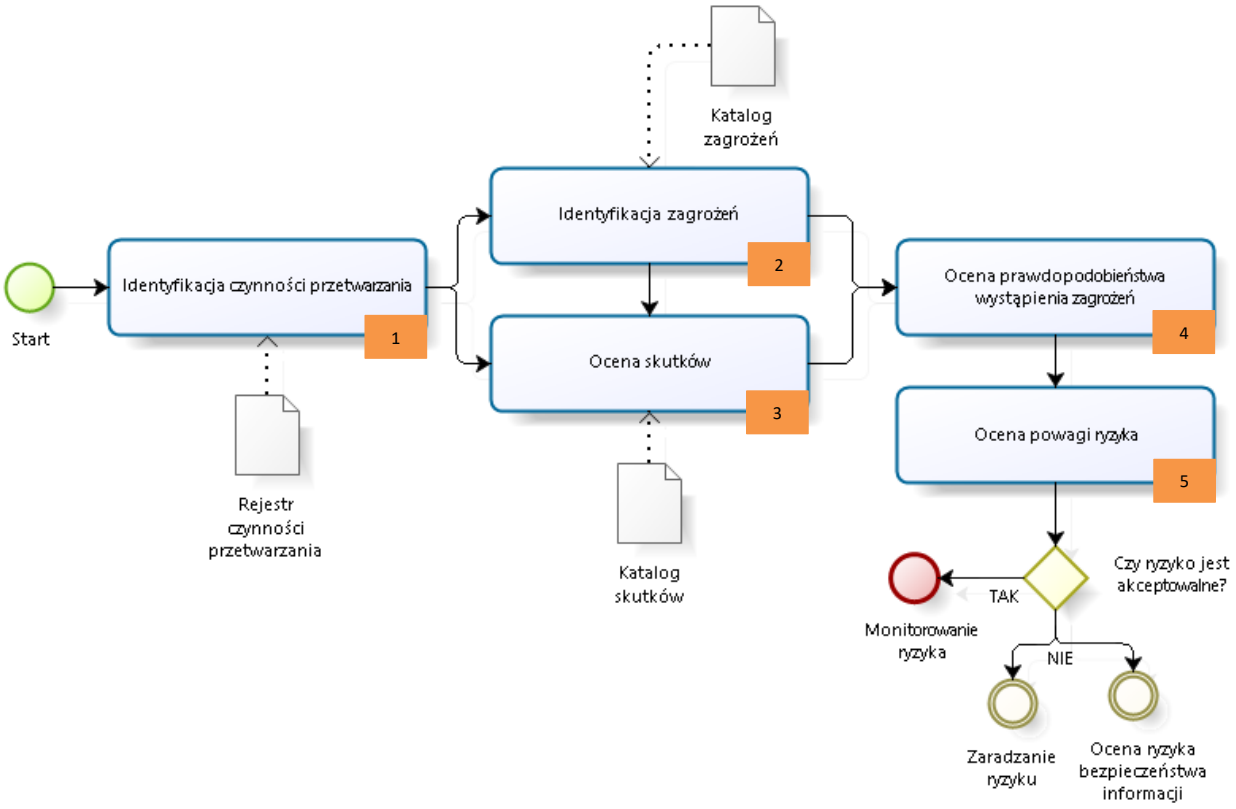

Diagram 2. Proces oceny ryzyka naruszenia praw lub wolności osób fizycznych
Źródło: Opracowanie własne

5.1. Identyfikacja zagrożeń naruszenia praw i wolności osób fizycznych

Zagrożenie należy rozumieć jako potencjalną przyczynę niepożądanego incydentu, która może wywołać naruszenie praw lub wolności osób fizycznych.

Każdą zidentyfikowaną czynność przetwarzania należy rozważyć w kontekście możliwości wystąpienia poniżej wskazanych zagrożeń:

Lp.	Katalog zagrożeń naruszenie praw lub wolności osób fizycznych
1	Przypadkowe lub niezgodne z prawem zniszczenie danych osobowych
2	Utracenie powierzonych lub pozyskanych danych osobowych
3	Nieuprawnione zmodyfikowanie danych osobowych
4	Nieuprawnione ujawnienie danych osobowych
5	Nieuprawniony dostęp do danych osobowych przesyłanych
6	Nieuprawniony dostęp do danych przechowywanych
7	Nieuprawniony sposób przetwarzania danych (brak postawy prawnej do przetwarzania danych)

Tabela 3. Przykładowy katalog zagrożeń naruszenia praw lub wolności osób fizycznych
Źródło: Opracowanie własne, na podstawie RODO

Wskazany katalog zagrożeń nie jest listą zamkniętą, w zależności od rodzaju, wielkości i natury prowadzonej działalności, w tym realizowanych czynności przetwarzania danych osobowych, należy rozważyć rozszerzenie katalogu.

Zagrożenia można identyfikować min. na podstawie:

a) historii dotychczasowych incydentów przetwarzania danych osobowych w organizacji lub w organizacjach podobnych;
b) informacji uzyskanych z przeprowadzonych konsultacji z interesariuszami wewnętrznymi i zewnętrznymi, np. prawnikami, informatykami, ekspertami ds. bezpieczeństwa, audytorami, właścicielami procesów i zasobów;
c) przykładowych katalogów zagrożeń wynikających z dobrych praktyk stanowi Załącznik B normy ISO/IEC 29134:2017 Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dotyczące oceny wpływu na prywatność.

Należy pamiętać, że zagrożenia powinny być identyfikowane tylko w kontekście naruszenia praw lub wolności osób fizycznych, a nie w innym tak ocena skutków dla organizacji.

Na potrzeby metody oceny ryzyka naruszenia praw lub wolności osób fizycznych, identyfikowane zagrożenia nie są wartościowane. Istotność zagrożeń nie jest priorytetyzowana, ponieważ każde ich urzeczywistnienie skutkować może naruszeniem praw lub wolności osób fizycznych.

5.2. Ocena skutków urzeczywistnienia się zagrożeń

Dla każdej pary „czynność przetwarzania – zagrożenie" należy ocenić skutki (tj. konsekwencje) zmaterializowania się zagrożenia naruszenia praw lub wolności osób fizycznych w kontekście realizowanej czynności przetwarzania danych osobowych.

Katalog skutków dla którego należy ocenić konsekwencje dla każdej pary „czynność przetwarzania – zagrożenie" został opisany w tabeli poniżej.

Lp.	Katalog skutków naruszenia praw lub wolności osób fizycznych, podlegający ocenie
1	Dyskryminacja osób fizycznych, których dane dotyczą
2	Kradzież tożsamości lub oszustwo dotyczące tożsamości osoby fizycznej
3	Strata finansowa osób fizycznych, których dane dotyczą
4	Naruszenie dobrego imienia osób fizycznych, których dane dotyczą
5	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową
6	Nieuprawnione odwrócenie pseudonimizacji danych osób fizycznych
7	Wszelka inna znacząca szkoda gospodarcza lub społeczna dla osób fizycznych, których dane dotyczą

Tabela 4. Przykładowy katalog skutków naruszenia praw lub wolności osób fizycznych
Źródło: Opracowanie własne, na podstawie RODO

Wskazany katalog skutków nie jest listą zamkniętą, w zależności od realizowanych czynności przetwarzania danych osobowych, należy rozważyć rozszerzenie katalogu.

Skutki można identyfikować min. na podstawie:

a) historii dotychczasowych incydentów przetwarzania danych osobowych w organizacji lub w organizacjach podobnych;
b) informacji uzyskanych z przeprowadzonych konsultacji z interesariuszami wewnętrznymi i zewnętrznymi, np. prawnikami, informatykami, ekspertami ds. bezpieczeństwa, audytorami, właścicielami procesów i zasobów.

Należy pamiętać, że skutki powinny być identyfikowane tylko w kontekście naruszenia praw lub wolności osób fizycznych, a nie w innym takim jak oddziaływanie na organizację.

Na potrzeby metody oceny ryzyka naruszenia praw lub wolności osób fizycznych każdy analizowany skutek zmaterializowania się zagrożenia należy ocenić poprzez wykorzystanie skal opisanych w poniższej tabeli 5.

Ocena skutków naruszenia praw lub wolności osób fizycznych		
Wartość (S)	Nazwa	Opis
3	Wysokie	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych.
2	Średnie	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie.
1	Niskie	Identyfikuje się nieznaczne skutki mogące prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych.
0	Nie dotyczy	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują.

Tabela 5. Ocena skutków naruszenia praw lub wolności osób fizycznych
Źródło: Opracowanie własne

5.3. Ocena prawdopodobieństwa wystąpienia zagrożeń

Dla każdego zestawienia „czynność przetwarzania – zagrożenia - skutek" należy ocenić prawdopodobieństwa wystąpienia zagrożeń umożliwiająca urzeczywistnienie się skutków.

Skutki należy ocenić na podstawi przyjętej w metodyce skali.

Ocena prawdopodobieństwa wystąpienia zagrożenia		
Wartość (P_{Pb})	Nazwa	Opis
4	Bardzo prawdopodobne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż połowa szans na wystąpienie lub Zagrożenie zmaterializowało się w przeciągu ostatniego roku.
3	Prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa lub Zagrożenie zmaterializowało się sporadycznie w przeszłości (w ciągu ostatnich 2 lat)
2	Mało prawdopodobne	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (bliska zeru) lub Zagrożenie zmaterializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat).
0	Nie dotyczy	Ocena prawdopodobieństwa wystąpienia zagrożenia nie podlega analizie, ponieważ skutki zostały ocenione na zero.

Tabela 6. Ocena prawdopodobieństwa wystąpienia zagrożenia
Źródło: Opracowanie własne

5.4. Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych

Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych oblicza się na podstawie niniejszego wzoru:

$$\boldsymbol{R_{NW} = S * P_{Pb}}$$

gdzie:

R_{NW} – Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych;

S – Ocena skutków naruszenia praw lub wolności osób fizycznych;

P_{Pb} – Ocena prawdopodobieństwa urzeczywistnienia się zagrożenia.

Uwaga, w kontekście ochrony dany osobowych nie piorytetyzuje się istotności czynności przetwarzania danych osobowych między sobą.

Na potrzeby metody oceny ryzyka naruszenia praw lub wolności osób fizycznych przyjęto następujący rozkład ryzyka opisany w tabeli nr 7 i tabeli nr 8.

Ocena prawdopodobieństwa		Ocena skutków		
		2	**3**	**4**
	1	2	3	4
	2	4	6	8
	3	6	9	12

Tabela 7. Macierz rozkładu oceny ryzyka naruszeniem praw lub wolności osób fizycznych
Źródło: Opracowanie własne

Gdzie:

Poziom	Skala wartości	Opis
Niskie ryzyko	od 2 do 4	Ryzyka akceptowane, niewymagające dalszego postępowania (tj. zaradzania).
Średnie ryzyko	6	Ryzyka akceptowane, niewymagające dalszego postępowania (tj. zaradzania), jednakże należy je na bieżąco monitorować.
Wysokie ryzyko	od 8 do 12	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem (tj. zaradzania) lub/i przeprowadzenia oceny ryzyka bezpieczeństwa informacji.

Tabela 8. Poziom akceptacji ryzyka naruszeniem praw lub wolności osób fizycznych
Źródło: opracowanie własne

Otrzymane wyniki powagi ryzyka naruszenia praw lub wolności osób fizycznych należy przedstawić w postaci Raportu oceny ryzyka naruszenia praw i wolności osób fizycznych.

Raport swoim zakres powinien uwzględniać:

a) Wyniki oceny ryzyka przestawione w postaci rankingu ryzyka, czyli od największego do najmniejszego;
b) Poziom akceptacji ryzyka, w ramach którego oceniana jest istotność ryzyka;
c) Wnioski z oceny ryzyka, poprzez wskazanie ryzyk nieakceptowalnych wymagających dalszego postepowania.

6. Ocena ryzyka bezpieczeństwa informacji

Ocenę ryzyka bezpieczeństwa informacji można przeprowadzić w oparciu o:

a) wszystkie zidentyfikowane zasoby zaangażowane w przetwarzanie danych osobowych (przykładowy katalog zasobów znajduje się w załączniku nr 4) – podejście rekomendowane; lub
b) zidentyfikowane zasoby bezpośrednio powiązane, czynnościami przetwarzania dla których ryzyko jest wysokie.

Zastosowane podeście do przeprowadzenia oceny ryzyka należy udokumentować.

Poniższy diagram prezentuje proces przeprowadzenia oceny ryzyka bezpieczeństwa informacji.

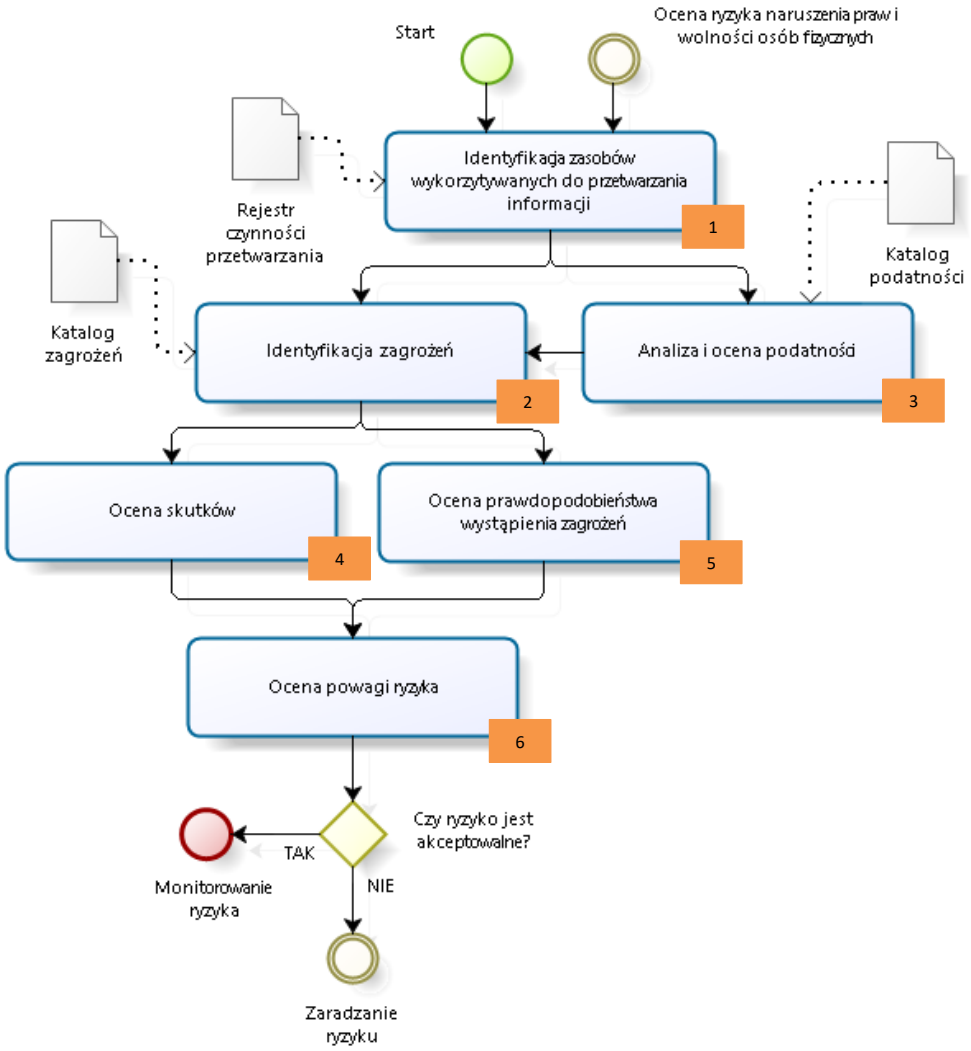

Diagram 3. Proces oceny ryzyka bezpieczeństwa informacji
Źródło: Opracowanie własne

6.1. Identyfikacja zagrożeń bezpieczeństwa informacji

Do zidentyfikowanych zasobów podlegających ocenie ryzyka należy przypisać zagrożenia. Zagrożenia identyfikowane są w kontekście konkretnego zasobu. Nie należy brać pod uwagę zagrożeń, które nie mają odniesienia do danego zasobu.

Bardzo istotną kwestią jest branie pod uwagę jedynie tych zagrożeń, które mogą realnie wystąpić. Niewskazane jest uwzględnianie zagrożeń teoretycznych, dla których prawdopodobieństwo wystąpienia jest znikome.

Wyróżnia się min. zagrożenia takie jak:

a) zniszczenia fizyczne – pożar, zalanie, zanieczyszczenie;
b) utrata podstawowych usług – awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego;
c) naruszenie bezpieczeństwa informacji – szpiegostwo zdalne, podsłuch, kradzież nośników lub dokumentów;
d) awarie techniczne – awaria urządzenia, niewłaściwe funkcjonowanie urządzeń, przeciążenie systemu informacyjnego;
e) nieautoryzowane działania – nieautoryzowane użycie urządzeń, nieuprawnione kopiowanie oprogramowania, zniekształcenie danych;
f) naruszenie bezpieczeństwa funkcji – błąd użytkowania, naruszenie praw.

Przykładowy katalog zagrożeń stanowi załącznik nr 4 niniejszego dokumentu.

Zagrożenia należy identyfikować na podstawie:

a) historii incydentów dotychczasowej eksploatacji systemów IT i zarządzania bezpieczeństwem informacji (należy dokonać przeglądu incydentów);
b) informacji uzyskanych od właścicieli zasobów oraz interesariuszy;
c) katalogów zagrożeń np. Załącznik C, normy PN-ISO/IEC 27005:2014-01.

6.2. Identyfikacja podatności

Do każdej zidentyfikowanej pary „zasób – zagrożenie” należy przypisać podatności. Jako podatność należy rozumieć słabość lub lukę, która może być wykorzystana przez źródło zagrożenia do spowodowania szkody zasobu i procesu biznesowego (w tym czynności przetwarzania), który go wykorzystuje (podatnością jest np. brak zabezpieczenia).

Należy pamiętać, iż identyfikowane są tylko istniejące podatności, w przypadku których istnieją zagrożenia. Nie należy identyfikować podatności, w stosunku do których nie istnieją realne zagrożenia.

Wyróżnia się następujące grupy podatności:

a) sprzęt – niewystarczające utrzymanie/błędna instalacja nośników pamięci, brak planów okresowej wymiany, wrażliwość na wilgoć, pył, zanieczyszczenie;
b) oprogramowanie – brak lub niewystarczające testowanie oprogramowania, dobrze znane wady oprogramowania, brak wylogowania przy opuszczaniu stacji roboczej;
c) sieć – niebezpieczna architektura sieciowa, przesyłanie hasła w jawnej postaci, nieodpowiednie zarządzanie siecią (elastyczność routingu);
d) personel – nieobecność personelu, nieodpowiednie procedury rekrutacji, niewystarczające szkolenie z bezpieczeństwa.

Przykładowy katalog zagrożeń stanowi załącznik nr 5 niniejszego dokumentu.

6.3. Estymacja ryzyka

Celem przeprowadzenia estymacji ryzyka jest określenie poziomu ryzyka dla bezpieczeństwa informacji w kontekście analizowanych elementów ryzyka. Estymacja ryzyk obejmuje określenie istotności zasobów oraz oszacowanie powagi zagrożeń i podatności. Wyliczenia są podstawą do określenia poziomu skutków, dla których określane jest prawdopodobieństwo wystąpienia. Na podstawie poziomu skutków i prawdopodobieństwa wystąpienia skutków określane jest ryzyko bezpieczeństwa informacji.

6.3.1. Ocena istotności zasobów

Ocenę wartości zasobów określa się na podstawie poniższej skali:

Wartość	Nazwa	Opis
5	Krytyczne	Zasób jest krytyczny dla funkcjonowania organizacji, bez niego nie można realizować statutowych zadań (w tym czynności przetwarzania).
4	Bardzo ważne	Zasób jest bardzo ważny dla funkcjonowania organizacji, znacząco Zasób a na realizowane statutowe zadania (w tym czynności przetwarzania).
3	Ważne	Zasób jest ważny dla funkcjonowania organizacji, umiarkowanie wpływa na realizację zadań statutowych (w tym czynności przetwarzania).
2	Średnio ważne	Zasób jest średnio ważny dla funkcjonowania organizacji, nieznacznie wpływa na realizację statutowych zadań (w tym czynności przetwarzania).
1	Mało istotne	Zasób jest mało istotny dla funkcjonowania organizacji, nie wpływa na realizację statutowych zadań (w tym czynności przetwarzania).

Tabela 9. Ocena istotności zasobów
Źródło: Opracowanie własne

Uwaga, w każdym przypadku dla zasobu powiązanego z czynnościami przetwarzania, dla których powaga ryzyka naruszenia praw lub wolności osób fizycznych została określone jako wysokie, należy ocenić wartość zasobu na co najmniej 4 (bardzo ważne) lub 5 (krytyczne).

6.3.2. Ocena powagi zagrożeń

Na potrzeby metody oceny ryzyka bezpieczeństwa informacji, dla każdego zidentyfikowanego zagrożenia, nie określa się jego powagi. Istotność zagrożeń nie jest priorytetyzowana, ponieważ każde ich urzeczywistnienie może skutkować, w tym samym stopniu, naruszenie bezpieczeństwa informacji.

6.3.3. Ocena powagi podatności

Wartość podatności jest określana w skali trójstopniowej. Poszczególnym wartościom przypisywane są cyfry celem wyliczenia wartości. Powaga podatności jest określana następująco:

Wartość	Nazwa	Opis
3	Wysoka	Wykorzystanie podatności jest stosunkowo proste lub oczywiste.
2	Średnia	Wykorzystanie podatności jest proste, ale wymaga zaangażowania czasowego lub działań niepraktycznych.
1	Niska	Wykorzystanie podatności jest skomplikowane lub wymaga dużego nakładu pracy.

Tabela 10. Ocena powagi podatności
Źródło: Opracowanie własne

6.4. Ocena powagi skutków

Wartość skutku zmaterializowania się zagrożenia wyliczana jest na podstawie wzoru:

$$W_{Skut} = W_{Akt} \times W_{Pod}$$

gdzie:

W_{Skut} – Ocena powagi skutków wystąpienia zagrożenia bezpieczeństwa informacji;
W_{Akt} – Ocena istotności zasobów;
W_{Pod} – Ocena powagi podatności.

6.5. Ocena prawdopodobieństwa

Wartość prawdopodobieństwa określana jest na zasadzie identyfikacji częstotliwości wystąpienia danego zdarzenia. Określana jest na podstawie skali procentowej, przy wykorzystaniu następujących wartości tj. 10%, 30%, 50% lub 80%.

Wartość prawdopodobieństwa jest określana następująco:

Wartość	Nazwa	Opis
80%	Bardzo prawdopodobne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż połowa szans na wystąpienie lub Materializowało się w przeciągu ostatniego roku.
50%	Prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa lub Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 2 lat)
30%	Mało prawdopodobne	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest niewielkie lub Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat).
10%	Szczątkowe	Zdarzenie nigdy nie wystąpiło w organizacji.

Tabela 11. Ocena prawdopodobieństwa wystąpienia zagrożenia bezpieczeństwa informacji
Źródło: Opracowanie własne

6.6. Ocena powagi ryzyka bezpieczeństwa informacji

Ryzyko bezpieczeństwa informacji jest szacowane na podstawie:

$$R_{BI} = W_{Skut} \times P_{Pd}$$

gdzie:

R_{BI} – Ocena powagi ryzyka bezpieczeństwa informacji,
W_{Skut} – Ocena powagi skutków wystąpienia zagrożenia bezpieczeństwa informacji,
P_{Pd} – Ocena prawdopodobieństwa wystąpienia danego zagrożenia.

Ocena ryzyka obejmuje porównanie poziomów ryzyka z kryteriami oceny ryzyka, w szczególności z poziomem akceptacji ryzyka.

Poprzez poziom akceptacji ryzyka rozumiemy określenie wartości ryzyka, którego zmaterializowanie, a w konsekwencji straty, są dopuszczalne przez Administratora danych.

Na potrzeby metody oceny ryzyka bezpieczeństwa informacji przyjęto następujący rozkład ryzyka.

		Prawdopodobieństwo			
		10%	30%	50%	80%
Warotość aktywa x Wartość podatności	1	0,1	0,3	0,5	0,8
	2	0,2	0,6	1	1,6
	3	0,3	0,9	1,5	2,4
	4	0,4	1,2	2	3,2
	6	0,6	1,8	3	4,8
	8	0,8	2,4	4	6,4
	10	1	3	5	8
	12	1,2	3,6	6	9,6
	15	1,5	4,5	7,5	12

Tabela 12. Macierz rozkładu oceny ryzyka bezpieczeństwa informacji
Źródło: Opracowanie własne

Gdzie:

Poziom ryzyka	Skala wartości	Opis
Niskie	od 0,1 do 1,2	Ryzyka akceptowane, nie wymaga dalszego postępowania.
Średnie	od 1,3 do 4	Ryzyka akceptowane, wymaga stałego monitorowania.
Wysokie	od 4,1 do 12	Ryzyka nieakceptowane, wymaga dalszego postępowania z ryzykiem zgodnie z rozdziałem 7 niniejszego dokumentu.

Tabela 13. Poziom akceptacji ryzyka bezpieczeństwa informacji
Źródło: opracowanie własne

7. Postępowanie z ryzykiem

Celem postępowania z ryzykiem (tj. zaradzaniem) jest dokonanie wyboru wariantu postępowania z ryzykiem oraz zaplanowanie zabezpieczeń organizacyjnych i technicznych mających zapewnić ochronę danych osobowych, z uwzględnieniem przepisów prawnych i prawnie uzasadnionych interesów osób fizycznych, których dane dotyczą, i innych osób fizycznych, których sprawa dotyczy.

W ramach postępowania z ryzykiem należy dokonać wyboru wariantu postępowania z ryzykiem. Wyróżniamy następujące warianty:

a) minimalizacja ryzyka - wdrożenie odpowiednich zabezpieczeń organizacyjnych i technicznych mających na celu minimalizację ryzyka do poziomu akceptowalnego oraz zapewnianie zgodności z RODO;

b) unikanie ryzyka – rezygnacja z realizacji działań lub warunków, które powodują powstanie określonych ryzyk;

c) transfer ryzyka - przeniesienie ryzyka na inny podmiot, który może skutecznie zarządzać ryzykiem;

d) akceptacja ryzyka - podjęcie przez Administratora danych decyzji o zachowaniu ryzyka bez podejmowania dalszych działań. W przypadku ryzyk bezpośrednio związanych naruszeniem praw i wolności osób fizycznych (tj. czynności przetwarzania oraz zasobów bezpośrednio powiązanych z czynnościami przetwarzania o wysokim ryzyku) decyzję tą Administrator danych może podjąć tylko po wydania pozytywnej opinii przez organ nadzorujący przetwarzania danych osobowych.

W wyniku postępowania z ryzykiem powinien powstać dokument „Plan postępowania z ryzykiem", który powinien uwzględniać:

a) dane wejściowe do utworzenia planu postępowania z ryzykiem - informacje o kontekście przetwarzania danych, zidentyfikowanych wysokich ryzykach dotyczących naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji (jeśli była przeprowadzona);

b) wariant postępowania z ryzykiem - informacja jaki wariant obsługi dla wysokich ryzykach naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji (jeśli była przeprowadzona) został przyjęty wraz z uzasadnieniem (w przypadku przyjęcia innego sposobu obsługi niż minimalizacja ryzyka);

c) opis planu działania – opis działań jakie zostaną podjęte w celu minimalizacji ryzyka;

d) oczekiwany efekt – opis mechanizmów organizacyjnych lub/i technologicznych jakie powstaną po realizacji planu postępowania;

e) mierniki oceny skuteczności realizacji planu postępowania – należy określić wskaźniki, na podstawie których będzie możliwość oceny skuteczności mechanizmów organizacyjnych lub/i technologicznych mających na celu minimalizację zidentyfikowanego ryzyka do poziomu akceptowalnego;

f) odpowiedzialność za realizację – informacja kto (z imienia i nazwiska) będzie odpowiedzialny za realizację wskazanego planu postępowania;

g) termin realizacji – informacja, kiedy planowane jest zakończenie wdrożenia mechanizmów organizacyjnych lub/i technologicznych mających na celu minimalizację zidentyfikowanego ryzyka.

Dokument „Plan postępowania z ryzykiem" ma charakter ogólny. Na podstawie tego dokumentu każda osoba odpowiedzialna za realizację planu działania powinna definiować szczegółowy sposób realizacji celu osiągania deklarowanego efektu w zadeklarowanym terminie.

Dokument „Plan postępowania z ryzykiem" tworzony jest dla poszczególnych, pojedynczo zidentyfikowanych ryzyk lub grupy ryzyk, jeśli dotyczą tej samej czynności przetwarzania lub zasobu.

Przykładowe środki zmierzające do ograniczenia ryzyka naruszenia praw lub wolności osób fizycznych zgodnie z RODO [art. 35 ust. 7 lit. d oraz preambuła 90, RODO] i bezpieczeństwa informacji zostały opisane w załączniku nr 6 niniejszego dokumentu.

8. Monitorowanie i przegląd ryzyka

Monitorowanie i przegląd mechanizmów ochrony danych osobowych powinien być realizowany na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych, tj.:

a) weryfikacji, czy zidentyfikowano nowy proces (w tym czynności przetwarzania) w którym przetwarzane są dane osobowe;
b) weryfikacji, czy zidentyfikowane procesy, zasobu i przepływ danych osobowych nie uległ zmianie lub planowane są ich modyfikacje, np. wdrożenie nowej technologii lub rozwiązań biznesowych, co może powodować realizację nowych operacji przetwarzania danych lub/i modyfikację realizację procesów wykorzystywanych do przetwarzania danych;
c) weryfikacji, czy organ nadzorczy ustanowił nowy lub zaktualizował wykaz rodzajów operacji przetwarzania podlegających i niepodlegających wymogowi dokonania oceny skutków dla ochrony danych;
d) weryfikacji, czy nie zmieniły się lub planowane są zmiany warunków przyczyniających się do niezbędności i proporcjonalności przetwarzania danych;
e) weryfikacji, czy zidentyfikowane ryzyka naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji są wciąż adekwatne;
f) weryfikacji, czy zastosowane zabezpieczenia lub/i ograniczenie przetwarzania danych są skuteczne i nadal oddziaływają na minimalizację ryzyka.

Proces monitorowania powinien być realizowany na bieżącą. Natomiast przegląd ww. punktów powinien być przeprowadzony co najmniej raz w roku lub częściej w przypadku modyfikacji lub planowania modyfikacji kontekstu przetwarzania danych.

Wyniki procesu monitorowania i przeglądu powinny być dokumentowane, w tym zgłaszane i obsługiwane nieprawidłowości i słabości mechanizmów ochrony danych osobowych, w celach dowodowych.

9. Informowanie o ryzyku i konsultacje

W proces informowania o ryzyku i konsultacjach powinny być zaangażowane wszystkie strony zainteresowane na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych, tj.:

a) administrator danych osobowych;
b) inspektor ochrony danych lub inne osoby powołane przez administratora danych odpowiedzialne za ochronę danych osobowych w organizacji;
c) właściciele procesów odpowiedzialni za realizację czynności przetwarzania;
d) właściciele zasobów odpowiedzialni za zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania wykorzystywanych do realizacji procesów;
e) podmioty przetwarzające powierzone lub planowane do powierzenia dane osobowe (tylko jeśli istnieje potrzeba).

W stosownych przypadkach zaleca się zasięgniecie opinii niezależnych ekspertów różnych zawodów, np. prawników, informatyków, ekspertów ds. bezpieczeństwa.

Informowanie o ryzyku powinno być realizowane zgodnie z zasadą "need to know".

Celem informowania o ryzyku jest zapewnienie, że:

a) wszystkie zaangażowane strony znają swoją rolę w procesie zarządzania ryzykiem ochrony danych osobowych;

b) odpowiednie informacje przekazywane są do administratora danych i/lub właścicieli zasobów;

c) ustanowiony jest przepływ informacji w dół, w górę i w poprzek struktury organizacyjnej;

d) ustanowione są odpowiednie kanały wymiany informacji ze stronami trzecimi, w tym organem nadzorczym odpowiedzialnym za ochronę danych osobowych.

9.1. Konsultacje z organem nadzorczym

Administrator konsultując się z organem nadzorczym zobowiązany jest przedstawić [art. 35 ust. 3, RODO]:

a) odpowiednie obowiązki administratora, współadministratorów oraz informacje o podmiotach uczestniczących w przetwarzaniu (w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw) - gdy ma to zastosowanie;
b) cele i sposoby zamierzonego przetwarzania danych;
c) wykaz zabezpieczeń mający na celu chronić prawa i wolności osób, których dane dotyczą;
d) dane kontaktowe inspektora ochrony danych - gdy ma to zastosowanie;
e) ocenę skutków dla ochrony danych [art. 35 ust. 7, RODO];
f) inne wszelkie informacje, których żąda organ nadzorczy.

Jeżeli organ nadzorczy jest zdania, że administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu, pisemnego zalecenia - korzystając z uprawnień, o których mowa w art. 58, RODO.

Okres ten organ nadzorczy może przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. O takim przedłużeniu informuje w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

Uwaga, identyfikuje się przypadki, gdzie może być wymagane, aby administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednią zgodę na przetwarzanie danych osobowych do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania danych w związku z ochroną socjalną i zdrowiem publicznym [art.36 ust. 5, RODO].

Wszystkie wyniki konsultacji powinny być udokumentowane, w celach dowodowych.

10. Role i odpowiedzialności

Podział ról i odpowiedzialności zaangażowanych w realizację procesu zarządzania ryzykiem ochrony danych osobowych został przedstawiona na podstawie modelu RACI.

RACI jest skrótem dla:

R - Osoba, której powierzono realizację zadań *(ang. Responsible);*

A - Osoba nadzorująca i zatwierdzająca, odpowiedzialna za końcowy efekt zadań *(ang. Approver);*

C - Osoba konsultująca i doradzająca w realizacji zadań *(ang. Consulted);*

I - Osoba informowana o prowadzonych działaniach oraz niewpływająca na realizację zadań *(ang. Informed);*

Rola	Opis roli
Administrator danych	Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych [art. 4, ust. 7, RODO]
Inspektor ochrony danych lub inna osoba/osoby powołane przez administratora danych odpowiedzialna/-e za ochronę danych osobowych w organizacji	Uwaga, proponowane odpowiedzialności są tylko sugerowane, nie wynikają one z wymagań RODO. W ramach zarządzania ryzykiem odpowiedzialna jest za: a) zidentyfikowanie czynności przetwarzania danych osobowych o wysokim ryzyku naruszenia praw lub wolności osób fizycznych; b) nadzorowanie postępowanie z ryzykiem w celu zredukowania ryzyka; c) informowanie o ryzyku interesariuszy i konsultacje eksperckie; d) monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem w organizacji.
Właściciele czynności przetwarzania	Osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie realizacji zadania lub grupy zadań w celu osiągnięcia zamierzonego celu. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do zasobów.
Właściciele zasobów	Osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo powierzonych zasobów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do zasobów.

Rola	Opis roli
Organ nadzorujący przetwarzanie danych osobowych w organizacji	Oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO np. Prezes Urzędu Ochrony Danych Osobowych.
Eksperci	Niezależni eksperci różnych zawodów, np. prawnicy, informatycy, eksperci ds. bezpieczeństwa i ciągłości działania.

Tabela 14. Role w procesie zarządzania ryzykiem
Źródło: Opracowanie własne

Krok	Działanie	Rola i odpowiedzialność					
		Administrator danych	Inspektor ochrony danych lub inna osoba/osoby	Właściciele Procesu	Właściciele zasobów	Organ nadzorujący	Eksperci
1.	Inwentaryzacja czynności przetwarzania	A	C	R	R		C
2.	Ocena, czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych	A	R				C
3.	Ocena, czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych	A	R				C
5.	Ocena ryzyka naruszenia praw lub wolności osób fizycznych	A	R	R	R	C	C
6.	Ocena, czy ryzyko naruszenia praw lub wolności osób fizycznych jest akceptowalne	AR	R	I	I	C	C
7.	Ocena ryzyka bezpieczeństwa informacji (jeśli była przeprowadzana)	A	R	R	R	C	C
8.	Ocena, czy ryzyko bezpieczeństwa informacji jest akceptowalne (jeśli pkt 7 był realizowany)	AR	R	I	I	C	C
9.	Przeprowadzenie postępowania z ryzykiem	A	R	R	R		C
10.	Ocena, czy ryzyko szczątkowe jest akceptowalne	AR	R	I	I	C	C
11.	Informowanie o ryzyku lub/i przeprowadzenie konsultacji	A	R	C	C	C	C
12.	Nie ma potrzeby przeprowadzenia oceny skutków dla ochrony danych osobowych	AR	R			C	C
13.	Monitorowanie i przegląd ryzyka	A	R	R	R		C

Tabela 15. Podział ról i odpowiedzialności
Źródło: Opracowanie własne

11. Wykaz działań wymagających udokumentowania

W poniższym rozdziale zostały wymienione działania wymagające udokumentowania w celu potwierdzenie funkcjonowania procesu zarządzania ryzykiem ochrony danych osobowych w organizacji.

Lp.	Działania wymagające udokumentowania
1.	Inwentaryzacja czynności przetwarzania i zasobów
2.	Opis zastosowanego podejście do przeprowadzenia oceny ryzyka
3.	Ocena naruszenia praw lub wolności osób fizycznych
4.	Ocena bezpieczeństwa informacji (jeśli jest realizowana)
5.	Plan postępowania z ryzykiem
6.	Wyniki procesu monitorowania zarządzania ryzykiem
7.	Wyniki przeprowadzonych konsultacji
8.	Wyniki procesu przeglądu zarządzania ryzykiem

Tabela 16. Wykaz działań wymagających udokumentowanie
Źródło: Opracowanie własne

Załączniki

Załącznik nr 1	Przykłady rodzajów operacji przetwarzania danych mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych
Załącznik nr 2	Przykłady rodzaju operacji przetwarzania mogące nie powodować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych
Załącznik nr 3	Przykłady zasobów wspierających realizacje czynności przetwarzania
Załącznik nr 4	Przykłady zagrożeń bezpieczeństwa informacji
Załącznik nr 5	Przykłady podatności zasobów wykorzystywanych do operacji przetwarzania
Załącznik nr 6	Przykłady środków przyczyniających się do ograniczenia ryzyka naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji.

Spis diagramów

Spis tabel

Załącznik nr 1 - Przykłady rodzajów operacji przetwarzania danych mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych

Poniżej zostały opisane rodzaje operacji związanych z przetwarzaniem, które wymagają oceny skutków dla ochrony danych osobowych ze względu na ich wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Opisane operacje niekiedy wykraczają poza wyjaśnienie tego, co należy rozumieć w trzech przykładach podanych w art. 35 ust. 3, RODO.

Poniższe informacje pochodzą z opinii Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218, Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017 roku. Ostatnio zmienione i przyjęte w dniu 4 października 2017 r.

Należy pamiętać, że poniższy wykaz operacji nie jest listą zamkniętą i należy ją traktować jako przekład.

1. Ocena lub punktacja, w tym profilowanie i przewidywanie

Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" [preambuła 71 i 91]. Przykładem tego może być instytucja finansowa sprawdzająca swoich klientów w referencyjnej bazie danych kredytowych lub bazie danych w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu lub w bazie danych zawierającej informacje o nadużyciach finansowych; przykładem może być również przedsiębiorstwo biotechnologiczne bezpośrednio oferujące konsumentom badania genetyczne w celu oceny i prognozowania ryzyka wystąpienia choroby lub zagrożeń dla zdrowia, a także przedsiębiorstwo tworzące profile zachowań lub profile marketingowe w oparciu o wykorzystanie lub nawigację na swojej stronie internetowej.

2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku

Przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" [art. 35 ust. 3 lit. a), RODO]. Przykładowo przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium. Dalsze wyjaśnienia dotyczące tych pojęć zostaną przedstawione w przyszłych wytycznych Grupy Roboczej Art. 29 dotyczących profilowania.

3. Systematyczne monitorowanie

Przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego

monitorowania na dużą skalę miejsc dostępnych publicznie" [art. 35 ust. 3 lit. c), RODO]. Ten rodzaj monitorowania stanowi jedno z kryteriów, ponieważ dane osobowe mogą być gromadzone w sytuacji, gdy osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).

4. Dane wrażliwe lub dane o charakterze wysoce osobistym

Szczególne kategorie danych osobowych określone w art. 9, RODO (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10, RODO. Przykładem może być szpital przechowujący dokumentację medyczną pacjentów lub prywatny detektyw przechowujący szczegółowe dane przestępców.

Oprócz tych przepisów zawartych w RODO niektóre kategorie danych można uznać za zwiększające potencjalne ryzyko naruszenia praw i wolności osób fizycznych. Te dane osobowe uznaje się za szczególnie wrażliwe (zgodnie z powszechnym rozumieniem tego terminu), ponieważ są powiązane z gospodarstwem domowym i działalnością prywatną (taką jak łączność elektroniczna, której poufność należy chronić) lub ponieważ wpływają na wykonanie prawa podstawowego (takie jak dane dotyczące lokalizacji, których gromadzenie jest sprzeczne ze swobodą poruszania się), lub ponieważ ich naruszenie ma wyraźny wpływ na codzienne życie osób, których dane dotyczą (takie jak dane finansowe, które mogą zostać wykorzystane do oszustw płatniczych). W tym względzie może mieć znaczenie fakt, czy dane zostały upublicznione przez osobę, której dane dotyczą, czy przez osoby trzecie.

Okoliczność, że dane osobowe są publicznie dostępne, może być uznana za czynnik w ocenie, jeżeli zgodnie z założeniami dane te miały być dalej wykorzystywane do określonych celów. Kryterium to może również obejmować dane takie jak dokumenty osobiste, wiadomości e-mail, pamiętniki, notatki z e-czytników wyposażonych w funkcję notatnika oraz dane mające bardzo osobisty charakter zawarte w aplikacjach rejestrujących codzienną aktywność.

5. Dane przetwarzane na dużą skalę

W RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie. W każdym razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
b) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
c) czas trwania lub trwałość czynności przetwarzania danych;
d) zakres geograficzny czynności przetwarzania.

6. Dopasowywanie lub łączenie zbiorów danych

Dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

7. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą

Przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć dzieci (można je uznać za niezdolne do świadomego i przemyślanego sprzeciwienia się przetwarzaniu danych lub do wyrażenia zgody na przetwarzanie danych), pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.) oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

8. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych

Wykorzystanie nowych technologii lub rozwiązań takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd. W RODO [art. 35 ust. 1 i preambule 89 i 91, RODO] wyjaśniono, że wykorzystanie nowej technologii zdefiniowanej „zgodnie ze stanem wiedzy technicznej” [preambuła 91, RODO] może sprawić, iż konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Wynika to z tego, że zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. W istocie osobiste i społeczne skutki wprowadzenia nowej technologii mogą nie być znane. Ocena skutków dla ochrony danych pomoże administratorowi danych zrozumieć takie ryzyko i je wyeliminować. Na przykład niektóre aplikacje „internetu rzeczy” mogą mieć znaczący wpływ na codzienne życie i prywatność osób fizycznych; dlatego wymagane jest przeprowadzenie oceny skutków dla ochrony danych..

9. Uniemożliwienie osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy

Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy” [art. 22 i preambuła 91, RODO]. Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu. Przykładem tego jest

sytuacja, w której bank sprawdza swoich klientów w referencyjnej bazie danych kredytowych, aby zdecydować, czy udzielić im kredytu.

Należy pamiętać, że im bardziej spełniane są powyższe kryteria, tym bardziej prawdopodobne jest, że stwarzają one ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe dotyczą, a zatem wymagają przeprowadzenia oceny skutków dla ochrony danych osobowych.

Zasadniczo można przyjąć, że operacja przetwarzania spełniająca co najmniej dwa wyżej wymienione kryteria wymaga przeprowadzenia oceny skutków dla ochrony danych osobowych. Jednak w niektórych przypadkach przetwarzanie spełniające tylko jeden z tych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych osobowych i odwrotnie, jeśli przetwarzanie spełnia co najmniej dwa kryteria, lecz nie uważa się za "prawdopodobnie wysokie ryzyko" ocena nie musi zostać przeprowadzona. Taką sytuację należy jednak udokumentować, tzn. opisać przyczyny niepodjęcia przeprowadzenia oceny.

Załącznik nr 2 - Przykłady rodzaju operacji przetwarzania mogące nie powodować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych

Ocena skutków dla ochrony danych osobowych nie jest wymagana, gdy operacje przetwarzania prawdopodobnie nie spowodują wysokiego ryzyka, lub zostały już dopuszczone przez organ nadzorczy lub są uzasadnione podstawą prawną.

Ocena skutków dla ochrony danych osobowych nie jest wymagana w następujących przypadkach:

a) jeżeli przetwarzanie nie prowadzi "prawdopodobnie do wysokiego ryzyka dla praw lub wolności osób fizycznych" [art. 35 ust. 1, RODO];
b) jeśli charakter, zakres, kontekst i cele przetwarzania są bardzo podobne do przetwarzania, dla którego przeprowadzono już ocenę skutków. W takich przypadkach można wykorzystać wyniki przeprowadzanej oceny skutków do podobnego przetwarzania [art. 35 ust. 1, RODO];
c) jeżeli operacja przetwarzania ma podstawę prawną w prawie UE lub w państwie członkowskim i stwierdziła, że nie musi być przeprowadzana ocena skutków dla ochrony danych osobowych [art. 35 ust. 10, RODO];
d) jeżeli przetwarzanie znajduje się na liście fakultatywnej (ustanowionej przez organ nadzoru) w odniesieniu do operacji przetwarzania, dla których nie jest wymagane przeprowadzanie oceny skutków dla ochrony danych osobowych [art. 35 ust. 5, RODO].

Załącznik nr 3 – Przykłady zasobów wspierających realizacje czynności przetwarzania

Poniżej przedstawiono przykładowe zasoby, wspierające realizacje czynności przetwarzania danych osobowych.

Kategoria zasobów	Zasoby szczegółowe	Przykłady
Personel	Użytkownicy	Personel z pełnym lub ograniczonym dostępem do danych osobowych i uprawnieniami do ich przetwarzania
	Deweloperzy	Personel z dostępem do danych osobowych, mogący przetwarzać je w środowiskach testowych
	Administratorzy	Personel z pełnym dostępem do danych osobowych, gdzie monitorowanie ich aktywności może być ograniczone
Siedziba	Pomieszczenia biurowe	Centrala organizacji, odziały, lokalizacje
	Pomieszczenia specjalne	Serwerownia, Archiwum, Kancelaria
Sprzęt	Urządzenia przetwarzania danych	Urządzenia automatycznego przetwarzania (np. systemy backupu), macierze dyskowe
	Urządzenia przenośne	Laptopy, PDA
	Serwery	Serwery poszczególnych systemów
	Urządzenia stacjonarne	Stacje robocze, terminale
	Urządzenia peryferyjne	Drukarka, kserokopiarka, wymienne napędy dyskowe
	Nośniki elektroniczne	CD-ROM, USB, Kaseta streamera
	Inne nośniki	Fax, slajdy, wydruki
Oprogramowanie	System operacyjny	Wszelkie systemy operacyjne (np. Windows, Linux, Unix)
	Bazy danych	Grupy plików bazodanowych
	Oprogramowanie usługowe, utrzymania lub administracyjne	Narzędzia służące do monitorowania systemów, service desk
	Pakiety oprogramowania lub oprogramowanie standardowe	Pakiet biurowy (np. MS Office, Open Office, przeglądarki)
	Standardowe aplikacje biznesowe	Oprogramowanie komercyjne wspierające realizację usług biznesowych - np. programy kadrowo-płacowe, baza CRM
	Dedykowane aplikacje biznesowe	Oprogramowanie stworzone na zamówienie - np. system transakcyjny
Sieć	Media	ADSL, PSTN, WiFi

Kategoria zasobów	Zasoby szczegółowe	Przykłady
	Przekaźniki aktywne lub pasywne	Router, hub, switch, most
	Interfejsy komunikacyjne	Modemy LTE/GPRS
Organizacja	Struktura organizacyjna	Schemat zarządzania organizacją np. outsourcing procesów wspierających
	Podwykonawcy (procesor)	Strony zewnętrzne, którym powierza się przetwarzanie danych osobowych
	Dostawcy	Strony zewnętrzne, świadczące usługi na rzecz organizacji

Tabela 17. Przykłady zasobów wspierających realizacje czynności przetwarzania
Źródło: Opracowanie własne, na podstawie normy PN-ISO/IEC 27005:2014-01

Załącznik nr 4 – Przykłady zagrożeń bezpieczeństwa informacji

Poniżej przedstawiono przykładowe zagrożenia, które mogą oddziaływać na naruszenie bezpieczeństwa informacji w organizacji.

Nazwa zagrożenia
Naruszenie bezpieczeństwa informacji
Przechwycenie sygnałów na skutek zjawiska interferencji
Szpiegostwo zdalne
Podsłuch
Kradzież nośników lub dokumentów
Kradzież urządzenia
Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników
Ujawnienie
Dane z niewiarygodnych źródeł
Manipulowanie urządzeniem
Sfałszowanie oprogramowania
Detekcja umiejscowienia
Nieautoryzowane działania
Nieautoryzowane użycie urządzeń
Nieuprawnione kopiowanie oprogramowania
Użycie fałszywego lub skopiowanego oprogramowania
Zniekształcenie danych
Naruszenie bezpieczeństwa funkcji
Nielegalne przetwarzanie danych
Błąd użytkowania
Naruszenie praw
Fałszowanie praw
Odmowa działania
Naruszenie dostępności personelu
Zagrożenia osobowe
Haker (włamanie do systemu)
Przestępca komputerowy (cybernetyczne prześladowanie, podszycie się)
Terroryzm
Szpiegostwo przemysłowe
Osoby wewnętrzne (źle wyszkolone, niezadowolone, złośliwe, niedbałe, nieuczciwe, zwolnieni pracownicy)

Tabela 18. Przykładowy katalog zagrożeń związany z naruszeniem bezpieczeństwa informacji
Źródło: Norma PN-ISO/IEC 27005:2014-01

Załącznik nr 5 – Przykłady podatności zasobów w kontekście bezpieczeństwa informacji

Poniżej przedstawiono przykładowe podatności, które mogą być wykorzystana do urzeczywistniania się zagrożenia w kontekście bezpieczeństwa informacji.

Rodzaj zasobów	Przykład podatności
Organizacja	Brak opracowanych, aktualizowanych lub testowanych planów ciągłości działania
	Brak dokumentacji technicznej systemów
	Brak dokumentacji wymaganej prawem
	Brak dzienników operatorów
	Brak kontroli zmian
	Brak listy osób upoważnionych do dostępu do przetwarzania danych osobowych
	Brak procedur dostępu do pomieszczeń
	Brak opracowanych lub aktualizowanych procedur eksploatacyjnych
	Brak procedur wymiany danych i oprogramowania
	Brak procedury monitorowania użycia urządzeń do przetwarzania informacji
	Brak ustanowionych mechanizmów monitorowania naruszeń bezpieczeństwa
	Brak wymagań bezpieczeństwa w procesach rozwojowych
	Niedostateczne procedury kontroli zmian
Sieć	Brak zabezpieczenia linii telekomunikacyjnych
	Brak zabezpieczenia transmisji danych osobowych
	Transmitowanie haseł w jawnej postaci
Oprogramowanie	Brak aktualizacji oprogramowania (usługi sieciowe i systemy operacyjne)
	Brak kontroli pobieranego oprogramowania
	Brak lub niedostateczne mechanizmy 'patch management'
	Brak lub niewystarczające procedury testowania oprogramowania
	Brak mechanizmów identyfikacji i uwierzytelniania
	Brak mechanizmów monitorowania aktywności użytkowników (logowania zdarzeń)
	Brak sformułowanych wymagań bezpieczeństwa dla tworzonych aplikacji
	Niedostateczne zarządzanie hasłami (hasła łatwe do odgadnięcia)
	Przechowywanie haseł w jawnej postaci, niedostateczna częstotliwość zmiany haseł
	Brak kontroli kopiowanych danych
	Niewłaściwe skonfigurowane aplikacje, usługi lub systemy operacyjne
	Skomplikowany interfejs użytkownika
	Użytkowanie usług powszechnie uznanych za niegwarantujące bezpieczeństwa
	Znane błędy (dziury), podatności w oprogramowaniu lub bazach danych
	Brak regularnych audytów
Personel	Brak wykonywanych regularnie procedur nadzoru
	Brak wymagań bezpieczeństwa na stanowiskach pracy
	Brak wyznaczonych osób odpowiedzialnych za systemy, procesy i zasoby
	Niewłaściwy przydział uprawnień dostępu
	Praca pracowników podmiotów zewnętrznych bez nadzoru
	Przechowywanie kopii w miejscu wytworzenia
	Absencja personelu
	Brak stosowania „polityki czystego biurka i ekranu”
	Brak wylogowania się przy opuszczaniu miejsca pracy
	Brak szkoleń w zakresie bezpieczeństwa
Sprzęt	Brak testowania urządzeń zasilających
	Brak alternatywnych dróg połączenia
	Brak kopii zapasowych/archiwalnych

Rodzaj zasobów	Przykład podatności
	Niewłaściwe przygotowywanie nośników do ponownego użycia
	Niewłaściwe wycofywanie nośników z użycia
	Niewłaściwe zabezpieczenie okablowania
	Pojedynczy punkt uszkodzenia (brak rezerwy)
Siedziba	Brak elektronicznej kontroli dostępu
	Brak fizycznej ochrony budynków, drzwi, okien
	Brak gwarantowanego zasilania
	Brak systemów sygnalizacji napadu i włamania
	Lokalizacja na terenie zagrożonym powodzią
	Stan techniczny budynku
	Stan techniczny instalacji grzewczych
	Stan techniczny instalacji odgromowych
	Stan techniczny instalacji zasilania
	Stan techniczny systemu ogrzewania
	Usytuowanie budynku

Tabela 19. Przykładowy katalog podatności zasobów w kontekście bezpieczeństwa informacji.
Źródło: MAGERIT – version 2

Załącznik nr 6 - Przykłady środków przyczyniających się do ograniczenia ryzyka naruszenia praw lub wolności osób fizycznych i bezpieczeństwa informacji

Poniżej określono przykładowe środki zmierzające do ograniczenia ryzyka naruszenia praw lub wolności osób fizycznych zgodnie z RODO [art. 35 ust. 7 lit. d oraz preambuła 90, RODO] i bezpieczeństwa informacji.

W celu zapewniania ograniczenia ryzyka należy dobrać adekwatne zabezpieczenia wynikające z dobrych praktyk opisanych w normach:

a) PN-ISO/IEC 27002:2014-12,
b) ISO/IEC 27018:2014,
c) ISO/IEC 29151:2017.

Normy te, jako zbiór dobrych praktyk, opisujących zabezpieczenia organizacyjne i techniczne, które mogą pomóc w ochronie informacji w organizacji w podziale na:

a) Cele stosowania zabezpieczeń – informacja jaki cel ma osiągnąć wdrożenie zabezpieczenia lub grupy zabezpieczeń;
b) Zabezpieczenia – opis zabezpieczenia, które wspiera osiągniecie celu stosowania zabezpieczenia.

Zabezpieczenia wskazane w Załączniku A normy ISO/IEC 270018:2014 należy traktować jako uzupełnienie zabezpieczeń opisanych w normie PN-ISO/IEC 27002:2014-12 adekwatnych do zapewniania ochrony danych osobowych w organizacji.

1. Cele stosowania zabezpieczeń i obszary zabezpieczeń według załącznika A normy PN-ISO/IEC 27001:2014-12

Załącznik A ISO 27001	Obszary zabezpieczeń
A.5 Polityki bezpieczeństwa informacji	
A.5.1 Wsparcie kierownictwa dla bezpieczeństwa informacji	
Cel: Zapewnienie, że kierownictwo wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami biznesowymi i właściwymi przepisami prawa oraz regulacjami wewnętrznymi.	
A.5.1.1	Polityki bezpieczeństwa informacji
A.5.1.2	Przegląd polityk bezpieczeństwa informacji
A.6 Organizacja bezpieczeństwa informacji	
A.6.1 Organizacja wewnętrzna	
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.	
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji
A.6.1.2	Rozdzielanie obowiązków
A.6.1.3	Kontakty z organami władzy
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami
A.6.2 Urządzenia mobilne i telepraca	
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych.	
A.6.2.1	Polityka stosowania urządzeń mobilnych
A.6.2.2	Telepraca
A.7 Bezpieczeństwo zasobów ludzkich	
A.7.1 Przed zatrudnieniem	
Cel: Zapewnić, żeby pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.	
A.7.1.1	Postępowanie sprawdzające
A.7.1.2	Warunki zatrudnienia
A.7.2 Podczas zatrudnienia	
Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.	
A.7.2.1	Odpowiedzialność kierownictwa
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
A.7.2.3	Postępowanie dyscyplinarne
A.7.3 Zakończenie lub zmiana zatrudnienia	
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.	
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków
A.8 Zarządzanie zasobami	
A.8.1 Odpowiedzialność za zasoby	
Cel: Zidentyfikować zasoby organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.	
A.8.1.1	Inwentaryzacja zasobów
A.8.1.2	Własność zasobów
A.8.1.3	Akceptowalne użycie zasobów
A.8.1.4	Zwrot zasobów
A.8.2 Klasyfikacja informacji	

Załącznik A ISO 27001	Obszary zabezpieczeń
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.	
A.8.2.1	Klasyfikacja informacji
A.8.2.2	Oznaczanie informacji
A.8.2.3	Postępowanie z zasobami
A.8.3 Obsługa nośników	
Cel: Zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji przechowywanej na nośniku.	
A.8.3.1	Zarządzanie nośnikami wymiennymi
A.8.3.2	Wycofywanie nośników
A.8.3.3	Przekazywanie nośników
A.9 Kontrola dostępu	
A.9.1 Wymagania biznesowe wobec kontroli dostępu	
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.	
A.9.1.1	Polityka kontroli dostępu
A.9.1.2	Dostęp do sieci i usług sieciowych
A.9.2 Zarządzanie dostępem użytkowników	
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.	
A.9.2.1	Rejestrowanie i wyrejestrowywanie użytkowników
A.9.2.2	Przydzielanie dostępu użytkownikom
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników
A.9.2.5	Przegląd praw dostępu użytkowników
A.9.2.6	Odebranie lub dostosowanie praw dostępu
A.9.3 Odpowiedzialność użytkowników	
Cel: Uczynienie użytkowników odpowiedzialnymi za zabezpieczenie ich danych uwierzytelniających.	
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających
A.9.4 Kontrola dostępu do systemu i aplikacji	
Cel: Ochrona przed nieautoryzowanym dostępem do systemów i aplikacji.	
A.9.4.1	Ograniczanie dostępu do informacji
A.9.4.2	Procedury bezpiecznego logowania
A.9.4.3	System zarządzania hasłami
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych
A.9.4.5	Kontrola dostępu do kodów źródłowych programów
A.10 Kryptografia	
A.10.1 Zabezpieczenia kryptograficzne	
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.	
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych
A.10.1.2	Zarządzanie kluczami
A.11 Bezpieczeństwo fizyczne i środowiskowe	
A.11.1 Obszary bezpieczne	
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.	
A.11.1.1	Fizyczna granica obszaru bezpiecznego
A.11.1.2	Fizyczne zabezpieczenie wejść

Załącznik A ISO 27001	Obszary zabezpieczeń
A.11.1.3	Zabezpieczanie biur, pomieszczeń i obiektów
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi
A.11.1.5	Praca w obszarach bezpiecznych
A.11.1.6	Obszary dostaw i załadunku
A.11.2 Sprzęt	
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności zasobów oraz zakłóceniom w działaniu organizacji.	
A.11.2.1	Lokalizacja i ochrona sprzętu
A.11.2.2	Systemy wspomagające
A.11.2.3	Bezpieczeństwo okablowania
A.11.2.4	Konserwacja sprzętu
A.11.2.5	Wynoszenie zasobów
A.11.2.6	Bezpieczeństwo sprzętu i zasobów poza siedzibą
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia
A.11.2.8	Pozostawienie sprzętu użytkownika bez opieki
A.11.2.9	Polityka czystego biurka i czystego ekranu
A.12 Bezpieczna eksploatacja	
A.12.1 Procedury eksploatacyjne i odpowiedzialność	
Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.	
A.12.1.1	Dokumentowanie procedur eksploatacyjnych
A.12.1.2	Zarządzanie zmianą
A.12.1.3	Zarządzanie pojemnością
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych
A.12.2 Ochrona przed szkodliwym oprogramowaniem	
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.	
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem
A.12.3 Kopie zapasowe	
Cel: Ochrona przed utratą danych.	
A.12.3.1	Zapasowe kopie informacji
A.12.4 Rejestrowanie zdarzeń i monitorowanie	
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.	
A.12.4.1	Rejestrowanie zdarzeń
A.12.4.2	Ochrona informacji w dziennikach zdarzeń
A.12.4.3	Rejestrowanie działań administratorów i operatorów
A.12.4.4	Synchronizacja zegarów
A.12.5 Nadzór nad oprogramowaniem produkcyjnym	
Cel: Zapewnić integralność systemów produkcyjnych.	
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych
A.12.6 Zarządzanie podatnościami technicznymi	
Cel: Zapobiec wykorzystywaniu podatności technicznych.	
A.12.6.1	Zarządzanie podatnościami technicznymi
A.12.6.2	Ograniczenia w instalowaniu oprogramowania
A.12.7 Rozważania dotyczące audytu systemów informacyjnych	
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.	
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych
A.13 Bezpieczeństwo komunikacji	

Załącznik A ISO 27001	Obszary zabezpieczeń
A.13.1 Zarządzanie bezpieczeństwem sieci	
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.	
A.13.1.1	Zabezpieczenia sieci
A.13.1.2	Bezpieczeństwo usług sieciowych
A.13.1.3	Rozdzielanie sieci
A.13.2 Przekazywanie informacji	
Cel: Utrzymanie bezpieczeństwa informacji i oprogramowania przekazywanej wewnątrz organizacji oraz z każdym podmiotem zewnętrznym.	
A.13.2.1	Polityki i procedury przesyłania informacji
A.13.2.2	Porozumienia dotyczące przesyłania informacji
A.13.2.3	Wiadomości elektroniczne
A.13.2.4	Umowy o zachowaniu poufności
A.14 Pozyskiwanie, rozwój i utrzymanie systemów	
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych	
Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.	
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych
A.14.1.3	Ochrona transakcji usług aplikacyjnych
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia	
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.	
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych
A.14.2.2	Procedury kontroli zmian w systemach
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania
A.14.2.5	Zasady projektowania bezpiecznych systemów
A.14.2.6	Bezpieczne środowisko rozwojowe
A.14.2.8	Testowanie bezpieczeństwa systemów
A.14.2.9	Testy akceptacyjne systemów
A.14.3 Dane testowe	
Cel: Zapewnić ochronę danych stosowanych do testów.	
A.14.3.1	Ochrona danych testowych
A.15 Relacje z dostawcami	
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami	
Cel: Zapewnić ochronę zasobów organizacji udostępnianych dostawcom.	
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami
A.15.1.3	Łańcuch dostaw technologii informacyjnych i komunikacyjnych
A.15.2 Zarządzanie usługami świadczonymi przez dostawców	
Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami.	
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców
A.15.2.2	Zarządzenie zmianami w usługach świadczonych przez dostawców
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji	
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami	

Załącznik A ISO 27001	Obszary zabezpieczeń
Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.	
A.16.1.1	Odpowiedzialność i procedury
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
A.16.1.7	Gromadzenie materiału dowodowego
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	
A.17.1 Ciągłość bezpieczeństwa informacji	
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarządzania ciągłością działania organizacji.	
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji
A.17.2 Nadmiarowość	
Cel: Zapewnić dostępność środków przetwarzania informacji.	
A.17.2.1	Dostępność środków przetwarzania informacji
A.18 Zgodność	
A.18.1 Zgodność z wymaganiami prawnymi i umownymi	
Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.	
A.18.1.1	Określenie stosownych wymagań prawnych i umownych
A.18.1.2	Prawa własności intelektualnej
A.18.1.3	Ochrona zapisów
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych
A.18.2 Przeglądy bezpieczeństwa informacji	
Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.	
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami
A.18.2.3	Sprawdzanie zgodności technicznej

Tabela 20. Cele stosowania zabezpieczeń i obszary zabezpieczeń według załącznika A normy PN-ISO/IEC 27001:2014-12
Źródło: PN-ISO/IEC 27001:2014-12

2. Zabezpieczenia danych osobowych według załącznika A normy ISO/IEC 27018:2014

Załącznik A ISO 27018	Obszary zabezpieczeń
A.1 Zgody i możliwości wyboru	
A.1.1 Obowiązek współpracy w zakresie praw osób fizycznych	
Zabezpieczenie: Podmiot przetwarzający dane musi zapewnić środki umożliwiające wypełnienia zobowiązania ułatwiających wykonywania praw osób fizycznych w zakresie: dostępu do danych, poprawiania, usuwania lub wyrażenia sprzeciwu wobec ich przetwarzania.	
A.2 Cel przetwarzania	
A.2.1 Obowiązek współpracy w zakresie praw osób fizycznych	
Zabezpieczenie: Dane osobowe przetwarzane w ramach umowy nie powinny być przetwarzane w żadnym innym celu niż zostały powierzone.	
A.2.2 Wykorzystanie danych do celów komercyjnych lub promocyjnych	
Zabezpieczenie: Dane osobowe przetwarzane w ramach umowy nie powinny być wykorzystywane przez podmiot przetwarzający do celów marketingowych, reklama i innych komercyjnych bez wyraźnej zgody podmiotu powierzającemu przetwarzanie danych. Taka zgoda nie powinna być warunkiem otrzymania świadczenia usługi.	
A.3 Ograniczanie niezbędności przetwarzania danych	
Żadne dodatkowe kontrole nie mają związku z tą zasadą prywatności.	
A.4 Minimalizacja danych	
A.4.1 Bezpieczne usuwanie plików tymczasowych	
Zabezpieczenie: Tymczasowe pliki i dokumenty powinny zostać usunięte lub zniszczone w określonym, udokumentowanym okresie.	
A.5 Ograniczenie użycia, przechowywania i ujawniania	
A.5.1 Powiadomienie o ujawnieniu informacji przez podmiot przetwarzający	
Zabezpieczenie: W umowie zawieranej między podmiotem przetwarzającym a podmiotowi powierzającym przetwarzanie danych należy uregulować zasady powiadamiania o każdym prawnie wiążącym żądaniu ujawnienia informacji osobowych przez prawo organ wykonawczy, chyba że takie ujawnienie jest zabronione.	
A.5.2 Rejestracja ujawnień	
Zabezpieczenie: Należy rejestrować informacje dot. ujawnianiu danych na rzecz osób trzecich, w tym informacje na temat ujawnionych informacji osobowych, do kogo a o której godzinie.	
A.6 Dokładność i jakość	
Żadne dodatkowe kontrole nie mają związku z tą zasadą prywatności.	
A.7 Otwartość, przejrzystość i ogłoszenie	
A.7.1 Ujawnianie informacji o podwykonawcach podmiotu przetwarzającego	
Zabezpieczenie: Informacje o wykorzystywanych podwykonawcach przez podmiot przetwarzający do przetwarzania danych osobowych powinno zostać ujawnione podmiotowi powierzającemu przetwarzanie danych przed ich użyciem.	
A.8 Indywidualny dostęp do przetwarzania danych	
Żadne dodatkowe kontrole nie mają związku z tą zasadą prywatności.	
A.9 Odpowiedzialność	
A.9.1 Powiadomienie o naruszeniu bezpieczeństwa danych osobowych	
Zabezpieczenie: Podmiot przetwarzający powinien niezwłocznie powiadomić podmiot powierzający przetwarzanie danych o zdarzeniu nieuprawnionego dostępu do danych osobowych lub nieuprawnionego dostępu do urządzeń przetwarzanych dane osobowe lub w przypadku utraty, ujawnienia lub zmiany danych osobowych.	
A.9.2 Okres przechowywania udokumentowanych zasad ochrony danych osobowych	

Załącznik A ISO 27018	Obszary zabezpieczeń
Zabezpieczenie: Kopie polityk bezpieczeństwa i procedur operacyjnych powinny być zachowane dla określonych, udokumentowanych okresów po wymianie (łącznie z aktualizacją).	
A.9.3 Zwrot, przekazywanie i usuwanie danych osobowych	
Zabezpieczenie: Podmiot przetwarzający powinien mieć politykę dotyczącą zwrotu, przekazania i / lub usuwania Powierzonych danych osobowych oraz powinien udostępnić tę politykę podmiotowi powierzającemu przetwarzanie danych.	
A.10 Bezpieczeństwo informacji	
A.10.1 Poufność lub umowy o poufności	
Zabezpieczenie: Przedstawiciele podmiotu przetwarzającego kontrolowani przez podmiot powierzający przetwarzanie danych, powinni podlegać procedurze obowiązku zachowania poufności.	
A.10.2 Ograniczenie tworzenia materiałów drukowanych	
Zabezpieczenie: Tworzenie materiałów drukowanych zawierających informacje osobowe powinno być ograniczone.	
A.10.3 Kontrola i rejestracja przywracania danych	
Zabezpieczenie: Powinna istnieć procedura i dziennik działań związanych z przywracaniem danych.	
A.10.4 Ochrona danych na nośnikach pamięci wynoszonych z pomieszczeń	
Zabezpieczenie: Dane osobowe dotyczące nośników opuszczających siedzibę podmiotu przetwarzającego powinny podlegać procedurze udzielania zezwoleń i nie powinien być dostępny dla nikogo poza upoważnionym personelem (np. przez zaszyfrowanie danych).	
A.10.5 Wykorzystanie niezaszyfrowanych przenośnych nośników danych i urządzeń	
Zabezpieczenie: Nie należy używać przenośnych nośników fizycznych i urządzeń przenośnych, które nie pozwalają na szyfrowanie	
A.10.6 Szyfrowanie danych osobowych transmitowanych w sieciach publicznych	
*Zabezpieczenie: D*ane osobowe przesyłane przez publiczne sieci transmisji danych powinny być szyfrowane przed transmisją.	
A.10.7 Bezpieczne usuwanie materiałów drukowanych	
Zabezpieczenie: W przypadku zniszczenia materiałów drukowanych należy je bezpiecznie zniszczyć za pomocą mechanizmów takich jak przecinanie, rozdrabnianie, spopielanie, roztwarzanie itp.	
A.10.8 Unikalne wykorzystanie identyfikatorów użytkowników	
Zabezpieczenie: Jeśli więcej niż jedna osoba ma dostęp do przechowywanych danych osobowych, to każdy z nich powinien mieć odrębny identyfikator użytkownika w celu zapewnienia identyfikacji, uwierzytelniania i autoryzacji.	
A.10.9 Zapisy upoważnionych użytkowników	
Zabezpieczenie: Bieżący zapis użytkowników lub profili użytkowników, którzy autoryzowali dostęp do informacji system powinien być utrzymany.	
A.10.10 Zarządzanie identyfikatorami użytkownika	
Zabezpieczenie: Dezaktywowane lub wygasłe identyfikatory użytkowników nie powinny być udzielane innym osobom.	
A.10.11 Środki zabezpieczeń	
Zabezpieczenie: Umowy między podmiotem powierzającym przetwarzanie, a podmiotem przetwarzającym dane osobowe powinny określać minimalne środki techniczne i organizacyjne. Takie środki nie powinny podlegać jednostronnej redukcji przez podmiot przetwarzający.	
A.10.12 Przetwarzanie danych osobowych zlecone podwykonawcom	
Zabezpieczenie: W kontraktach pomiędzy podmiotem przetwarzającym a ewentualnymi podwykonawcami przetwarzającymi dane osobowe należy określić minimalne środki techniczne i organizacyjne spełniające wymogi bezpieczeństwa informacji i ochrony danych osobowych. Takie środki nie powinny podlegać jednostronnej redukcji przez podwykonawcę.	
A.10.13 Dostęp do danych na wcześniej wykorzystanej przestrzeni dyskowej	
Zabezpieczenie: Podmiot przetwarzający powinien zapewnić, że gdy przestrzeń pamięci jest przypisana do podmiotu powierzającego przetwarzanie, żadne dane, które wcześniej znajdowały się w tej przestrzeni dyskowej, nie są widoczne dla tego podmiotu.	
A.11 Zgodność z zasadami ochrony prywatności	
A.11.1 Lokalizacja geograficzna przetwarzanych danych osobowych	

Załącznik A ISO 27018	Obszary zabezpieczeń
Zabezpieczenie: Podmiot przetwarzający powinien określić i udokumentować kraje, w których dane osobowe mogą być przechowywane.	
A.11.2 Transfer danych osobowych	
Zabezpieczenie: Dane osobowe przesyłane za pomocą sieci transmisji danych powinny podlegać odpowiednim kontrolom, zaprojektowanym w celu zapewnienia, że dane docierają do zamierzonego miejsca przeznaczenia.	

Tabela 21. Zabezpieczenia danych osobowych według załącznika A normy ISO/IEC 27018:2014
Źródło: ISO/IEC 27018:2014