GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Jak stosować podejście oparte na ryzyku?

Poradnik RODO
Podejście oparte na ryzyku

Część 2.

przygotowujemy do RODO 25.05.2018

grudzień 2017

Poradnik przygotowali pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych:

dr inż. Andrzej Kaczmarek - dyrektor Departamentu Informatyki

Monika Młotkiewicz - zastępca dyrektora Departamentu Rejestracji

Agnieszka Łapińska - specjalista w Departamencie Rejestracji

Agata Miłocha - specjalista w Departamencie Rejestracji

Michał Mazur - informatyk w Departamencie Informatyki

Konsultacja naukowa:

dr hab. n. ekon. inż. Janusz Zawiła-Niedźwiecki, prof. Politechniki Warszawskiej

Wprowadzenie

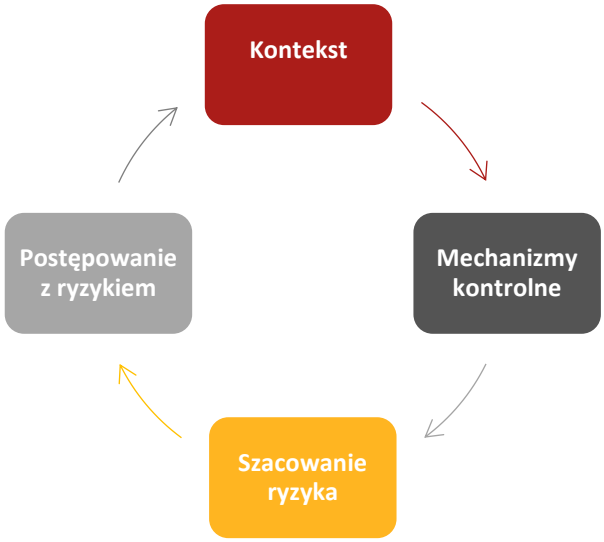
Ocena ryzyka oraz ocena skutków dla ochrony danych wymaga poznania szczegółów dotyczących przeprowadzanych operacji przetwarzania danych oraz uwarunkowań wewnętrznych i zewnętrznych dotyczących środowiska, w którym przetwarzanie się odbywa. Żeby tego dokonać, należy przyjąć określoną systematykę i kolejność działań.

W niniejszym opracowaniu, będącym uzupełnieniem informacji zawartych w części 1: *Jak rozumieć podejście oparte na ryzyku?*, proponujemy 4 podstawowe etapy (rys. 1) działań podejmowanych w celu przeprowadzania:

- ogólnej oceny ryzyka, oraz
- szczegółowej oceny ryzyka, ukierunkowanej na skutki w zakresie naruszenia praw lub wolności osób fizycznych (tzw. oceny skutków dla ochrony danych).

Ogólną ocenę ryzyka w zakresie bezpieczeństwa przetwarzania informacji, w tym danych osobowych, należy przeprowadzić, biorąc pod uwagę potencjalne negatywne skutki (straty materialne i niematerialne) zarówno dla administratora, jak i osób, których dane dotyczą.

Ocenę skutków dla ochrony danych przeprowadza się natomiast wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. W ostatniej części tego opracowania wskazujemy, że do oceny skutków dla ochrony danych można wykorzystać taki sam schemat postępowania, jak dla ogólnej oceny ryzyka, uwypuklając w poszczególnych etapach (od opisu kontekstu do postępowania z ryzykiem) te elementy, które mają istotny wpływ na skutki, jakie naruszenie ochrony danych może powodować dla osób, których dane dotyczą.



Rys. 1 Proponowane etapy stosowania podejścia opartego na ryzyku.

Poradnik nie stanowi gotowej metodyki w zakresie dostosowania organizacji do wymogów RODO. Wskazujemy w nim najistotniejsze elementy, które powinien wziąć pod uwagę administrator lub podmiot przetwarzający, wdrażając podejście oparte na ryzyku, aby zgodnie z RODO zapewnić skuteczną ochronę praw i interesów osób, których dane są przetwarzane.

Etapy szacowania ryzyka

Etap 1.
Ustalenie kontekstu

01

1.1 Krok 1.1.
Określenie informacji i uwarunkowań związanych z działaniem organizacji

Ustanowienie kontekstu to określenie wszystkich informacji i uwarunkowań związanych z działaniem organizacji, w tym posiadanych aktywów i zadań realizowanych przez konkretną organizację.

Ponieważ na ryzyko w zakresie ochrony danych wpływają różne czynniki, zarówno zewnętrzne, jak i wewnętrzne, ważne jest sporządzenie ich listy.

W odniesieniu do *aktywów informacyjnych*, w tym danych osobowych, powinny to być informacje obejmujące zakres, charakter i cele przetwarzania, a także potencjalne zagrożenia związane z ich nieuprawnionym ujawnieniem, utratą lub zniszczeniem, o których mowa w art. 24 i 32 RODO.

Informacje te najogólniej należy podzielić na zewnętrzne i wewnętrzne.

Do informacji zewnętrznych można przykładowo zaliczyć:

- informacje dotyczące środowiska prawnego,
- informacje dotyczące środowiska społecznego,
- informacje dotyczące środowiska politycznego,
- informacje dotyczące korzystania z usług lub zasobów podmiotów zewnętrznych,
- informacje o zasięgu terytorialnym działalności organizacji.

Do informacji wewnętrznych można przykładowo zaliczyć:

- strukturę i rozmiary organizacji,
- strategie i polityki stosowane w organizacji,
- systemy obiegu informacji, procesy podejmowania decyzji, rola przywództwa,
- informacje dotyczące środowiska technologicznego i możliwości jego zmian (finansowych, technicznych, organizacyjnych),
- normy i standardy przyjęte przez organizację, tzw. kultura organizacyjna.

1.2 Krok 1.2. Szczegółowy opis przetwarzanych danych i ich klasyfikacja

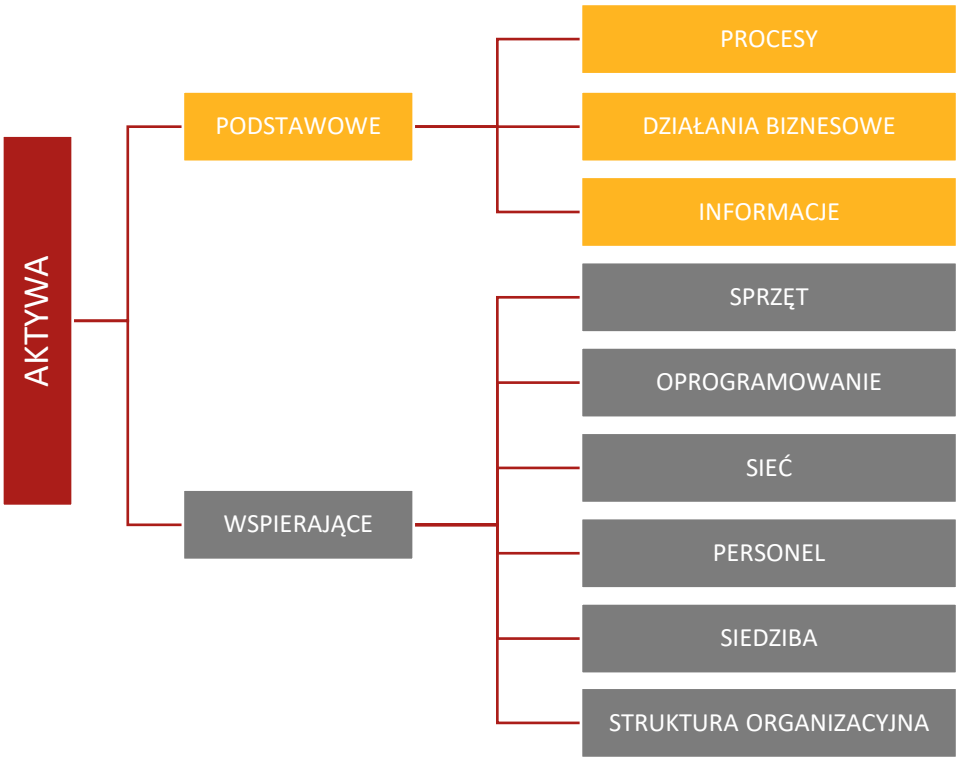
☑ **Należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych.**

Poprzez „aktywa" rozumieć należy zarówno informacje, w tym dane osobowe, jak i inne zasoby organizacji, takie jak:

- posiadana wiedza,
- personel,
- sprzęt,
- oprogramowanie,
- oraz inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych.

Identyfikacja i klasyfikacja aktywów w danej organizacji powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie *szacowania ryzyka*.

Posługując się schematem zaczerpniętym z *normy ISO/IEC 27005*, aktywa te można podzielić na podstawowe i wspierające, co pokazano na rysunku nr 2.



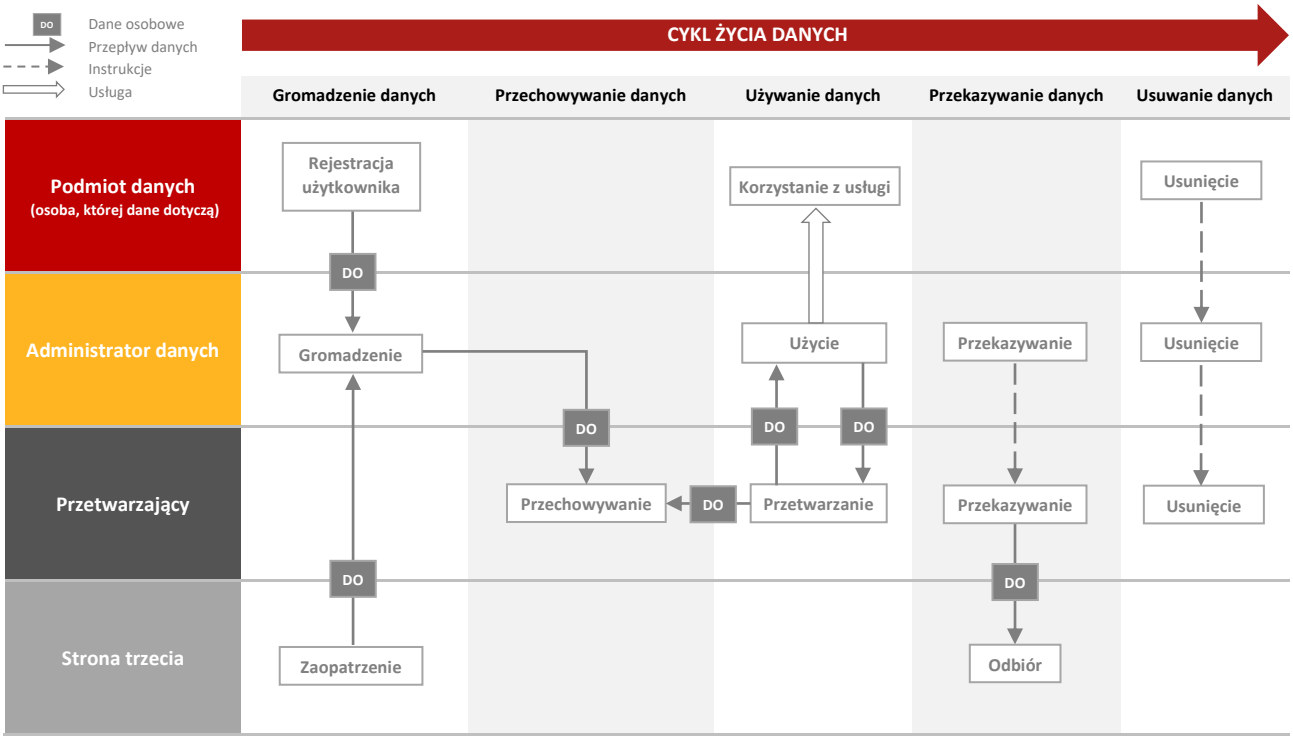
Rysunek 2. Podział aktywów wg PN-ISO/IEC 27005

W porównaniu z aktywami wspierającymi, działania związane z identyfikacją aktywów podstawowych nie zawsze są proste.

Należy ustalić właścicieli aktywów

W tym celu konieczne jest zidentyfikowanie wszystkich procesów biznesowych, aktywów w nich wykorzystywanych oraz zadań, aktywności i ról poszczególnych osób w prowadzonych procesach.

Na tym etapie trzeba ustalić, kto i za co ponosi odpowiedzialność w danej organizacji. Wykorzystując np. rozmowy z pracownikami, wskazane jest ustalenie konkretnych zadań i obowiązków, które są wykonywane przez poszczególne osoby oraz komórki organizacyjne. To pozwala na przypisanie odpowiedzialności *właścicielom aktywów* (np. przypisanie odpowiedzialności konkretnym osobom i konkretnym komórkom organizacyjnym). Właścicielem aktywów jest osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji. Ustalenie właścicieli aktywów wymaga zaangażowania wielu osób na różnych poziomach struktury organizacyjnej.



Rysunek 3. Przykładowy przepływ danych w organizacji

Należy określić wartości aktywów

W tym celu należy uzgodnić kryteria oraz skale, które będą wykorzystywane do wszystkich zidentyfikowanych aktywów.

Kolejnym istotnym krokiem podczas identyfikacji aktywów jest określenie ich wartości. Zwykle najbardziej odpowiednią osobą do określenia wartości aktywów jest ich właściciel.

Przykładowo, jako kryteria można przyjąć:

- koszty początkowe,
- koszty związane z odtworzeniem aktywów,
- koszty utraty reputacji organizacji,
- koszty związane z utratą:
  - poufności,
  - integralności
  - dostępności danych,
- możliwość nałożenia kary przez organ nadzorczy,
- koszty związane z możliwością nakazania przez organ nadzorczy zaprzestania lub czasowego zaprzestania przetwarzania danych, np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

Po ustaleniu kryteriów, należy przyjąć skalę, która będzie wykorzystywana w całej organizacji. W zależności od rodzaju aktywów można wykorzystać:

- skalę ilościową (np. wyrażoną w wartościach pieniężnych)
- lub skalę jakościową (zwaną również wskaźnikową lub przedziałową), np.: bardzo niska, niska, średnia, wysoka, bardzo wysoka.

Uwaga:

Nie należy przyjmować bezkrytycznie skali wykorzystywanych w innych organizacjach bez ich szczegółowej analizy. Każda organizacja dla określonych wartości skali może przyjąć inne limity, np. wartość „niska" dla jednej organizacji może odpowiadać wartości „wysoka" w innej organizacji. Na tym etapie bardzo często zapomina się o uwzględnieniu zależności pomiędzy aktywami, np. poufność danych jest zależna od systemów przechowywania, zaś systemy te są zależne od systemów zasilania.

W wyniku identyfikacji aktywów powinno się uzyskać listę aktywów istotnych z punktu widzenia zarządzania ryzykiem oraz listę procesów biznesowych, w których aktywa te są wykorzystywane.

1.3 Krok 1.3. Szczegółowy opis stosowanych zabezpieczeń i innych ograniczeń

W tym kroku należy zebrać informacje na temat istniejących ***zabezpieczeń***. Głównym celem stosowania zabezpieczeń jest zmniejszenie występującego ryzyka. Wg normy ISO/IEC 27005, *zabezpieczenie* to środek, który modyfikuje ryzyko naruszenia bezpieczeństwa przetwarzanych danych. W praktyce mogą wystąpić przypadki, kiedy określone zabezpieczenie zmniejsza jeden rodzaj ryzyka, powodując zwiększenie innego.

Przykład:

Zmniejszenie ryzyka nieuprawnionego ujawnienia danych poprzez wprowadzenie zabezpieczeń kryptograficznych może spowodować wzrost ryzyka w zakresie dostępności danych np. na skutek awarii systemu zarządzania kluczami kryptograficznymi lub ich utraty.

Ogólną klasyfikację podziału zabezpieczeń z uwzględnieniem zagrożeń przedstawiono na rysunku nr 4.

Rysunek 4. Przykładowe kryteria podziału zabezpieczeń z uwzględnieniem zagrożeń

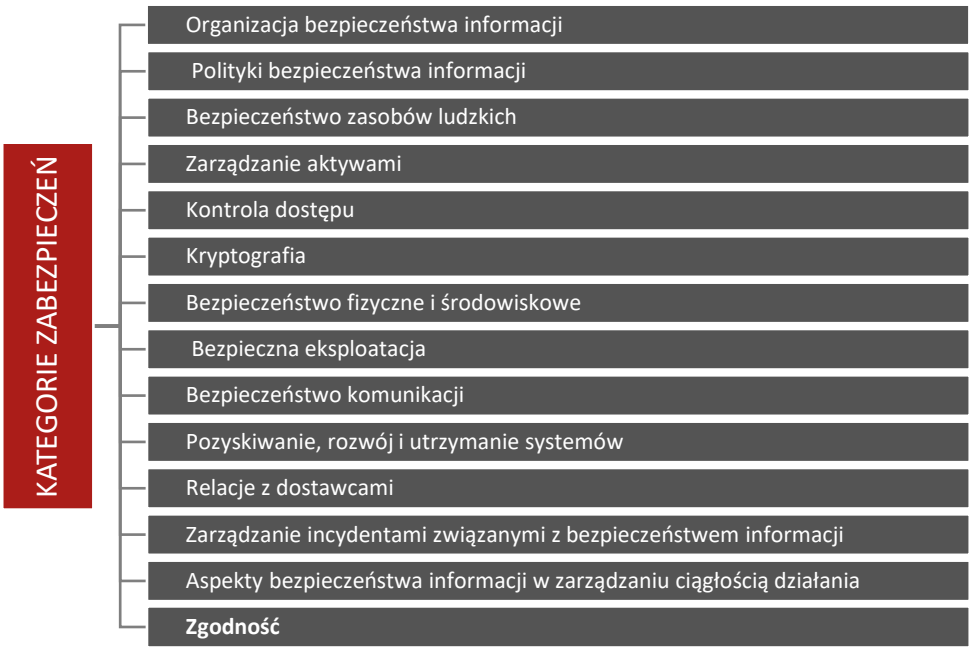
W celu określania istniejących zabezpieczeń można wykorzystać:

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

Informacja:

Uzupełnieniem listy mogą być wyniki przeprowadzonych audytów (pomagają określić listę dodatkowych, potencjalnych zabezpieczeń).

Pomocna w usystematyzowaniu zastosowanych zabezpieczeń i identyfikacji ewentualnych braków czy niedoskonałości może być klasyfikacja przedstawiona w normach **ISO/IEC 27001** i **ISO/IEC 27002**. Klasyfikacja ta pokazana została na rys. nr 5.



Rysunek 5. Kategorie zabezpieczeń wg Załącznika A normy PN-ISO/IEC 27001

W kontekście klasyfikacji zabezpieczeń dla systemów, w których przetwarzane są dane osobowe, szczególną uwagę warto zwrócić na ostatnią z kategorii, jaką zaznaczono na rys. 5, tj. zgodność. W kategorii tej chodzi o zgodność z przepisami RODO, co oznacza potrzebę zidentyfikowania wszystkich wynikających z przepisów prawa zobowiązań prawnych, nadzorczych, umownych oraz podejścia do ich przestrzegania. W kontekście RODO istotne zatem będzie dostosowanie procesów przetwarzania danych do wszystkich wymogów wynikających z przepisów tego aktu prawnego, w tym np. zasad i przesłanek przetwarzania danych określonych w art. 5 i 6 RODO, obowiązków informacyjnych wobec osób, których dane dotyczą (art. 13 i 14 RODO), uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych i stosowania zabezpieczeń adekwatnie do stanu wiedzy technicznej, kosztów wdrożenia, oraz charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw lub wolności osób fizycznych, o których mowa w art. 32 RODO.

1.4 Krok 1.4. Określenie kryteriów akceptacji ryzyka

Kryteria akceptacji ryzyka definiuje się zwykle przez wartość progową, np. przy przedziałach ryzyka w zakresie 0-2, 3-5 oraz 6-8. Jako akceptowalną wartość ryzyka można przyjąć wartość mniejszą od 2. Kryteria akceptacji ryzyka są niezwykle istotne w postępowaniu z ryzykiem, ponieważ na ich podstawie podejmowane są decyzje dotyczące zidentyfikowanych ryzyk w zakresie ich dopuszczalności.

Przy ustalaniu kryteriów należy uwzględniać nie tylko potencjalny, bezpośredni wpływ urzeczywistnienia się danego ryzyka na działalność biznesową organizacji (jak np. utrata klientów czy kary finansowe za naruszenie ich praw). Przede wszystkim pod uwagę należy brać wyniki klasyfikacji przetwarzanych danych ustalone w kroku nr 2. Nie można zapominać przy tym o uwarunkowaniach prawnych, w tym karach za naruszenie przepisów RODO, jak również o zawartych umowach i przyjętych regulaminach.

Etap 2.
Mechanizmy kontrolne

02

Głównym celem tego etapu jest opis i identyfikacja zastosowanych środków bezpieczeństwa i mechanizmów kontrolnych mających na celu spełnienie wymagań biznesowych, prawnych i innych ograniczeń dla procesów przetwarzania danych, w tym danych osobowych.

2.1 Krok 2.1.
Identyfikacja wymagań dla procesów przetwarzania danych w kontekście konkretnych celów działalności administratora

Dla każdego procesu przetwarzania danych należy sprawdzić, czy dane osobowe są przetwarzane:

- *zgodnie z zasadami wyrażonymi w art. 5 RODO, a w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych w art. 44-49 RODO,*
- *na podstawie jednej z przesłanek wskazanych w art. 6-10 RODO,*
- *przy zapewnieniu osobom, których dane dotyczą, możliwości realizacji ich praw wskazanych w art. 12-22 RODO.*

W tym celu należy określić:

☑ **konkretny cel przetwarzania danych oraz odpowiednią do tego celu podstawę prawną przetwarzania danych (pomocne w tym zakresie są motywy 39-56 RODO), np.:**

- jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego (art. 6 ust. 1 lit. c RODO)

> Przykład:
> *Na podstawie art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta podmiot udzielający świadczeń zdrowotnych ma prawny obowiązek prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w rozdziale 7 oraz w ustawie o systemie informacji w ochronie zdrowia, a także zapewnić ochronę danych zawartych w tej dokumentacji.*

lub wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e RODO).

> Przykład:
> *W celu realizacji swoich ustawowych zadań straż gminna na podstawie art. 10a ustawy z 29 sierpnia 1997 r. o strażach gminnych może przetwarzać dane osobowe (z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym), bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia.*

Konieczne jest wskazanie przepisów prawa unijnego lub krajowego odnoszących się do tego obowiązku prawnego lub zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 3 oraz motyw 45 RODO). Przepisy takie najczęściej określają cele przetwarzania, kategorie danych osobowych, a także mogą doprecyzowywać, kto jest uprawniony do przetwarzania danych w tym celu. Mogą one wskazywać również, na jakich warunkach, w jaki sposób i przez jaki okres dane mają być przetwarzane. **Konieczne jest staranne przeanalizowanie, czy prowadzone we wskazanym celu przetwarzanie jest zgodne ze szczegółowymi wymogami wynikającymi z powyższych przepisów.**

- jeżeli przetwarzanie następuje na podstawie **zgody** (art. 6 ust. 1 lit. a RODO), należy upewnić się, czy administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych w określonym celu w sposób spełniający warunki określone w art. 7-8 oraz motywie 42 i 43 RODO.

> Przykład:
> *Realizowanie przez określony podmiot wysyłki newsletterów zamówionych w ramach serwisu internetowego na podstawie zgody osoby dotyczącej tego celu.*

- przetwarzanie szczególnych kategorii danych osobowych **w celu dochodzenia lub obrony roszczeń** na podstawie art. 9 ust. 2 lit. f RODO (motyw 52 RODO).

> Przykład:
> *Przetwarzanie danych o przynależności do związku zawodowego w celu dochodzenia lub obrony roszczeń w postępowaniu przed sądem w sprawie z zakresu prawa pracy.*

- realizacja prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f i motyw 4 RODO).

> Przykład:
> *Marketing bezpośredni usług administratora kierowany do osoby będącej już jego klientem (osoba taka ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu - motyw 47 RODO).*

Trzeba pamiętać, że przesłanka „prawnie uzasadnionego interesu" nie może mieć zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Zasada ograniczenia celu (art. 5 ust. 1 lit. b RODO)

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania.

Należy również pamiętać, że przetwarzanie danych w celu innym niż cel, w którym dane osobowe zostały zebrane, musi odpowiadać warunkom określonym w art. 6 ust. 4 RODO (zobacz: motyw 50 RODO).

☑ **Wymagania dotyczące przejrzystości informacji udzielanych osobom, których dane dotyczą, na temat przetwarzania ich danych osobowych oraz ułatwiania im wykonania ich praw. Należy sprawdzić m.in.:**

- czy osoby, których dane dotyczą, zostały w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem poinformowane o przetwarzaniu ich danych osobowych zgodnie z art. 13 i 14 oraz motywem 58 i 60-62 RODO,
- czy wszelkie informacje i komunikaty kierowane do dzieci na temat przetwarzania ich danych osobowych zostały sformułowane w sposób, który pozwoli im bez trudu je zrozumieć,
- czy zostały wprowadzone procedury gwarantujące i ułatwiające osobom, których dane dotyczą, wykonywanie praw przysługujących im na mocy art. 15–22 RODO, m.in. mechanizmy żądania dostępu do danych osobowych, ich sprostowania lub usunięcia, możliwości wykonywania prawa do sprzeciwu i przenoszenia danych (motyw 59 i 63-72 RODO) oraz prawa do wyrażania stanowiska i zakwestionowania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

Zasada zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a i motyw 39 RODO) oraz zasada ograniczenia celu (art. 5 ust. 1 lit. b i motyw 39 RODO)

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania.

Należy również pamiętać, że przetwarzanie danych w celu innym niż cel, w którym dane osobowe zostały zebrane, musi odpowiadać warunkom określonym w art. 6 ust. 4 RODO (zobacz: motyw 50 RODO).

☑ **Zakres danych niezbędny do realizacji celów przetwarzania, w tym m.in.:**

- w kontekście zdefiniowanych celów przetwarzania - rodzaj przetwarzanych danych, a w ramach danego rodzaju - typ informacji, np. w przypadku „adresu osoby fizycznej” należy wskazać, o jaki adres chodzi, tj. adres zameldowania, adres zamieszkania, adres korespondencyjny, jak również elementy typu: nazwa kraju, miasta, ulicy, nr domu, nr mieszkania, nr telefonu czy adres poczty elektronicznej,
- częstotliwość zbierania danych, w celu upewnienia się, czy dane nie są zbierane zbyt często i w sposób nadmierny do celu (np. dla rozliczenia poboru energii konieczny jest odczyt z liczników zużywanej energii w ściśle określonych odstępach czasowych).

Zasada minimalizacji danych (art. 5 ust. 1 lit. c i motyw 39 RODO)

Pozyskiwane mogą być jedynie dane adekwatne i niezbędne dla osiągnięcia celów konkretnych, uzasadnionych i określonych w momencie zbierania danych. Nie można zbierać danych osobowych, które nie mają związku z celem przetwarzania, są nadmiarowe lub już nieprzydatne (np. ze względu na ich nieaktualność).

☑ **Źródła i sposób pozyskiwania danych oraz przepływy danych w czasie ich przetwarzania**:

- czy dane są pobierane bezpośrednio od osób, których dotyczą,
- sposób ich pozyskiwania, np. bezpośrednio od osób w biurze obsługi klienta czy poprzez formularze internetowe,
- w przypadku uczestnictwa w tych procesach podmiotów przetwarzających, ich zadania i odpowiedzialność,
- ewentualne wymogi dotyczące przekazywania danych do państw trzecich.

☑ **Wymagania w zakresie jakości przetwarzanych danych oraz weryfikacji tej jakości**:

- czy przetwarzane dane są prawidłowe, tj.: czy są merytorycznie poprawne, kompletne, zgodne ze stanem rzeczywistym i aktualne.

Zasada prawidłowości danych (art. 5 ust. 1 lit. d RODO)

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Realizując wskazaną zasadę, administrator powinien wdrożyć mechanizmy umożliwiające:

- weryfikację jakości danych oraz
- korektę danych.

Przykład:
Wprowadzenie możliwości zmiany adresu zamieszkania przez klienta banku poprzez system informatyczny oraz okresowe przypominanie przez bank swoim klientom o konieczności aktualizacji przez nich ich danych w razie zmiany miejsca zamieszkania.

☑ **Czas, przez jaki dane będą przetwarzane** oraz **wymagania dotyczące sposobu ich usunięcia po czasie, kiedy będą już zbędne** (jeśli cel przetwarzania zostanie osiągnięty).

Zasada ograniczenia czasowego (art. 5 ust. 1 lit. e RODO)

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane. Przechowywanie danych zgromadzonych np. w celu realizacji umowy powinno być zakończone w momencie przedawnienia roszczeń czy innych praw i obowiązków wynikających z przepisów prawa (np. kodeksu cywilnego w zakresie umów).

2.2 Krok 2.2. Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ich wypełnienia

Na tym etapie należy opisać wymagania w zakresie kontroli przetwarzania danych oraz wymagania w zakresie zapewnienia im bezpieczeństwa wynikające z przepisów RODO, norm w zakresie bezpieczeństwa, a także przepisów sektorowych związanych z branżą, w której działalność prowadzi administrator danych lub podmiot przetwarzający[1]. Wymagania te powinny być skonfrontowane z działaniami i faktami potwierdzającymi ich spełnienie w odniesieniu do ocenianych czynności.

Zasada integralności i poufności (art. 5 ust. 1 lit. f RODO)

Dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zamieszczone w tym kroku informacje dotyczące zastosowanych środków powinny umożliwić:

- ☑ **Oszacowanie ogólnego ryzyka naruszenia ochrony przetwarzanych danych (w tym ww. praw i wolności)[2] z** uwzględnieniem takich atrybutów bezpieczeństwa, jak: poufność, integralność i dostępność.
- ☑ **Rozpoznanie, czy** w procesie przetwarzania **występują elementy, które wymagają przeprowadzenia oceny skutków dla ochrony danych**, o których mowa w art. 35 RODO, a następnie konsultacji z organem nadzorczym, jeśli jej wyniki wskazują wysokie ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

Prawidłowe wykonanie powyższych zadań wiąże się przede wszystkim z określeniem wymagań dotyczących:

- ☑ **zabezpieczeń organizacyjnych,** tj. środków organizacyjnych oraz wymagań dotyczących polityki zarządzania procesem przetwarzania, w tym zastosowanych procedur:
  - zarządzania projektem,
  - zarządzania incydentami,
  - zarządzania personelem,
  - zarządzania udziałem stron trzecich, w tym podmiotów przetwarzających,
  - zarządzania eksploatacją używanych systemów i innych narzędzi przetwarzania danych,

[1] Przykładami szczególnych wymagań odnoszących się do stosowanych środków kontroli oraz bezpieczeństwa danych są „Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach", stanowiąca załącznik do uchwały Nr 7/2013 Komisji Nadzoru Finansowego z 8 stycznia 2013 r. w sprawie wydania ww. Rekomendacji, czy rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10 stycznia 2013 r. w sprawie sposobu utrwalania przebiegu imprezy masowej wydane na podstawie art. 11 ust. 9 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych.

[2] Bazując np. na normie PN-ISO/IEC 27005:2014-01 - zarządzanie ryzykiem w bezpieczeństwie informacji, lub PN-ISO/IEC 31000:2012 - zasady i wytyczne dotyczące zarządzania ryzykiem.

- sposobu nadzoru, w tym audytów i raportowania alertów.

☑ **środków kontroli logicznej procesu przetwarzania[3],** w tym wymagań dotyczących zastosowania takich środków ochrony, jak:

- anonimizacja i pseudonimizacja,
- środki ochrony kryptograficznej,
- środki kontroli integralności danych,
- środki kontroli dostępu do danych,
- środki kontroli dotyczące rozliczalności wykonywanych operacji,
- środki wspierające weryfikację danych na etapie ich wprowadzania, typu: zgodność z wzorcem, podanymi wartościami granicznymi itp.,
- środki bieżącego monitoringu,
- zastosowane środki ochrony przed działaniem oprogramowania szkodliwego typu wirusy, środki szpiegujące, środki służące ochronie przed wykradaniem danych itp.
- środki ochrony sieci przed działaniem osób z zewnątrz.

☑ **środków ochrony fizycznej** wszystkich aktywów informacyjnych i technicznych, w tym:

- dotyczących miejsca przetwarzania danych, takich jak: ukształtowanie terenu (np. podatność na powódź, wyładowania atmosferyczne itp.), sąsiedztwo obiektów lub podmiotów, mogących wpływać na bezpieczeństwo, jak np. lotnisko, stacja paliw, zakłady przetwórstwa chemicznego itp.,
- środków bezpieczeństwa infrastruktury technicznej wykorzystywanej do przetwarzania danych,
- środków bezpieczeństwa dokumentacji papierowej, w tym papierowych rejestrów zawierających dane osobowe,
- środków bezpieczeństwa związanych z przepływem informacji w postaci dokumentów papierowych lub nośników elektronicznych,
- środków ochrony przed żywiołami niezależnymi od człowieka, typu ogień, woda.

[3] Do ustanawiania i oceny zabezpieczeń organizacyjnych oraz środków kontroli logicznej procesu przetwarzania danych można wykorzystać np. normę PN-EN ISO/IEC 27001:2017-06, która określa wymagania dla systemu zarządzania bezpieczeństwem informacji oraz PN-EN ISO/IEC 27002:2017-06, która zawiera zalecenia dotyczące standardów bezpieczeństwa informacji w organizacjach i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrażania i zarządzania zabezpieczeniami, z uwzględnieniem środowiska (środowisk), w którym (których) w organizacji występuje (ą) ryzyko w bezpieczeństwie informacji.

Etap 3.
Szacowanie ryzyka

03

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

W ramach tego działania dla zidentyfikowanych procesów przetwarzania danych i występujących tam aktywów należy wskazać, przeanalizować i oszacować:

- *występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,*
- *zastosowane środki bezpieczeństwa,*
- *podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa na urzeczywistnienie się zidentyfikowanych zagrożeń, oraz*
- *potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.*

Nie można wskazać jednej, uniwersalnej metody szacowania ryzyka.

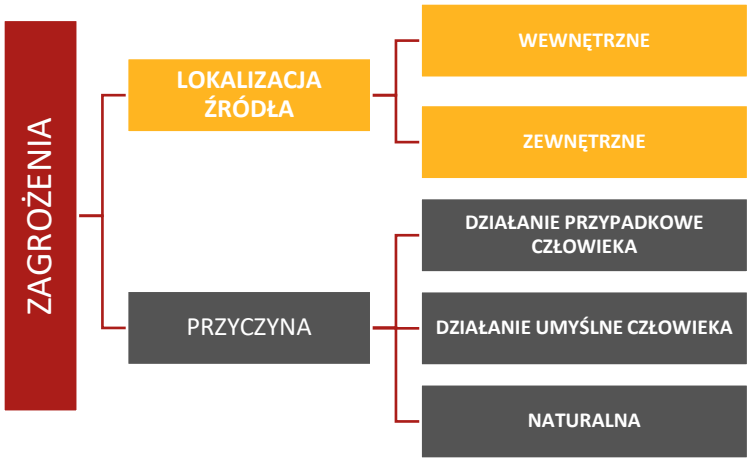
Do najbardziej popularnych metod identyfikacji, analizy i oceny ryzyka (ewaluacji ryzyka) można zaliczyć metody eksperckie (lista pytań kontrolnych, metoda delficka) oraz metody heurystyczne (metoda scenariuszy, metoda burzy mózgów). Oczywiście każda z tych metod ma wady i zalety. Dlatego każda organizacja, w zależności od obszaru swojej działalności, wielkości oraz kultury bezpieczeństwa, musi opracować własną metodę, zwykle stanowiącą kombinację kilku metod.

W etapie tym zgodnie z powyższym wykazem można wyróżnić 4 następujące kroki.

3.1 Krok 3.1. Identyfikacja zagrożeń

Zagrożenie wg PN-ISI Guide 73:2012 to źródło potencjalnej szkody. Zagrożenie może być uszczegółowione przez podanie pochodzenia (np. zagrożenie mechaniczne, zagrożenie elektryczne) albo charakteru potencjalnej szkody (np. ujawnienie poufnych danych).

W analizie zagrożeń wykorzystuje się różne klasyfikacje, np. zagrożenia można podzielić ze względu na lokalizację źródła zagrożenia oraz ze względu na jego przyczynę, co przedstawia rysunek nr 6.



Rysunek 6. Przykładowe kryteria podziału zagrożeń[4]

W powyższej klasyfikacji wyróżnia się zagrożenia wewnętrzne (np. działania pracownika, awaria systemu spowodowana brakiem zasilania) i zewnętrzne (np. atak DDoS). W przypadku drugiej klasyfikacji zagrożenia mogą być następstwem działań człowieka (przypadkowe lub umyślne) lub wynikać z przyczyn naturalnych (środowiskowych). Do umyślnych działań człowieka można zaliczyć np. kradzież lub modyfikację danych, zaś do przypadkowych np. skasowanie pliku czy uszkodzenie urządzenia. Oczywiście niektóre działania człowieka mogą być klasyfikowane zarówno jako umyślne, jak i jako przypadkowe, np. uszkodzenie nośnika danych. Do zagrożeń naturalnych możemy zaliczyć np. pożar czy też powódź. W przypadku danych osobowych, zgodnie z RODO, należy przeprowadzić identyfikację zagrożeń dla każdej operacji przetwarzania tych danych, a więc dla operacji takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Inny podział zagrożeń, przedstawiony na rysunku 7, publikuje na swoich stronach Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, który pełni rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym.

[4] Przykładową listę typowych zagrożeń, z podziałem na przyczyny, zawiera również Załącznik C normy PN-ISO/IEC 27005.

Katalog zagrożeń CERT.GOV.PL

	ZAGROŻENIA	PODATNOŚCI				
1. DZIAŁANIA CELOWE	1.1 - OPROGRAMOWANIE ZŁOŚLIWE	1.1.1 - wirus	1.1.2 - robak sieciowy	1.1.3 - koń trojański	1.1.4 - dialer	1.1.5 - klient botnetu
	1.2 - PRZEŁAMANIE ZABEZPIECZEŃ	1.2.1 - nieuprawnione logowanie	1.2.2 - włamanie na konto/ataki siłowe		1.2.3 - włamanie do aplikacji	
	1.3 - PUBLIKACJE W SIECI INTERNET	1.3.1 - treści obraźliwe	1.3.2 - pomawianie (zniesławianie)	1.3.3 - naruszenie praw autorskich	1.3.4 - dezinformacja	
	1.4 - GROMADZENIE INFORMACJI	1.4.1 - skanowanie	1.4.2 - podsłuch	1.4.3 -inżynieria społeczna	1.4.4 - szpiegostwo	1.4.5 - SPAM
	1.5 - SABOTAŻ KOMPUTEROWY	1.5.1 - nieuprawniona zmiana informacji	1.5.2 - nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji			
		1.5.3 - atak odmowy dostępu (np. DDoS, DoS)	1.5.4 - skasowanie danych			
		1.5.5 - wykorzystanie podatności w urządzeniach	1.5.6 - wykorzystanie podatności aplikacji			
	1.6 - CZYNNIK LUDZKI	1.6.1 - naruszenie procedur bezpieczeństwa	1.6.2 - naruszenie obowiązujących przepisów prawnych			
	1.7 - CYBERTERRORYZM	1.7.1 -Przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni				
2. DZIAŁANIA NIECELOWE	2.1 - WYPADKI I ZDARZENIA LOSOWE	2.1.1 - awarie sprzętowe	2.1.2 - awarie łącza	2.1.3 - awarie (błędy) oprogramowania		
	2.2 - CZYNNIK LUDZKI	2.2.1 - naruszenie procedur	2.2.2 - zaniedbanie	2.2.3 - błędna konfiguracja urządzenia	2.2.4 - brak wiedzy	2.2.5 - naruszenie praw autorskich

Rysunek 7. Katalog zagrożeń stosowany przez CERT.GOV.PL (źródło: www.cert.gov.pl)

Uwaga:

Wyżej wymieniona lista i katalog zagrożeń mają charakter pomocniczy, nie należy traktować ich jako zamkniętej listy (katalogu), ponieważ zagrożenia powinny zostać określone indywidualnie przez każdy podmiot.

3.2 Krok 3.2. Identyfikacja występujących podatności

Posiadając listy aktywów informacyjnych, wykaz zidentyfikowanych zagrożeń oraz zastosowanych zabezpieczeń, można przeprowadzić identyfikację podatności na urzeczywistnienie się określonych zagrożeń. Istotne jest to, że istnienie podatności nie powoduje jeszcze żadnej szkody. Może ona powstać dopiero po zmaterializowaniu się zagrożenia, które wykorzysta daną podatność. Przykładowo podatność, jaką jest słabe hasło dostępu do danych, nie powoduje szkody, dopóki ktoś nie podejmie próby jego „złamania" i nie zakończy się ona powodzeniem. Jednocześnie należy pamiętać, że analiza podatności nie jest przeprowadzana pod kątem zabezpieczeń. Zabezpieczenia stanowią jeden z mechanizmów wykorzystywanych na etapie postępowania z ryzykiem do minimalizowania tych podatności. Analiza podatności dotyczy głównie samych aktywów, zarówno tych podstawowych (przetwarzanych danych i

zastosowanych do przetwarzania urządzeń), jak i wspierających. Niemniej pod uwagę mogą być wzięte także istniejące zabezpieczenia.

Istotna informacja:

W przypadku aktywu, jakim jest zbiór danych osobowych, podatnością może być sam fakt wykorzystania tych danych w celu innym niż zamierzony.

W przypadku aktywów wspierających można wyróżnić wiele podatności związanych ze sprzętem, oprogramowaniem, siecią, personelem, siedzibą i organizacją – przykłady zaczerpnięte z normy PN-ISO/IEC 27005 przedstawione zostały na rysunku 8.

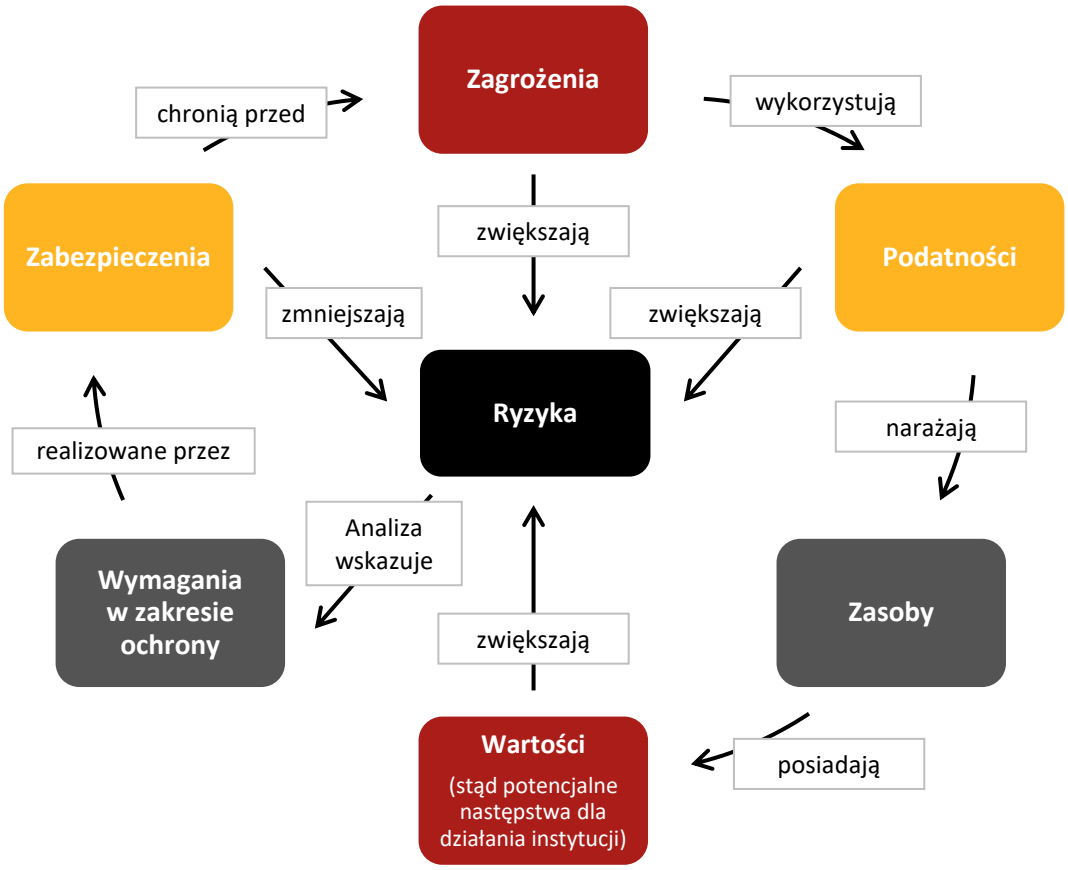
Rysunek 8. Przykładowe podatności wg normy PN-ISO/IEC 27005

3.3 Krok 3.3. Analiza i ocena następstw zmaterializowania się zagrożeń

Wykonanie działań określonych w kroku 1 i 2 pozwoli na zidentyfikowanie następstw, jakie może spowodować zmaterializowanie się zagrożenia (np. powstanie strat biznesowych, nałożenie kar finansowych z tytułu naruszenia prawa czy też utrata reputacji). Podczas identyfikacji następstw przygotowuje się listy scenariuszy incydentów (niepożądanych lub niespodziewanych zdarzeń). Scenariusz powinien opisywać

sposób, w jaki dane zagrożenie może wykorzystać określoną podatność oraz przedstawiać jego skutki. Skutki te należy określać zgodnie z przyjętymi kryteriami.

Oceniając następstwa urzeczywistnienia się zagrożeń, w przypadku przetwarzania danych osobowych, należy uwzględnić poza innymi czynnikami także dotkliwe kary finansowe, które mogą być nakładane przez organ nadzorczy na administratorów i podmioty przetwarzające w przypadku niewywiązywania się przez nie z nałożonych obowiązków właściwej ochrony danych. Dokonując identyfikacji ryzyka, warto mieć na uwadze związki, jakie występują pomiędzy wymienionymi wyżej czynnikami wpływającymi na to ryzyko, co zostało pokazane na rysunku 9.



Rysunek 9. Czynniki wpływające na ryzyko i związki między nimi. Wg PN-I-13335:1999

Po wykonaniu wyżej wymienionych kroków, w których dokonano pełnego rozpoznania występujących w danym kontekście przetwarzania aktywów informacyjnych (w tym danych osobowych), ustaleniu ich wrażliwości (dokonaniu klasyfikacji), zidentyfikowaniu zagrożeń, na jakie są narażone, uwzględnieniu zidentyfikowanych podatności oraz oceny potencjalnych skutków urzeczywistnienia występujących zagrożeń, należy ocenić całościowo poziom ryzyka, na jakie narażone są przetwarzane dane. Czynność taką nazywa się analizą ryzyka.

3.4 Krok 3.4. Szacowanie poziomu ryzyka

W ramach szacowania ryzyka, dla każdego scenariusza urzeczywistnienia się zidentyfikowanych zagrożeń, wykonywana jest ocena prawdopodobieństwa jego zajścia oraz szacowanie skutków jego zmaterializowania się. Mając wyznaczone prawdopodobieństwo wystąpienia określonego zdarzenia oraz straty, jakie mogą być nim spowodowane (tj. wielkość skutku), wyznacza się wartość ryzyka jako iloczyn prawdopodobieństwa wystąpienia danego zdarzenia i jego skutku.

Mimo posiadanej listy zidentyfikowanych aktywów i ich wartości, szacowanie następstw dla określonych zagrożeń nie jest proste, ponieważ następstwa mogą mieć dwojaki charakter: materialny oraz niematerialny.

W pierwszym przypadku szacowanie jest w miarę proste i może być związane z kosztami odtworzenia danego aktywu, co pokazano w Tabeli 1.

Drugi przypadek jest zwykle bardziej skomplikowany, ponieważ trudno jest ocenić wartości niematerialne, takie jak np. utrata dobrego wizerunku lub wpływ ujawnienia określonych danych na pozycję społeczną osoby, której one dotyczą.

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

Tabela 1. Przykładowe skutki ze względu na finanse i reputację

Przy szacowaniu prawdopodobieństwa incydentu zwykle uwzględnia się następujące czynniki:

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

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

Tabela 2. Przykładowe prawdopodobieństwo wystąpienia zdarzenia

Po przeprowadzeniu szacowania następstw oraz po określeniu prawdopodobieństwa wystąpienia poszczególnych incydentów przeprowadzane jest określanie poziomu ryzyka.

Najprostsza metoda to zdefiniowanie poziomu ryzyka jako iloczynu prawdopodobieństwa i skutków wystąpienia danego incydentu. Zwykle na tym etapie wykorzystuje się macierz ryzyka, która pozwala zobrazować poziomy ryzyka w sposób wizualny, grupując poziomy ryzyka za pomocą kolorów, dla których definiuje się odpowiednie działania.

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

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

Tabela 3. Przykładowa macierz ryzyka

Analiza ryzyka może być wykonywana na różnym poziomie szczegółowości i podczas jej przeprowadzania można zastosować podejście jakościowe, ilościowe lub mieszane.

W analizie jakościowej prawdopodobieństwo i potencjalne skutki prezentowane są w sposób opisowy. Wykorzystuje się w tym celu różnego rodzaju skale opisowe (rankingi), np. skalę o wartościach: niski, średni i wysoki. Zaletą analizy jakościowej jest łatwość jej zrozumienia, wadą - subiektywność wyboru skali.

W przypadku analizy ilościowej stosowane są skale numeryczne, zarówno dla prawdopodobieństwa, jak i skutków. Metoda ta wykorzystuje dane historyczne, zwykle związane z wystąpieniem poszczególnych incydentów, a jej poprawność zależy od jakości użytych danych, a także modeli statystycznych. Wadą tej metody może być potrzeba wykorzystania narzędzi informatycznych wspomagających te analizy, a także fakt, że w przypadku wystąpienia nowego typu ryzyk organizacja nie będzie dysponowała danymi historycznymi.

Biorąc pod uwagę wady i zalety przedstawionych powyżej analiz, większość organizacji przy analizie ryzyka stosuje podejście mieszane.

Uwaga:

Należy pamiętać, że np. norma PN-ISO/IEC 27001 nie określa metody, jakiej organizacje mają używać. Istotne jest to, żeby organizacja stosowała metodę zapewniającą powtarzalne rezultaty, które pozwolą na porównywanie wyników w czasie.

Oceniając ryzyko, powinno się pamiętać o tzw. efekcie domina, czyli kumulacji zagrożeń. Rzadko się zdarza, że w danym czasie wystąpi tylko jedno zagrożenie. Należy zawsze brać pod uwagę wystąpienie kilku zagrożeń w tym samym czasie, a także zmaterializowanie się nowego zagrożenia po wystąpieniu innego zagrożenia[5].

3.5 Krok 3.5. Określenie listy zidentyfikowanych ryzyk

Kolejnym działaniem powinno być porównanie poziomu ryzyk wyliczonych w kroku 4 dla poszczególnych operacji przetwarzania z kryteriami akceptacji ryzyka określonymi w kontekście danego rodzaju operacji przetwarzania i wymaganiami wskazanymi w kroku 2 etapu drugiego. W odniesieniu do operacji przetwarzania danych osobowych kontekst ten określony powinien być z uwzględnieniem warunków i zasad przetwarzania danych osobowych wskazanych w RODO. W wyniku tego porównania powinna zostać utworzona lista operacji przetwarzania z przyporządkowanymi im poziomami ryzyka.

Pomocna w realizacji tego kroku może okazać się poniższa tabela.

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

Tabela 4. Proponowana tabela operacji przetwarzania z oceną ryzyka.

[5] Do analizy wyzwań kumulacji zagrożeń wygodnym narzędziem może być metoda „Bow-tie, Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk; Praca pod redakcją bryg. dra inż. Dariusza Wróblewskiego wydana przez Narodowe Centrum Badań i Rozwoju, Józefów 2015; ISBN 978-83-61520-18-4; https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf, str. 77

Etap 4.
Postępowanie z ryzykiem - decyzja

04

Kolejną czynnością, jaką należy wykonać po oszacowaniu ryzyka dla poszczególnych operacji przetwarzania, jest podjęcie decyzji dotyczącej poszczególnych ryzyk.

Przykładowo w normie ISO/IEC 27005 wyróżnia się 4 możliwe rodzaje postępowań. Są to:

1) **modyfikowanie (redukcja) ryzyka** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia). Na przykład zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć, włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS-y, generatory). Zaś zmniejszenie związanych z tym zdarzeniem skutków utraty danych można osiągnąć, modyfikując system wykonywania kopii z wersji, w której kopia wykonywana jest jeden raz na dobę, do postaci, w której kopia jest wykonywana co 15 minut lub w sposób ciągły (na bieżąco) poprzez zastosowanie dodatkowych zabezpieczeń lub modyfikację procedur w sposób pozwalający na zaakceptowanie ryzyka szczątkowego;
2) **zachowanie (akceptacja) ryzyka** – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka;
3) **unikanie ryzyka** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków;
4) **dzielenie (przeniesienie) ryzyka** – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Trzeba zaznaczyć, że zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez dany podmiot do przepisów RODO. Ponadto administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie danych, to jako podmiot decydujący o zakresie i celach tego przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych.

Należy mieć na uwadze, że szczególnym przypadkiem jest sytuacja, gdy organizacja nie jest świadoma ryzyka i wobec tego nieświadomie wystawia się na nie w pełnym zakresie.

Możliwe rodzaje postępowań przedstawiono na rys. 10.

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

Na etapie tym, w przypadku, gdy określony rodzaj operacji przetwarzania danych osobowych związany jest z ryzykiem, które przekracza akceptowalny poziom, administrator lub podmiot przetwarzający musi podjąć decyzję co do dalszego działania/postępowania.

Najrozsądniejszym wyborem jest w takim przypadku podjęcie próby wprowadzenia dodatkowych środków bezpieczeństwa, które umożliwią obniżenie poziomu ryzyka lub całkowite jego wyeliminowanie.

To pierwsze rozwiązanie wymaga zazwyczaj dodatkowych inwestycji w środki zabezpieczające lub zmiany procedur, które mogą utrudnić lub wydłużyć czas wykonywania niektórych operacji przetwarzania.

W przypadku eliminacji ryzyka, konsekwencją jest najczęściej usunięcie określonych funkcjonalności. Na przykład dla systemu elektronicznej komunikacji spółki z jej akcjonariuszami wprowadzono moduł do elektronicznego głosowania podejmowanych uchwał z zamiarem wykorzystania go zarówno dla głosowań jawnych, jak i tajnych. Analiza ryzyka przeprowadzona dla tego modułu wykazała jednak wysokie ryzyko naruszenia tajności głosowania. Zespół koordynujący rozwój tego systemu na etapie postępowania z ryzykiem podjął w związku powyższym decyzję o rezygnacji z opcji systemu, która służyć miała do przeprowadzania głosowań tajnych.

W przypadku, gdy w kroku dotyczącym postępowania z ryzykiem podjęta zostanie decyzja o jego modyfikacji lub całkowitej eliminacji, cały proces dotyczący szacowania ryzyka powinien być powtórzony co najmniej od kroku 3 w etapie 1, a w skrajnym przypadku (jeśli ograniczono lub zmieniono cel przetwarzania danych) nawet od samego początku.

Dodatkowo, kiedy na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO wymagane jest przeprowadzenie dla danego procesu przetwarzania oceny jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.

Podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy administratora czy podmiotów przetwarzających, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

5. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Zarówno ogólna ocena ryzyka, jak i ocena skutków dla ochrony danych polega na wielokrotnym (cyklicznym) powtarzaniu 4 podstawowych etapów (kontekst, mechanizmy kontrolne, szacowanie ryzyka, postępowanie z ryzykiem) przedstawionych w niniejszym poradniku.

Jednakże ocena skutków dla ochrony danych powinna być zdecydowanie bardziej pogłębiona i przede wszystkim ukierunkowana na ochronę praw i wolności osób, których dane dotyczą. Innymi słowy ocena ta powinna koncentrować się na znalezieniu i wdrożeniu środków, które w jak największym stopniu zminimalizują ryzyko związane z naruszeniem tych praw i wolności.

Ocena ta może dotyczyć pojedynczej operacji przetwarzania danych. Należy jednak pamiętać, że art. 35 ust. 1 RODO stanowi, że „dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę". Motyw 92 RODO wskazuje, że „w niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach, gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną".

5.1 Ustalenie, czy przeprowadzenie oceny skutków jest wymagane

Przepisy ogólnego rozporządzenia o ochronie danych nie wymagają przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do każdej operacji przetwarzania, która może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe wyłącznie w przypadku, gdy przetwarzanie „**może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**" (zgodnie z art. 35 ust. 1, 3 i 4 RODO).

Przeprowadzenie oceny skutków dla ochrony danych jest wymagane zawsze wtedy, gdy:

1) **dany rodzaj przetwarzania został wskazany w przepisie prawa.** Przykładem takiego przepisu jest art. 35 ust. 3 RODO, zgodnie z którym przeprowadzenie oceny skutków dla ochrony danych wymagane jest w przypadku:

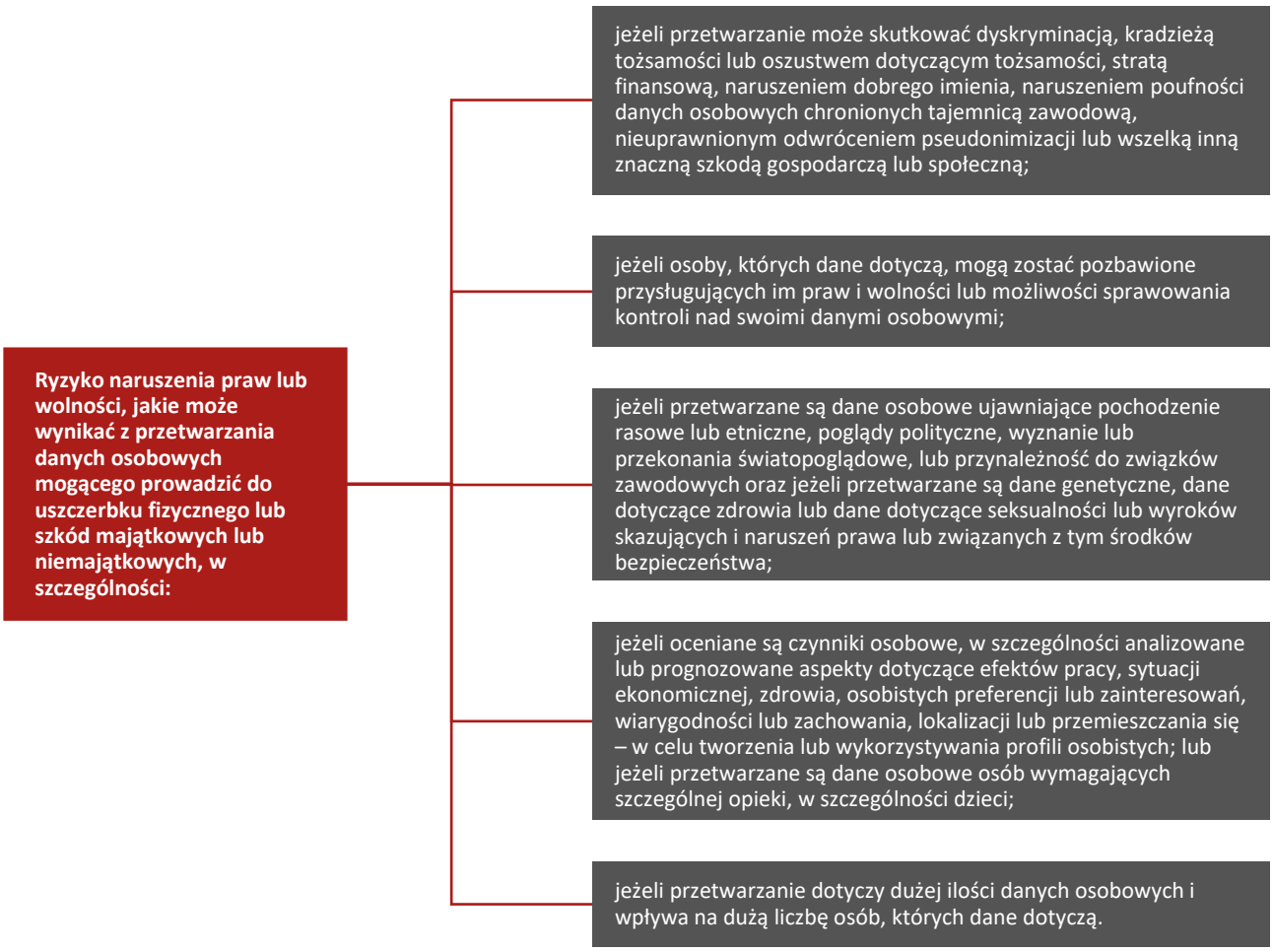
   a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

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

2) **dany rodzaj przetwarzania został wskazany w wykazie podanym** do publicznej wiadomości **przez krajowy organ nadzorczy**, zgodnie z art. 35 ust. 4 RODO.

3) **poziom ryzyka określony został jako wysoki w wyniku jego szacowania** przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania (w tablicy ryzyk, o której mowa w kroku 3.5).

Określając, czy ryzyko w konkretnym procesie przetwarzania jest wysokie i tym samym konieczne jest przeprowadzenie oceny skutków dla ochrony danych należy uwzględnić również motyw 75 RODO, który wskazuje przykładowe zagrożenia związane z przetwarzaniem danych, z wyszczególnieniem tych, prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, co przedstawiono na rysunku 11.



Rysunek 11. Kontekst i cele przetwarzania prowadzące do naruszenia praw i wolności.

Wymieniona w art. 35 ust. 3 RODO lista operacji przetwarzania, dla których należy przeprowadzać ocenę skutków dla ochrony danych, nie jest katalogiem zamkniętym. Wynika to również z wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych[6], w których wskazano wiele przykładów operacji wymagających przeprowadzania oceny skutków dla ochrony danych (str. 9 i następne).

Grupa Robocza Art. 29 przy analizie, czy ocena skutków dla ochrony danych jest wymagana, zaleca zweryfikowanie czy przetwarzanie spełnia następujące kryteria:

1. **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" (motywy 71 i 91 RODO);
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);
3. **Systematyczne monitorowanie**: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c RODO);
4. **Dane wrażliwe lub dane o charakterze wysoce osobistym,** np. obejmujące szczególne kategorie danych osobowych określone w art. 9 RODO oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO;
5. **Dane przetwarzane na dużą skalę**;
6. **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 (motyw 75 RODO);
8. **Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych;**
9. **Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy"** (art. 22 i motyw 91 RODO).

Im więcej kryteriów zostanie spełnionych w ramach przetwarzania, tym większe prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą. Oczywiście należy pamiętać, że w przypadkach, gdy przetwarzanie spełnia tylko jedno z wymienionych kryteriów, może ono również wymagać przeprowadzenia oceny skutków dla ochrony danych. W sytuacjach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, Grupa Robocza Art. 29 rekomenduje przeprowadzenie takiej oceny.

Należy nadmienić, że organ nadzorczy, stosownie do art. 35 ust. 5 RODO, może również ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania

[6] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, (WP 248 rev.01), przyjęte w dniu 4 kwietnia 2017 r., ostatnio zmienione i przyjęte w dniu 4 października 2017 r., http://www.giodo.gov.pl/pl/file/12864

oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.

Ocena skutków dla ochrony danych nie jest wymagana, jeżeli operacja przetwarzania, zgodnie z art. 6 ust. 1 lit. c lub e RODO, ma podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już w związku z przyjęciem tej podstawy prawnej (art. 35 ust. 10 RODO), chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem czynności przetwarzania.

5.2 Zasięgnięcie opinii ekspertów i osób, których dane dotyczą lub ich przedstawicieli. Stworzenie ram dla oceny skutków dla ochrony danych w kodeksach postępowania.

Dodatkowym działaniem, jakie powinno być przeprowadzone w niektórych przypadkach przeprowadzania oceny skutków dla ochrony danych, jest zasięgnięcie opinii ekspertów i osób, których dane dotyczą lub ich przedstawicieli.

Zgodnie z art. 35 ust. 9 RODO, w stosownych przypadkach administrator musi zasięgnąć opinii osób, których dane dotyczą lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania. Zasięgnięcie opinii takich podmiotów (np. potencjalnych klientów, stowarzyszeń konsumenckich), pozwoli administratorowi uwzględnić w swojej decyzji perspektywę osób, których dane dotyczą. W ten sposób administrator może uzyskać od danej społeczności dodatkowe informacje na temat ich ewentualnych obaw i zastrzeżeń dotyczących przetwarzania ich danych w określonym kontekście. Forma przeprowadzenia takich konsultacji (zebrania opinii) nie została wskazana w powołanym przepisie. Opinie osób można zatem uzyskać w dowolny, odpowiedni w danej sytuacji sposób, np. za pomocą ankiet, bezpośrednich rozmów z wybranymi osobami lub konsultacji z reprezentującymi je organizacjami.

Jeśli w organizacji wyznaczony został inspektor ochrony danych, należy konsultować z nim podejmowane działania (art. 35 ust. 2 RODO). Wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych[7] zalecają administratorowi i podmiotowi przetwarzającemu zasięganie porady inspektora ochrony danych, między innymi w następujących kwestiach:

- czy należy przeprowadzić ocenę skutków dla ochrony danych;
- jaką metodologię należy przyjąć przy przeprowadzeniu oceny skutków dla ochrony danych;
- czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu;
- jakie zabezpieczenia (w tym środki techniczne i organizacyjne) mają zastosowanie w celu złagodzenia wszelkich zagrożeń dla praw i interesów osób, których dane dotyczą;

[7] Wytyczne dotyczące inspektorów ochrony danych ('DPO') przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r. (16/EN WP 243 rew.01), dostępne: http://giodo.gov.pl/pl/1520281/9939

- czy ocena skutków została prawidłowo przeprowadzona oraz czy jej wyniki są zgodne z wymogami ochrony danych (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).

W procesie oceny skutków dla ochrony danych ułatwieniem może być przestrzeganie przez administratora lub podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO. Grupa Robocza Art. 29 w Wytycznych dotyczących oceny skutków dla ochrony danych zachęca do opracowywania ram oceny skutków dla ochrony danych dla poszczególnych sektorów, opartych na specyficznej dla danego sektora wiedzy. Dzięki temu ocena skutków dla ochrony danych może zaradzić problemom, które powstają w konkretnym sektorze gospodarki, przy stosowaniu konkretnych technologii lub przy przeprowadzaniu operacji przetwarzania określonego rodzaju.

W dużych organizacjach o złożonej strukturze może być potrzebne wyznaczenie zespołu odpowiedzialnego za prowadzenie procesu zarządzania ryzykiem. Biorąc pod uwagę, że zarządzanie ryzykiem obejmuje wszystkie szczeble organizacji, a także to, że proces ten powinien być częścią procesu zarządzania organizacją, osoby wybrane do zespołu powinny mieć odpowiednio wysokie umocowanie (więcej na ten temat znajduje się w Części I poradnika „Jak rozumieć podejście oparte na ryzyku?", str. 8).

Przeprowadzając ocenę skutków dla ochrony danych, warto przygotować plan działania utworzonego zespołu, w którym wymienione będą zadania, jakie należy wykonać. W planie tym powinny być wskazane między innymi takie elementy, jak:

a) przegląd i uzupełnienie kontekstu przetwarzania danych, o którym mowa w etapie 1, o elementy, które mogą wskazać powiązanie przetwarzanych danych z innymi zbiorami danych, np. czy dane dotyczące kontroli wejścia/wyjścia do/z siedziby/pomieszczeń firmy są łączone z danymi kadrowymi w celu ewidencji czasu pracy,

b) przegląd i uzupełnienie zastosowanych środków bezpieczeństwa, np. w przypadku wprowadzania danych typu PESEL, data urodzenia, uzupełnienie procedury wprowadzania o weryfikację zgodności tych danych z przyjętym formatem i/lub dopuszczalnymi wartościami, np. data urodzenia nie może być późniejsza niż data aktualna,

c) uwzględnienie elementów kulturowych i obyczajowych danej społeczności, której członków dane są przetwarzane, np. uwzględnienie niechęci osób do przetwarzania ich danych biometrycznych, takich jak odcisk linii papilarnych, z uwagi na ich negatywne psychologiczne konotacje z policyjnymi metodami śledczymi,

d) uwzględnienie elementów specyficznych dla danego kontekstu przetwarzania, np. szkody, jaką może spowodować brak dostępu do danych lub ich nieuprawniona zmiana w określonych okolicznościach, np. w szpitalu przed lub w czasie wykonywanej operacji lub zabiegu medycznego.

5.3 Uwzględnienie szczególnych elementów oceny skutków dla ochrony danych

Niezależnie od tego, jakie czynniki spowodowały konieczność przeprowadzenia oceny skutków dla ochrony danych, przeprowadzając taką ocenę można skorzystać z opisu kontekstu i celów przetwarzania, który został wykonany dla celów ogólnej oceny ryzyka. Na potrzeby oceny skutków dla ochrony danych, należy go

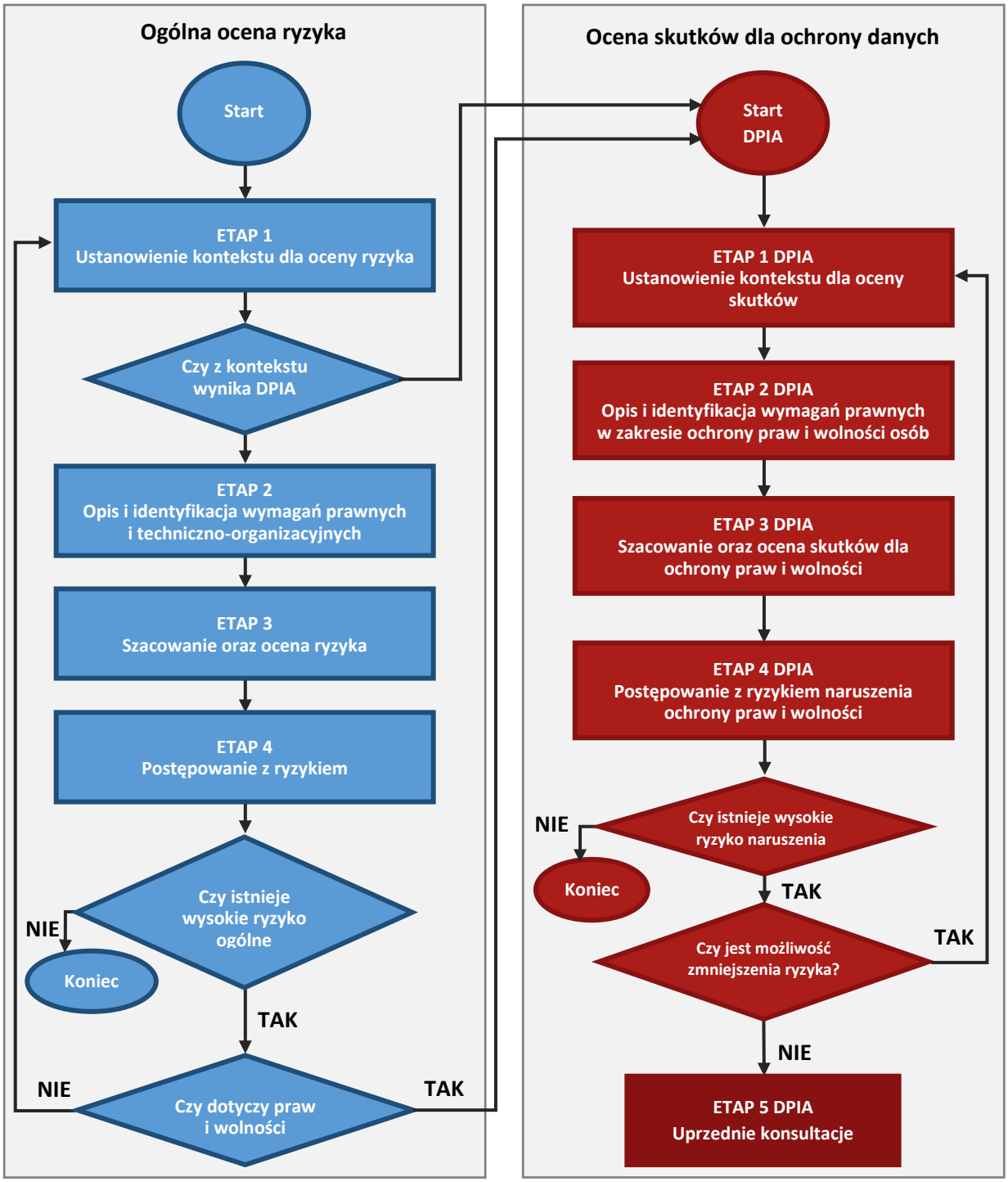
uzupełnić o elementy istotne z punktu widzenia skutków dla ochrony praw i wolności osób, których dane są przetwarzane.

Ocena skutków dla ochrony danych powinna być zdecydowanie bardziej pogłębiona i przede wszystkim ukierunkowana na ochronę praw i wolności osób, których dane dotyczą. Jest ona procesem pozwalającym opisać procesy przetwarzania danych, ale także - ocenić ich konieczność, proporcjonalność i wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych. Dlatego powinna być ona traktowana jako szczególny rodzaj szacowania ryzyka, w którym baczną uwagę należy zwrócić na zastosowane środki minimalizacji ryzyka.

Ogólne rozporządzenie o ochronie danych nie zawiera definicji pojęcia „*ocena skutków dla ochrony danych*”[8], ale w art. 35 ust. 7 RODO precyzuje, że ocena ta powinna zawierać co najmniej:

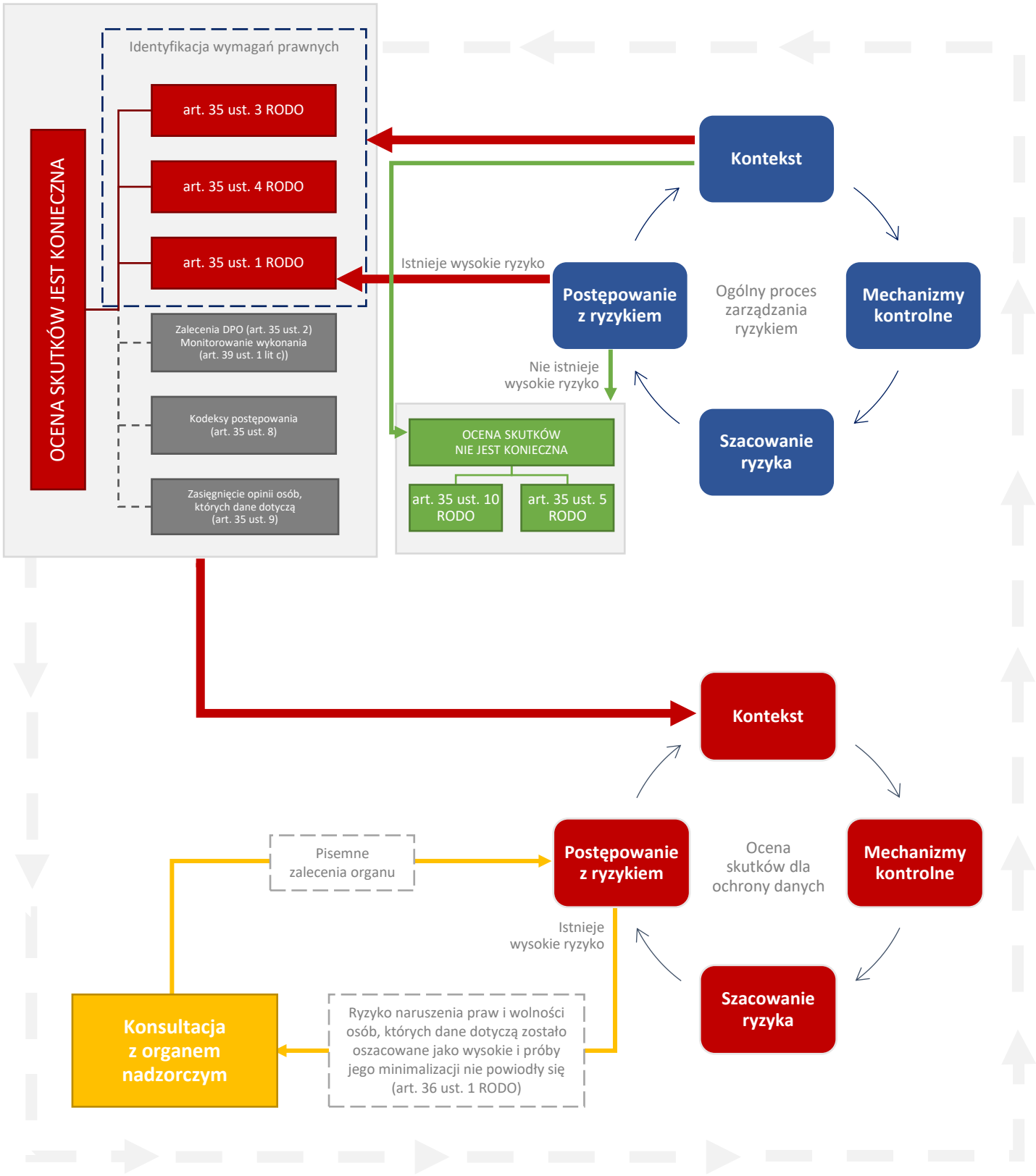
- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w art. 35 ust. 1 RODO;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

[8] Przykłady istniejących unijnych ram dokonywania oceny skutków dla ochrony danych wskazane zostały w załączniku 1 do Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych.



Rysunek 12. Ogólne etapy oceny ryzyka oraz oceny skutków dla ochrony danych.

Schemat relacji ogólnej oceny ryzyka do oceny skutków dla ochrony danych z uwzględnieniem niektórych elementów dotyczących opisu kontekstu i postępowania z ryzykiem przedstawiono na rysunku 13.



Rysunek 13. Szczegółowe etapy oceny ryzyka oraz oceny skutków dla ochrony danych.

Grupa Robocza Art. 29 w załączniku 2 do Wytycznych dotyczących oceny skutków dla ochrony danych zaproponowała listę warunków, których spełnienie należy zweryfikować oraz zagadnień, które w ocenie skutków należy uwzględnić, aby upewnić się, czy ocena została przeprowadzona z uwzględnieniem kompletności otoczenia i wszystkich czynników mających wpływ na prawa i wolności osób, których dane są przetwarzane. Lista ta obejmuje następujące grupy zagadnień:

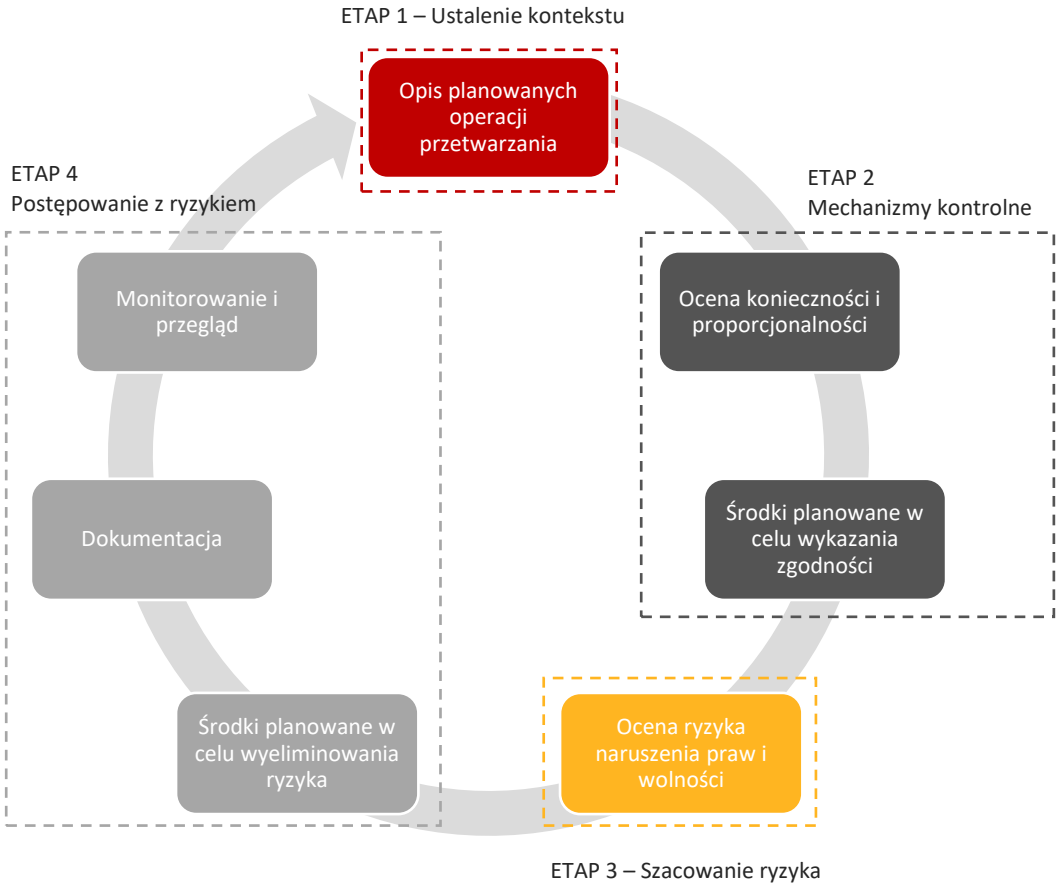
- ☐ **zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a):**
  - ☐ uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
  - ☐ w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
  - ☐ przedstawiono funkcjonalny opis operacji przetwarzania;
  - ☐ zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
  - ☐ uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);
- ☐ **oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b):**
  - ☐ wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
    - ☐ środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
      - ☐ konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b);
      - ☐ zgodność przetwarzania z prawem (art. 6);
      - ☐ dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c);
      - ☐ ograniczony czas przechowywania (art. 5 ust. 1 lit. e);
    - ☐ środki przyczyniające się do zachowania praw osób, których dane dotyczą:
      - ☐ poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
      - ☐ prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
      - ☐ prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
      - ☐ prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
      - ☐ relacje z podmiotem przetwarzającym (art. 28);
      - ☐ zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
      - ☐ uprzednie konsultacje (art. 36);
- ☐ **przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c):**
  - ☐ uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
    - ☐ uwzględniono źródła ryzyka (motyw 90);
    - ☐ zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
    - ☐ zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
    - ☐ oszacowano prawdopodobieństwo i powagę (motyw 90);

- ☐ określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d i motyw 90);

☐ **zaangażowano zainteresowane strony:**

- ☐ skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);
- ☐ w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).

W Wytycznych dotyczących oceny skutków dla ochrony danych został również zaproponowany wykres przedstawiający proces przeprowadzania oceny skutków dla ochrony danych (rysunek nr 14). Poszczególne fazy tego procesu można przyporządkować 4 podstawowym etapom ogólnej oceny ryzyka prezentowanym w niniejszym poradniku.



Rysunek 14.

Wynikiem przeprowadzonej oceny skutków powinno być oszacowanie poziomu ryzyka naruszenia praw i wolności osób, których dane dotyczą (np. ryzyko wysokie, ryzyko niskie).

Poniższa tabela może być pomocna przy przedstawieniu i usystematyzowaniu wyników oceny skutków dla ochrony danych.

Rodzaj operacji przetwarzania danych	Zidentyfikowane zagrożenia	Poziom ryzyka naruszenia praw i wolności	Decyzja	Uzasadnienie akceptacji wyliczonego poziomu ryzyka
Przechowywanie elektronicznej dokumentacji medycznej	Utrata dostępności danych w przypadku awarii nośnika danych.	Niski (uzasadnienie: wdrożono system kopii zapasowej w trybie ciągłym ze względu na niezbędność ciągłego dostępu do danych pacjentów).	Akceptacja ryzyka	Zastosowanie systemu kopii zapasowej w trybie ciągłym, w architekturze systemów pracujących równolegle, zapewniających ciągłość dostępu na poziomie wysokim.

Tabela 5. Przykład tabeli *operacji przetwarzania z oceną ryzyka.*

W sytuacji, kiedy w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i próby jego minimalizacji nie powiodły się - wówczas przed rozpoczęciem przetwarzania danych należy wyniki przeprowadzonej oceny skonsultować z organem nadzorczym, chyba że administrator podejmie decyzję o nieprzetwarzaniu danych, np. niewprowadzaniu nowej usługi.

Ponadto taka konsultacja będzie wymagana zawsze, gdy prawo państwa członkowskiego obliguje administratorów do konsultacji z organem nadzorczym lub uzyskiwania jego uprzedniej zgody w odniesieniu do przetwarzania danych osobowych przez administratora do celów wykonania zadania realizowanego przez niego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym (art. 36 ust. 5 RODO).

Zwracając się w trybie uprzednich konsultacji o pomoc w zakresie podjęcia decyzji o rozpoczęciu przetwarzania, powinno się przedstawić organowi nadzorczemu następujące dokumenty:

a) gdy ma to zastosowanie – wskazujące odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
b) wskazujące cele i sposoby zamierzonego przetwarzania;
c) wskazujące środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;
d) gdy ma to zastosowanie – wskazujące dane kontaktowe inspektora ochrony danych;
e) ocenę skutków dla ochrony danych, o której mowa w art. 35 RODO;
f) wszelkie inne informacje, których żąda organ nadzorczy.

Ogólna ocena ryzyka oraz ocena skutków dla ochrony danych, powinny być przeprowadzane systematycznie. Cały cykl powinien być przeprowadzony od początku każdorazowo, gdy zmieniają się okoliczności mające wpływ na proces przetwarzania danych, np. dojdzie do naruszenia ochrony danych, nastąpi zmiana kontekstu np. wymagań prawnych.

Nawet w przypadku niezaistnienia warunków, które obligują do przeprowadzenia obowiązkowej oceny skutków dla ochrony danych, należy pamiętać o ogólnym obowiązku wdrożenia przez administratora środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia praw i wolności osób, których dane dotyczą. Oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”.

Oceny te powinny być dokumentowane przez administratora zgodnie z zasadą rozliczalności. Ponadto, jeżeli ocena skutków dla ochrony danych nie wymaga przeprowadzenia procedury uprzednich konsultacji, obowiązki administratora polegające na przechowywaniu ww. dokumentacji związanej z oceną skutków dla ochrony danych i dokonywaniu aktualizacji oceny skutków dla ochrony danych w stosownym terminie, pozostają aktualne.

Jest to bardzo istotne, ponieważ ogólne rozporządzenie o ochronie danych przewiduje nałożenie administracyjnej kary pieniężnej w wysokości do 10 mln EUR lub, w przypadku przedsiębiorstwa, do 2 % całkowitego rocznego obrotu w skali światowej w poprzednim roku budżetowym, w zależności od tego, która kwota jest wyższa w sytuacji nieprzestrzegania wymogów dotyczących oceny skutków dla ochrony danych, np. nieprzeprowadzenia oceny skutków dla ochrony danych, gdy przetwarzanie podlega takiej ocenie (art. 35 ust. 1 i 3–4 RODO), nieprawidłowym przeprowadzeniu oceny skutków dla ochrony danych (art. 35 ust. 2 i 7–9 RODO) lub brakiem konsultacji z właściwym organem nadzorczym, gdy jest to wymagane (art. 36 ust. 3 lit. e RODO).

Zarówno ocena skutków dla ochrony danych, jak i ogólna ocena ryzyka nie powinny być odbierane przez podmioty zobligowane do ich przeprowadzenia jedynie jako dodatkowy, uciążliwy obowiązek. Z punktu widzenia administratora oba te procesy mogą przyczynić się do zapewnienia pełnej zgodności z przepisami RODO. Warto zatem do wyzwania stworzenia i wdrożenia przemyślanej, w pełni odpowiadającej nowym wymogom prawnym i specyfice danego podmiotu koncepcji zarządzania ryzykiem podejść z zaangażowaniem i rzetelnie. Tym samym uczynić z systemu zarządzania ryzykiem swój atut świadczący o wzorowym podejściu do przestrzegania przepisów ogólnego rozporządzenia o ochronie danych, a tym samym poszanowania praw i wolności, osób, których dane dotyczą.

Wyjaśnienie użytych terminów

- **Aktywa** - jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), jak np. dane osobowe.
- **Aktywa podstawowe** – są to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).
- **Aktywa wspierające –** są to środki umożliwiające korzystanie z aktywów podstawowych. Przykładem aktywów wspierających jest sprzęt, oprogramowanie, sieć, pracownicy.
- **Anonimizacja –** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.
- **Grupa Robocza Art. 29 -** Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.
- **Identyfikowanie ryzyka** – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.
- **Kontekst** – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.
- **Kryteria akceptacji ryzyka** – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2.
- **Kryteria oceny ryzyka** - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.
- **Naruszenie ochrony danych osobowych -** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
- **Ocena ryzyka** – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.

- **Operacja przetwarzania danych osobowych** - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- **Podatność** - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

- **Proces przetwarzania danych osobowych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

- **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

- **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 (ogólne rozporządzenie o ochronie danych), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

- **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)[9].

- **Właściciel aktywów –** jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.

- **Zabezpieczenie** - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

- **Zagrożenie** - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

---

[9] Podobna definicja znajduje się w publikacji sfinansowanej przez Narodowe Centrum Badań i Rozwoju w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne" nr DOBR/0016/R/ID2/003 pod tytułem „Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk" pod redakcją bryg. dra inż. Dariusza Wróblewskiego.
W ramach procesu „szacowanie ryzyka" ujęto takie zadania, jak: ustalenie kontekstu, ocena ryzyka, postępowanie z ryzykiem oraz jego monitorowanie i przegląd. Inny dokument - norma PN-ISO 31000:2012, zamiast pojęciem „szacowania ryzyka", posługuje się pojęciem „oceny ryzyka", które obejmuje proces identyfikacji ryzyka, jego analizę i ewaluację.

Przydatne materiały

1. Komisja Nadzoru Finansowego, Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, stanowiąca załącznik do uchwały nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r., dostępna pod: https://www.knf.gov.pl/dla_rynku/fin_tech/platnosci_elektroniczne/wybrane_stanowiska_i_regulacje?articleId=55482&p_id=18
2. Opinia Grupy Roboczej Art. 29, 3/2010 w sprawie zasady rozliczalności (WP 173), dostępna pod: http://giodo.gov.pl/pl/1520057/3732
3. Opinia Grupy Roboczej Art. 29, 4/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych (WP 205), dostępna pod: http://giodo.gov.pl/pl/1520167/6567
4. Opinia Grupy Roboczej Art. 29, 7/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci (WP 209), dostępna pod: http://giodo.gov.pl/pl/1520167/7546
5. Opinia Grupy Roboczej Art. 29, 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180), dostępna pod: http://giodo.gov.pl/pl/1520110/4085
6. Opinie i wytyczne Grupy Roboczej Art.29 dotyczące wdrożenia RODO: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
7. Privacy Impact Assessments - CNIL, dostępne pod: https://www.cnil.fr/fr/node/15798
8. Publikacje przygotowane przez ICO, dostępne pod: https://ico.org.uk/global/request-publications/
9. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dostępne pod: http://www.giodo.gov.pl/pl/1520284/9745
10. Rządowy Zespół Reagowania na Incydenty Komputerowe, dostępne pod: www.cert.gov.pl
11. Stanowisko Grupy Roboczej Art. 29 w sprawie podejścia opartego na ryzyku w ramach prawnych ochrony danych (WP 218), dostępne pod: http://giodo.gov.pl/pl/1520203/7936
12. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów Rozporządzenia 679/2016 (WP 248), dostępne pod: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
13. Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk; Praca pod redakcją bryg. dra inż. Dariusza Wróblewskiego wydana przez Narodowe Centrum Badań i Rozwoju, Józefów 2015; ISBN 978-83-61520-18-4; https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl