



Nowe elementy dokumentacji przetwarzania danych związane z RODO

Andrzej Kaczmarek

Dyrektor Departamentu Informatyki
Biuro Generalnego Inspektora Ochrony Danych Osobowych

Warszawa, 22 Marca 2018 r.

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

PLAN PREZENTACJI

1. Cel prowadzenia dokumentacji przetwarzania.
2. Zawartość dokumentacji przetwarzania (model dotychczasowy, model zgodny z RODO)
3. Dokumentowanie czynności przetwarzania
4. Dokumentowanie analizy ryzyka oraz oceny skutków
5. Zaangażowanie pracowników jednostki

Znaczenie dokumentacji przetwarzania?

Celem dokumentacji przetwarzania jest wskazanie i uporządkowanie przyjętych w jednostce organizacyjnej procesów przetwarzania, roli w tych procesach poszczególnych jednostek, wskazanie zakresu ich zadań i odpowiedzialności, a także przyjętych technicznych i organizacyjnych środków bezpieczeństwa.

Zadaniem dokumentacji przetwarzania danych w jednostce jest również wykazanie, że poszczególne procesy realizowane są prawidłowo, zgodnie ze wskazanym celem przy zachowaniu jednocześnie wszystkich obowiązków wynikających z przepisów prawa.

Główne elementy dokumentacji przetwarzania



W niektórych obszarach zakres dokumentacji mogą wskazywać przepisy prawa, lub przyjęte standardy.

Przykładem mogą być przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Rozporządzenie to wprost wskazywało, że na dokumentację przetwarzania danych osobowych składają się **polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**, zwana dalej „instrukcją”

Główne elementy dokumentacji przetwarzania – polityka bezpieczeństwa

W dalszej części Rozporządzenia wskazywano, że Polityka bezpieczeństwa, o zawiera w szczególności:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami;
- 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Główne elementy dokumentacji przetwarzania – Instrukcja zarządzania



Odnośnie instrukcji zarządzania systemem informatycznym Rozporządzenie wskazywało, że powinna ona zawierać w szczególności:

- 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności ([Internet -procedura rejestracji](#));
- 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem ([Internet – zapomniane hasło](#));
- 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu ([Internet – pliki cookies](#));
- 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

Główne elementy dokumentacji przetwarzania – Instrukcja zarządzania

- 5) sposób, miejsce i okres przechowywania:
 - a) elektronicznych nośników informacji zawierających dane osobowe,
 - b) kopii zapasowych, o których mowa w pkt 4,
- 6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
- 7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
- 8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych
- 9) **Sposób zabezpieczenia nośników z danymi przekazywanymi poza obszar przetwarzania danych (dla danych wrażliwych)**

Co powinna dodatkowo zawierać dokumentacja uwzględniająca przepisy RODO

Oдноśnie dokumentacji czynności przetwarzania RODO wypowiada się w art. 24 dotyczącym zadań administratora danych, który stanowi że:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i **aby móc to wykazać**. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują **wdrożenie przez administratora odpowiednich polityk ochrony danych**.
3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Co powinna dodatkowo zawierać dokumentacja uwzględniająca przepisy RODO

W RODO są elementy w odniesieniu do których bardziej szczegółowo wskazano zadania dotyczące dokumentacji.

Odnoszą się one między innymi do:

1. Wykazu czynności przetwarzania danych osobowych.
2. Wykazu kategorii czynności przetwarzania.
3. Zgłaszania incydentów naruszenia ochrony danych.
4. Zawartości raportu z oceny skutków dla ochrony danych osobowych.

Co powinna dodatkowo zawierać dokumentacja uwzględniająca przepisy RODO

Biorąc pod uwagę również potrzeby włączenia dotychczasowych elementów dokumentacji można podsumować, że dokumentacja przetwarzania zgodna z RODO powinna zawierać.

- **Rejestr czynności przetwarzania**
- **Wewnętrzny rejestr zbiorów i przepływu danych między nimi**
- **Wyniki przeprowadzonej analizy ryzyka**
- **Raport z oceny skutków dla ochrony prywatności**
- **Politykę bezpieczeństwa**
- **Instrukcję zarządzania**
- **Wytyczne dla prowadzenia wewnętrznego rejestru naruszeń, ich zgłaszania do organu nadzorczego oraz powiadamiania osób, których one dotyczyły**
- **Ewidencję osób upoważnionych**

Zakres dokumentacji przetwarzania

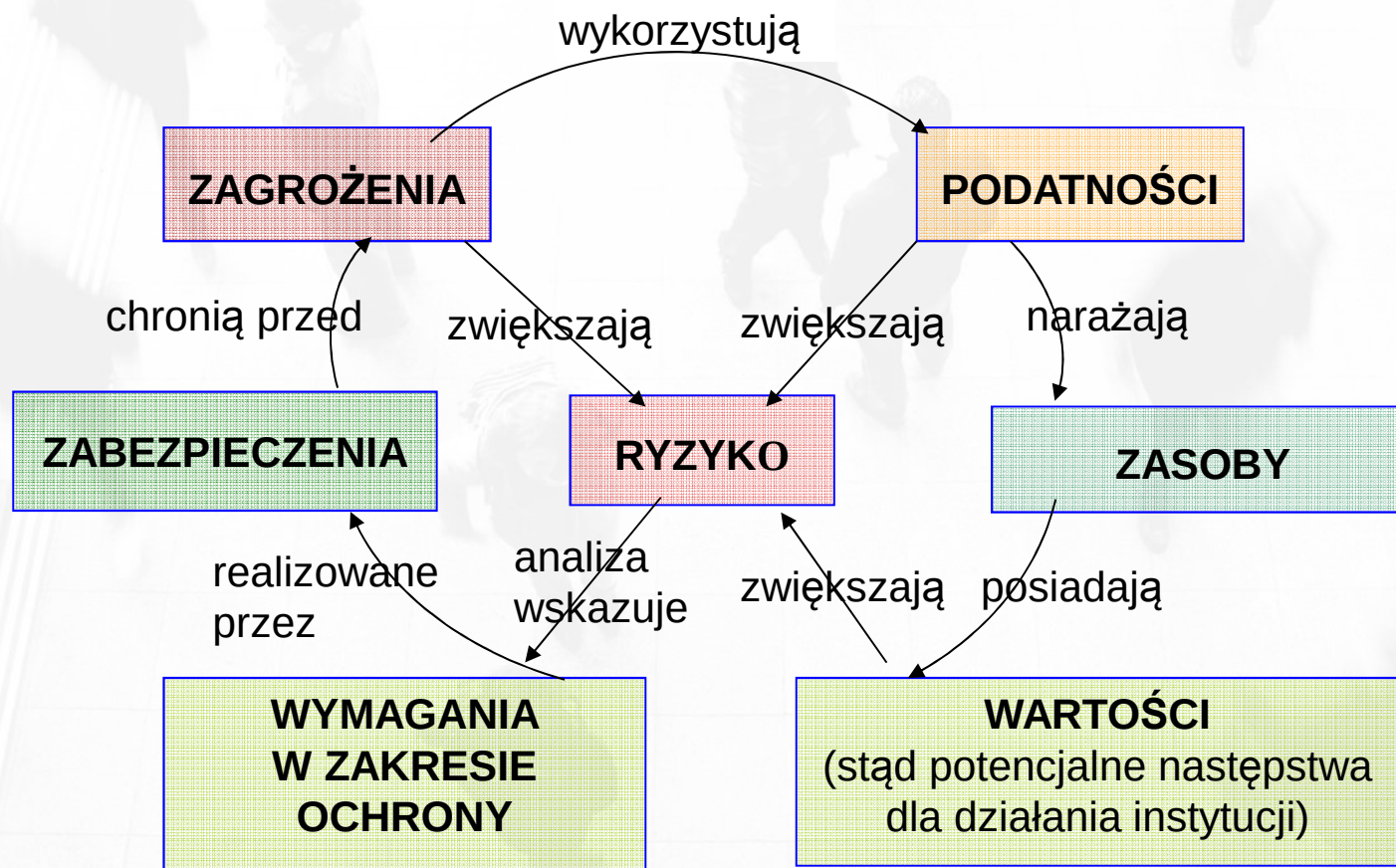
Elementy dokumentacji przetwarzania powinny odnosić się do wszystkich stosowanych narzędzi i technologii przetwarzania

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



Bezpieczeństwo informacji – proces zabezpieczania poufności, integralności i dostępności informacji

Model związków między elementami wpływającymi na bezpieczeństwo



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

Art. 36 u.o.d.o.

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

Art. 37 u.o.d.o.

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

Art. 38 u.o.d.o.

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

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



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

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

Wymagania wskazane w załączniku do rozporządzenia

Wymagania dotyczące ochrony (załącznik do rozporządzenia)

Podstawowy

Podwyższony

Wysoki

- 1) Zabezpieczenie obszaru przetwarzania;
- 2) Kontrola dostępu (indywidualne konto dla każdego użytkownika);
- 3) Zabezpieczenie przed szkodliwym oprogramowaniem i awarią zasilania;
- 4) Niepowtarzalność identyfikatora, odpowiednie parametry dotyczące hasła oraz obowiązek tworzenia kopii zapasowych;
- 5) Kryptograficzne zabezpieczenie komputerów przenośnych;
- 6) Odpowiednie procedury przenoszenia, likwidacji i napraw sprzętu;
- 7) Monitorowanie wdrożonych zabezpieczeń;
- 8) **Dodatkowa wymagania dotyczące hasła dla danych wrażliwych;**
- 9) **Dodatkowe zabezpieczenie danych wrażliwych opuszczających obszar przetwarzania (ochrona kryptograficzna);**
- 10) **Opis sposobu zabezpieczenia o którym mowa w punkcie 9 i jego ochrona;**
- 11) **Kontrola i zabezpieczenie przepływu danych na styku z siecią publiczną;**
- 12) **Kryptograficzna ochrona danych przesyłanych w sieci publicznej;**

Wymagania wskazane w załączniku do rozporządzenia

Wymagania dotyczące funkcjonalności (§ 7 rozporządzenia)

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
 - 1) daty pierwszego wprowadzenia danych do systemu;
 - 2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu posiada wyłącznie jedna osoba;
 - 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
 - 4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
 - 5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Wymagana określone w RODO

Obowiązki administratora. (Art. 24 rodo)

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

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

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

Sugerowane w RODO środki bezpieczeństwa

1. Pseudonimizacja i **szyfrowanie** danych

- rozdzielenie danych identyfikacyjnych od pozostałych, jak zorganizować ?
- Jak zapewnić ścisłą kontrola dostępu do danych identyfikacyjnych i sposobu ich połączenia z pozostałymi danymi ?
- kiedy dane należy szyfrować ?
- jaką zastosować metodę szyfrowania ?
- kryptografię symetryczną (EAS, Twofish – jak długi klucz 128,192, 256 bitów ?)
- kryptografię asymetryczną (RSA, DSA, Diffie-Hellmana – klucz 512 , 1024 - 4096)
- a może wystarczy funkcja hashująca (skrót); SHA-2, SHA-3, RIPEMD-160?
- wprowadzić zasady zarządzania kluczami kryptograficznymi

2. Zapewnienie zdolności do ciągłego zapewniania poufności, integralności, dostępności i odporności usług przetwarzania.

- jakie zastosować rozwiązania dla zapewnienia ciągłości poufności i integralności?
- czy dedykowana indywidualnie kontrola dostępu i suma kontrolna będą wystarczające?
- czy niezbędne jest szyfrowanie i podpis elektroniczny ? jak zarządzać kluczami?

Sugerowane w RODO środki bezpieczeństwa

3. Zapewnienie dostępności danych



- ustalenie dopuszczalnej utraty danych (Recovery Point Objective)
- ustalenie maksymalnego czasu niedostępności (Recovery Time Objective)
- wybór właściwej organizacji i technologii (Plan Ciągłości Działania BCP)
- testy sprawności (gotowości)

Obowiązek prowadzenia rejestru czynności wynika z treści art. 30 RODO. W rejestrze tym powinny znaleźć się następujące informacje:

- 1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- 2) cele przetwarzania;
- 3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- 4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- 5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- 6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Sposób prowadzenia rejestru czynności

Rozporządzenie nie narzuca wymagań dotyczących układu wymaganych informacji w prowadzonych rejestrach. Stanowi jedynie, że rejestry powinny być prowadzone w **formie pisemnej**.

Rozporządzenie nie narzuca również wymagań dotyczące **postaci** w jakiej przedmiotowe rejestry powinny być prowadzone, co oznacza, że może to być postać zarówno **papierowa**, jak i **elektroniczna**.

Brak szczegółowego wskazania układu wymaganych informacji w poszczególnych rejestrach oznacza, że np. administrator danych może przyjąć dowolny układ informacji dotyczących poszczególnych czynności przetwarzania.

Na przykład w odniesieniu do pozycji e) w rejestrze czynności przetwarzania dotyczącej informacji o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, administrator może podzielić te informacje na mniejsze jednostki np. na dwie podpozycje takie jak:

Kogo dotyczy obowiązek prowadzenia rejestru czynności i rejestru kategorii czynności przetwarzania?

Obowiązek prowadzenia rejestru czynności spoczywa na administratorze, czyli osobie fizycznej lub prawnej, organie publicznym, jednostce lub innym podmiocie, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych

Obowiązek prowadzenia rejestru czynności przetwarzania przez podmioty przetwarzające będzie dotyczył między innymi rejestracji czynności przetwarzania w odniesieniu do danych osobowych zatrudnionego personelu, których podmiot przetwarzający jest administratorem. Obowiązek taki będzie występował nawet w przypadku zatrudnienia mniej niż 250 osób z uwagi na fakt, że przetwarzania danych pracowników w związku z zatrudnieniem nie można zakwalifikować do przetwarzania o charakterze sporadycznym.

Cel prowadzenia rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania

Z treści motywu 82 wynika, że dla zachowania zgodności z RODO każdy administrator oraz podmiot przetwarzający powinni prowadzić odpowiednio rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania. Każdy administrator i każdy podmiot przetwarzający powinny mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępnić te rejestry w celu monitorowania tych operacji przetwarzania.

Biorąc pod uwagę wskazane w motywie 82 RODO cele prowadzenia ww. rejestrów, tj. :

1. zachowanie przez administratora zgodności z RODO;
2. umożliwienie organowi nadzorczemu monitorowania prowadzonych operacji w ramach współpracy między nim a organem nadzorczym,

Rejestry czynności i kategorii czynności mają być udostępniane przez administratorów na żądanie organu nadzorczego (art. 30 ust. 4 RODO).

Pojęcie czynności przetwarzania danych osobowych

W RODO nie zostało zdefiniowane wprost **pojęcie czynności przetwarzania** danych. Samo pojęcie „**przetwarzanie**” zostało zdefiniowane w art. 4 pkt 2 jako operacja lub zestaw operacji na danych takie 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*; Powstaje zatem pytanie jak należy interpretować pojęcie „czynności przetwarzania danych”

Z kontekstu w jakim w RODO użyto pojęcia **czynności przetwarzania** wynika, że pojęcie to może odnosić się kompleksowo do zestawu operacji przetwarzania związanych z określonym celem np. sprzedażą, a nie do częściowych operacji, takich jak: *rejestrowanie danych nabywcy (klienta), wystawienie faktury, wydanie klientowi oryginału faktury, przechowywanie kopii faktury w systemie sprzedaży, zapis danych z faktury w rejestrze VAT czy też po zakończeniu każdego miesiąca generowanie pliku JPK-VAT, jego weryfikowanie, podpisanie, wysłanie do Urzędu Skarbowego, itp.*

Pojęcie czynności przetwarzania danych osobowych



GIODO

Przy grupowanie poszczególnych, cząstkowych operacji przetwarzania w **zestawy operacji** nazywane **czynnościami przetwarzania** celowe wydaje się uwzględnienie rzeczywistego podziału czynności przetwarzania w danej jednostce organizacyjnej. W dużych jednostkach np., w strukturze organizacyjnej często wydziela się oddzielne zespoły do spraw Kadr i Płac. Zespół Kadr wykonuje wówczas najczęściej takie czynności przetwarzania jak prowadzenie ewidencji pracowników, czasu ich pracy, szkoleń, urlopów, zwolnień lekarskich itp. Zespół ten wykonuje najczęściej również takie czynności jak zgłaszanie pracowników i członków ich rodzin do ZUZ a także zgłaszanie wszelkich ich aktualizacji.

Zespół Płac natomiast prowadzi takie czynności przetwarzania jak wyliczanie wynagrodzeń i ich wypłata a także takie czynności jak wyliczanie składek na ubezpieczenie emerytalne, rentowe, chorobowe, wypadkowe a także ich przekazywanie do ZUS wraz z imiennymi raportami miesięcznymi ZUS RCA o należnych składkach i wypłaconych świadczeniach.

Czynności przetwarzania danych - to jedna lub więcej operacji przetwarzania danych wykonywanych jednocześnie lub w określonej sekwencji, w określonym miejscu, przez określoną osobę lub grupę osób w określonym celu.

Jak jest relacja między zbiorem danych osobowych a czynnościami przetwarzania?

W dotychczasowej praktyce przetwarzania danych osobowych istotne znaczenie miało pojęcie zbioru danych osobowych. Zbiór danych osobowych w art. 7 pkt 1 Ustawy o ochronie danych osobowych zdefiniowany jest jako: każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Podobnie zbiór danych został zdefiniowany w art. 4 pkt 6 RODO. Zbiór danych zdefiniowano tam jako zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rejestry **czynności przetwarzania danych**, o których mowa w RODO są skonstruowane w odmienny sposób niż dotychczasowe rejestry zbiorów danych. Nie odzwierciedlają one podziału całego zestawu przetwarzanych danych osobowych na zbiory danych, ale na czynności przetwarzania. Przy czym pojęcie „**czynność przetwarzania**” bliższe jest pojęciu określonej **funkcjonalności zbioru danych**, która ma służyć wykonaniu określonych czynności, niż do pojęciu samego zbioru danych.

Prowadzenie rejestru czynności przetwarzania

Pomimo, że art. 30 ust. 1 wprost mówi o prowadzeniu rejestru czynności przetwarzania, to nie wymaga się, aby w rejestrze tym wydzielone były i w jakiś sposób nazwane poszczególne czynności. Wydaje się jednak w pełni uzasadnione, zestawienie informacji w poszczególnych zapisach (rekordach) tego rejestru pod kątem ustalonych czynności przetwarzania.

Z drugiej strony biorąc pod uwagę fakt, że dany administrator prowadzi rejestr wszystkich czynności przetwarzania, które wykonywane są w jego organizacji, rejestr ten powinien być tak skonstruowany, aby dla każdej czynności nie było potrzeby powtarzania informacji o nazwie i danych kontaktowych administratora, jego przedstawiciela czy inspektora ochrony danych. Ponadto mając na uwadze fakt, że dany administrator, może wykonywać jedne czynności jako ich administrator, inne zaś jako współadministrator, celowe jest, aby:

- 1) Informacje o nazwie administratora danych, jego danych kontaktowych, nazwie przedstawiciela i jego danych kontaktowych a także nazwisku i danych kontaktowych inspektora ochrony danych umieścić jednorazowo np. na stronie tytułowej przedmiotowego rejestru.
- 2) Dla każdego wpisu w rejestrze czynności na pierwszej pozycji umieścić nazwę lub opis czynności przetwarzania a następnie pozostałe informacje o danej czynności wymienione w art. 30 ust 1 punkty od b) do g).

Czy rejestr czynności może obejmować inne elementy niż wskazane w art. 30 ust. 1 RODO

Wskazane w art. 30 ust. 1 RODO składniki rejestru (kryteria klasyfikacji przetwarzanych danych osobowych) są obligatoryjnie wymagane. Jednakże wskazany w tym przepisie zakres informacji o danej czynności nie ma charakteru zamkniętego. Zatem mogą się w nim znaleźć inne elementy, które administrator uzna za zasadne uwzględniając wiele specyficznych dla niego czynników, takich jak:

- wskazanie podstawy prawnej przetwarzania,
- wskazanie źródła pozyskania danych,
- wskazanie użytego do przetwarzania systemu informatycznego,
- informacje dotyczące przeprowadzonej oceny skutków dla ochrony danych, itp.

W niektórych przypadkach uzasadnione może okazać się odnotowanie w rejestrze dodatkowo takich informacji jak np.:

- określenie tzw. właścicieli procesów, czyli osób odpowiedzialnych u administratora za konkretne czynności przetwarzania danych (np. kierownik określonej komórki w organizacji, wydzielone stanowisko itp.), oraz
- dane kontaktowe podmiotu przetwarzającego oraz subprocesorów.

Czy rejestr czynności może obejmować inne elementy niż wskazane w art. 30 ust. 1 RODO

Zamieszczenie innych niż wymagane w art. 30 ust 1 RODO danych może być przydatne szczególnie w kontekście wykazania zgodności wykonywanych czynności przetwarzania z przepisami RODO. Jeśli zatem w rejestrze tym dla każdej czynności wskażemy np. przepis prawa dający podstawę przetwarzania danych w ramach danej czynności, czy np. w odniesieniu do informacji wysyłanej drogą elektroniczną wskażemy sposób jej zabezpieczenia, wówczas łatwiej w przypadku kontroli będzie wykazać zgodność z zasadami RODO. Ponadto rejestr taki, podczas jego tworzenia, aktualizacji i przeglądania będzie przypominał samemu administratorowi o obowiązku zapewnienia określonych w RODO zasad i warunków przetwarzania.

Podejście do tworzenia rozszerzonego o dodatkowe elementy rejestru czynności przetwarzania zalecane jest obecnie między innymi przez organy nadzorcze ochrony danych w Belgii www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement i Wielkiej Brytanii <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities>

Przykład zalecanego przez GIODO zestawu informacji jakie może obejmować rozszerzony rejestr czynności przetwarzania

Strona tytułowa rejestru

Informacje ogólne dotyczące rejestru czynności przetwarzania

Nazwa administratora

Adres

Email

Nr Telefonu/Faksu

Informacje dotyczące przedstawiciela administratora

Nazwa przedstawiciela

Adres

Email

Nr Telefonu/Faksu

Dane dotyczące inspektora Ochrony Danych

Imię i Nazwisko

Adres kontaktowy

Email

Nr Telefonu/Faksu

Rejestr czynności przetwarzania – co powinien zawierać - przykład

Zawartość informacji o poszczególnych czynnościach przetwarzania

1. Nazwa czynności przetwarzania;
2. Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)
3. Nazwa jednostki organizacyjnej administratora (Departament, Dział itp.);
4. Nazwy systemów lub oprogramowania;
5. Kategorie osób;
6. Kategorie danych;
7. Cel przetwarzania;
8. Podstawa prawna;
9. Planowany termin usunięcia kategorii danych (wskazać jeżeli jest to możliwe);
10. Źródło przetwarzanych danych;
11. Kategorie odbiorców – podmiot przetwarzający (jeśli dotyczy) + inni odbiorcy;
12. Nazwy państw trzecich lub organizacji międzynarodowych do których dane są przekazywane;
13. Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust 1 (nazwa dokumentu, załącznik lub link);
14. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe);
15. Informacje dotyczące DPIA (jeśli tak, wskazać lokalizację raportu).

Pojęcie kategorii czynności przetwarzania danych osobowych

RODO nie definiuje wprost pojęcia „kategorii przetwarzania” jak również pojęcia „kategorii czynności przetwarzania”.

Pojęcie kategorii przetwarzania nie jest w RODO również zdefiniowane. W RODO pojęcia „kategoria przetwarzania” użyto w art. 23 ust 2 pkt a w zdaniu „celach przetwarzania lub kategorii przetwarzania” oraz w art. 23 ust 2 pkt f w zdaniu „okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania”.

Pojęcie „kategorii czynności przetwarzania” natomiast po raz pierwszy i jednocześnie ostatni użyto w art. 30 ust. 2, który mówi o obowiązku prowadzenia przez podmioty przetwarzające rejestru **kategorii czynności przetwarzania**.

Mając na uwadze przyjętą w punkcie 2 definicję czynności przetwarzania oraz informacje, jakie powinny znaleźć się przy opisie zamieszczonej w tym rejestrze „kategorii czynności przetwarzania” zasadne wydaje się przyjęcie interpretacji, że:

Kategoria czynności przetwarzania - to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związany ze zleconymi czynnościami przetwarzania.

Pojęcie kategorii czynności przetwarzania danych osobowych

Z praktyki w zakresie oferowanych przez podmioty przetwarzające usług przetwarzania danych wynika, że zakres takich usług obejmuje między innymi:

- 1) przechowywanie danych rozumiane jako udostępnienie określonej przestrzeni w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający sam zarządza i decyduje o tym, jakie dane tam przechowuje – hosting zasobów pamięci elektronicznej;**
- 2) udostępnianie mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej lub innych usług na potrzeby instalacji i eksploatacji usług przetwarzania, którymi zamawiający w pełni zarządza – hosting infrastruktury informatycznej;**
- 3) udostępnienie określonej platformy sprzętowo programowej (np. serwera www wraz z odpowiednim oprogramowaniem do prowadzenia np. własnej strony internetowej, sklepu internetowego, prowadzenie księgowości, itp;**
- 4) wykonywanie na zamówienie klienta określonych usługi w zakresie konfiguracji sprzętowej, programowej, w tym zabezpieczeń serwerów klienta, innych urządzeń komputerowych oraz oprogramowania klienta – hosting usług administracyjnych i konserwacyjnych;**
- 5) wykonywanie na zamówienia klienta usług programistycznych, w tym aktualizacji oprogramowania na okoliczność zmieniających się przepisów prawnych lub wymagań klienta – hosting usług programistycznych, itp.**

Prowadzenie rejestru kategorii czynności przetwarzania



Art. 30 ust 2 RODO w odniesieniu do rejestru kategorii czynności przetwarzania nie wymaga, aby w rejestrze tym wydzielone były i w jakiś sposób nazwane poszczególne kategorie czynności przetwarzania.

Wydaje się jednak w pełni uzasadnione, że jeżeli ma to być **rejestr kategorii czynności przetwarzania**, to zestawienie informacji w poszczególnych zapisach (rekordach) tego rejestru powinno być uporządkowane pod kątem świadczonych na zlecenie administratorów kategorii czynności przetwarzania (rodzaju świadczonych usług).

Ponadto biorąc pod uwagę fakt, że każdy taki rejestr odnosi się do kategorii czynności przetwarzania świadczonych przez dany podmiot oraz że w rejestrze tym powinny być wymienione kategorie świadczonych usług dla każdego z administratorów celowe jest aby struktura zapisu była następująca:

Proponowana struktura rejestru kategorii czynności przetwarzania

- 1. Informacje o nazwie podmiotu przetwarzającego, jego danych kontaktowych, nazwie i danych kontaktowych jego przedstawiciela a także nazwisku i danych kontaktowych jego inspektora ochrony danych umieścić jednorazowo np. na stronie tytułowej przedmiotowego rejestru.**
- 2. Dla każdego wpisu w rejestrze czynności na pierwszej pozycji umieścić nazwę i dane kontaktowe administratora danych dla którego dana kategoria czynności przetwarzania jest wykonywana, nazwę i dane kontaktowe przedstawiciela administratora, nazwisku i danych kontaktowych wyznaczonego przez niego inspektora ochrony danych a następnie wszystkie pozostałe informacje wskazane w art. 30 ust 2 pkt b do pkt d.**

Przykład rejestru kategorii czynności przetwarzania

Strona tytułowa rejestru kategorii czynności przetwarzania

Informacje ogólne dotyczące rejestru kategorii czynności przetwarzania

Nazwa podmiotu przetwarzającego

Adres

Email

Nr Telefonu/Faksu

Informacje dotyczące przedstawiciela podmiotu przetwarzającego

Nazwa przedstawiciela

Adres

Email

Nr Telefonu/Faksu

Dane dotyczące inspektora Ochrony Danych

Imię i Nazwisko

Adres kontaktowy

Email

Nr Telefonu/Faksu

Przykład zalecanego przez GODO rejestru kategorii czynności przetwarzania



Zawartość informacji o poszczególnych kategoriach czynnościach przetwarzania realizowanych na zlecenia każdego z administratorów, w następującej kolejności:

- 1) Nazwa i dane kontaktowe administratora danych lub podmiotu przetwarzającego;
- 2) Nazwa i dane kontaktowe przedstawiciela administratora lub podmiotu przetwarzającego (jeśli dotyczy)
- 3) Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (administratora danych lub podmiotu przetwarzającego)
- 4) Kategoria przetwarzań (Typ, Rodzaj, kategoria świadczonej usługi przetwarzania);
- 5) Nazwy państw trzecich lub organizacji międzynarodowych do których dane są przekazywane;
- 6) Informacje dotyczące dokumentacji w zakresie odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust 1 – jeśli dotyczy;
- 7) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe).

Inne elementy dokumentacji przetwarzania

Zawartość dokumentacji powinna być dostosowana do potrzeb jej odbiorców. W dokumentacji każdy powinien znaleźć informacje dotyczące sposobu postępowania w określonych, a często również i krytycznych sytuacjach.

Wymagana określone w RODO i związane z nimi ryzyko

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



Ryzyko w
bezpieczeństwie
przetwarzania

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



Ryzyko nie wykonania
obowiązków
formalnych

Uwzględnienie ryzyka przy projektowaniu i
zarządzaniu bezpieczeństwem przetwarzania

Ocena wpływu przetwarzania na prawa i
wolności podmiotów danych



Ocena ryzyka / skutków
(DPIA)

Minimalizacji ryzyka dokonuje się stosując zabezpieczenia organizacyjne i techniczne

Działania jakie należy podejmować (1)

- 1) Zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- 2) Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
- 3) Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji;
- 4) Podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków;

Minimalizacji ryzyka dokonuje się stosując zabezpieczenia organizacyjne i techniczne

Działania jakie należy podejmować (2)

- 5) Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań lub zakresu obowiązków;
- 6) Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
 - a) zagrożenia bezpieczeństwa informacji,
 - b) skutki naruszenia zasad bezpieczeństwa informacji materialne, prawne),
 - c) stosowanie środków zapewniających bezpieczeństwo;
- 7) Zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
 - a) monitorowanie dostępu do informacji,
 - b) czynności zmierzające do wykrycia nieautoryzowanych działań,
 - c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

Minimalizacji ryzyka dokonuje się stosując zabezpieczenia organizacyjne i techniczne

Działania jakie należy podejmować (3)

- 8) Ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- 9) Zabezpieczenia informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
- 10) Zawierania w umowach serwisowych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
- 11) Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

Minimalizacji ryzyka dokonuje się stosując zabezpieczenia organizacyjne i techniczne

Działania jakie należy podejmować (4)

- 12) Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
- a) dbałości o aktualizację oprogramowania,
 - b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
 - c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
 - d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
 - e) zapewnieniu bezpieczeństwa plików systemowych,
 - f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.
 - g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
 - h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

Minimalizacji ryzyka dokonuje się stosując zabezpieczenia organizacyjne i techniczne

Działania jakie należy podejmować (4)

- 13) Bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
- 14) Zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Szacowanie ryzyka a systemy zarządzania

Normy, dobre praktyki, kodeksy postępowania

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

Zarządzanie ryzykiem

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

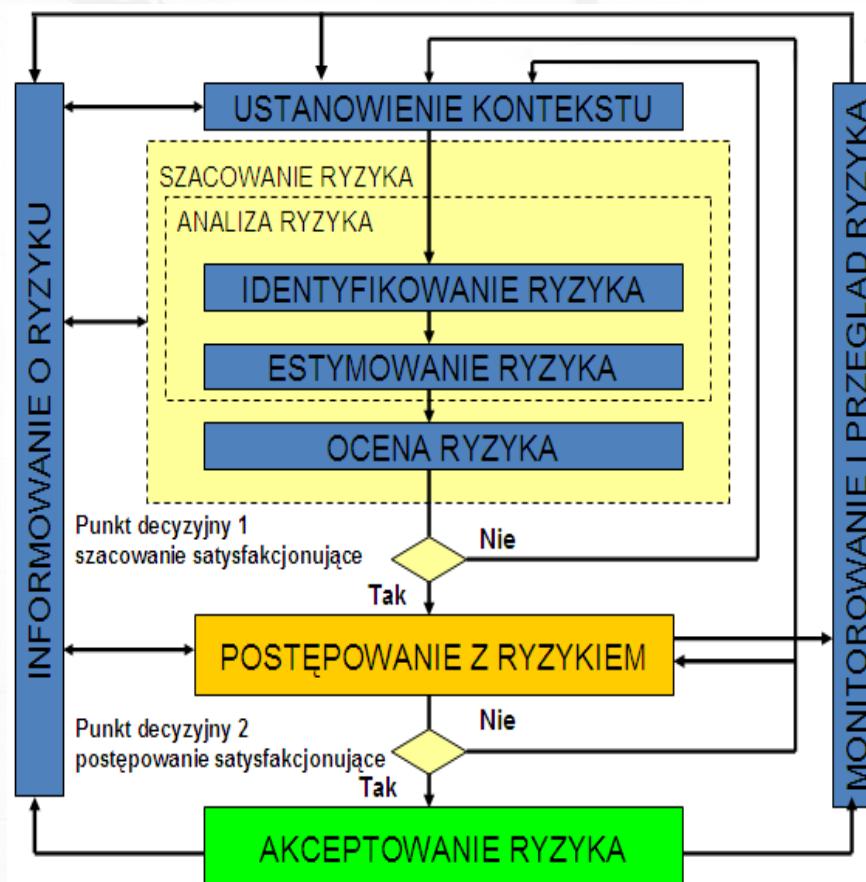
* Publikacja jest ogólnie dostępna, finansowana przez NCBIR w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”

Szacowanie ryzyka w bezpieczeństwie informacji

Identyfikacja ryzyka w BI (PDO)

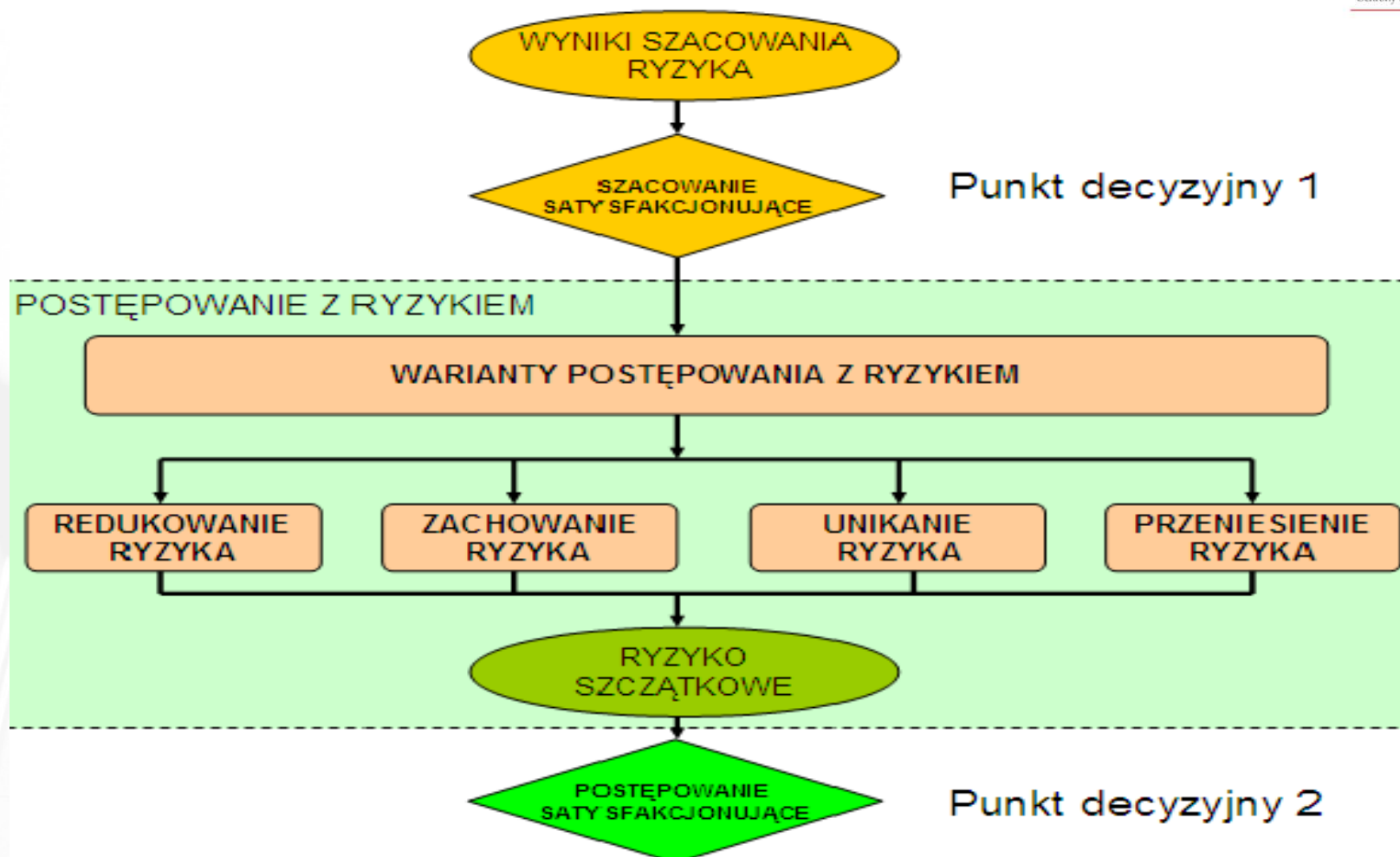
- ✓ Identyfikacja aktywów
- ✓ Identyfikacja zagrożeń - ich prawdopodobieństwa wystąpienia
- ✓ Identyfikacja podatności (środowiska przetwarzania)
- ✓ Identyfikacja zabezpieczeń i ich skuteczności
- ✓ Identyfikacja następstw

Analiza ryzyka- PN-ISO/IEC 27005



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

Szacowanie ryzyka w bezpieczeństwie informacji



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

Ryzyka wynikające z nakładania się różnych zagrożeń - przykład



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

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



WYNIKI POJEDYNCZEGO ZLECENIA
(Logowanie bez Karty Stałego Klienta)

Numer zlecenia:

Rok urodzenia: Miesiąc urodzenia: Dzień urodzenia:

ZALOGUJ ➔

Numer zlecenia znajdziesz na górze dokumentu, który otrzymałeś w punkcie pobrań. Jeżeli otrzymałeś paragon lub karteczkę z naklejonym kodem kreskowym, numer Zlecenia znajdziesz pod kodem kreskowym. Dowiedz się więcej o wynikach jednorazowych. [KLIKNIJ TU](#)

Uwzględnienie oceny skutków dla ochrony praw i wolności osób

Realizacja praw osoby – czynności administratora

- Podstawa przetwarzania art. 6 rodo
 - ✓ zgoda,
 - ✓ przepis prawna,
 - ✓ umowa.
- Warunki wyrażenia zgody art. 7 rodo
 - przechowywane dokumenty zgody, umowy,
 - wycofanie.
- Zgoda opiekuna art. 8 rodo
 - sprawdzić wiek osoby,
 - zmodyfikowanie aplikacji i baz informacyjnych,
 - brak wytycznych dot. realizacji.
- Dane szczególnej kategorii art. 9 i 10 rodo
 - sprawdzić czy występują,
 - czy jest podstawa do ich przetwarzania.
- Prawo dostępu
- Prawo do sprostowania
- Prawo do przeniesienia
- Prawo do ograniczenia
- Obowiązki powiadomienia o naruszeniu

Szacowanie ryzyka

Ustanowienie kontekstu

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

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

Informacje dotyczące:

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

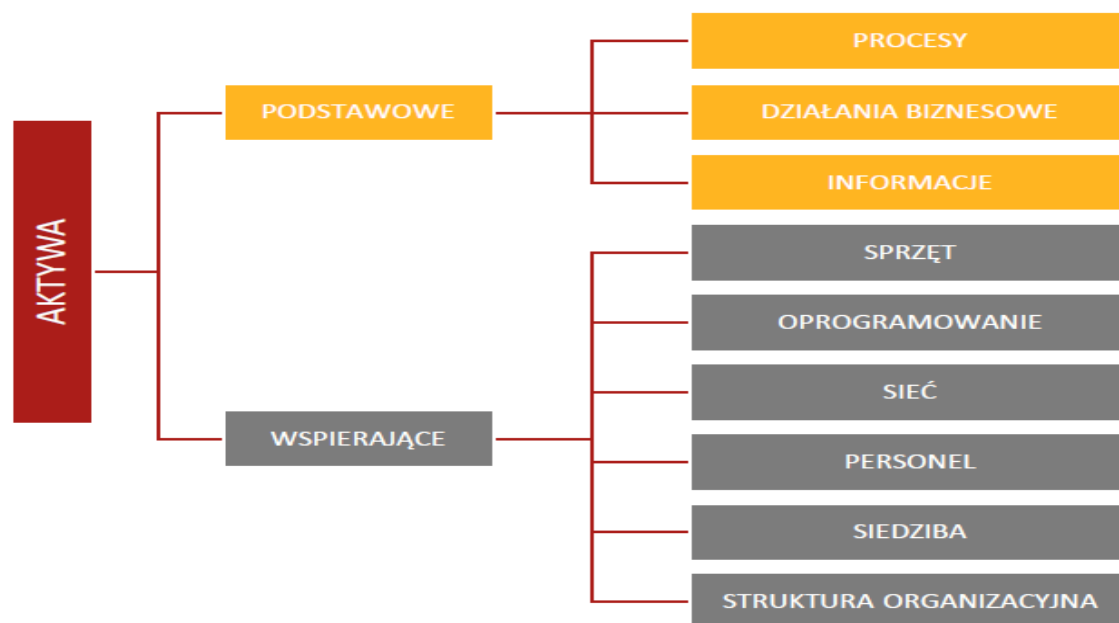
Informacje dotyczące:

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

Kontekst – opis, identyfikacja i klasyfikacja

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

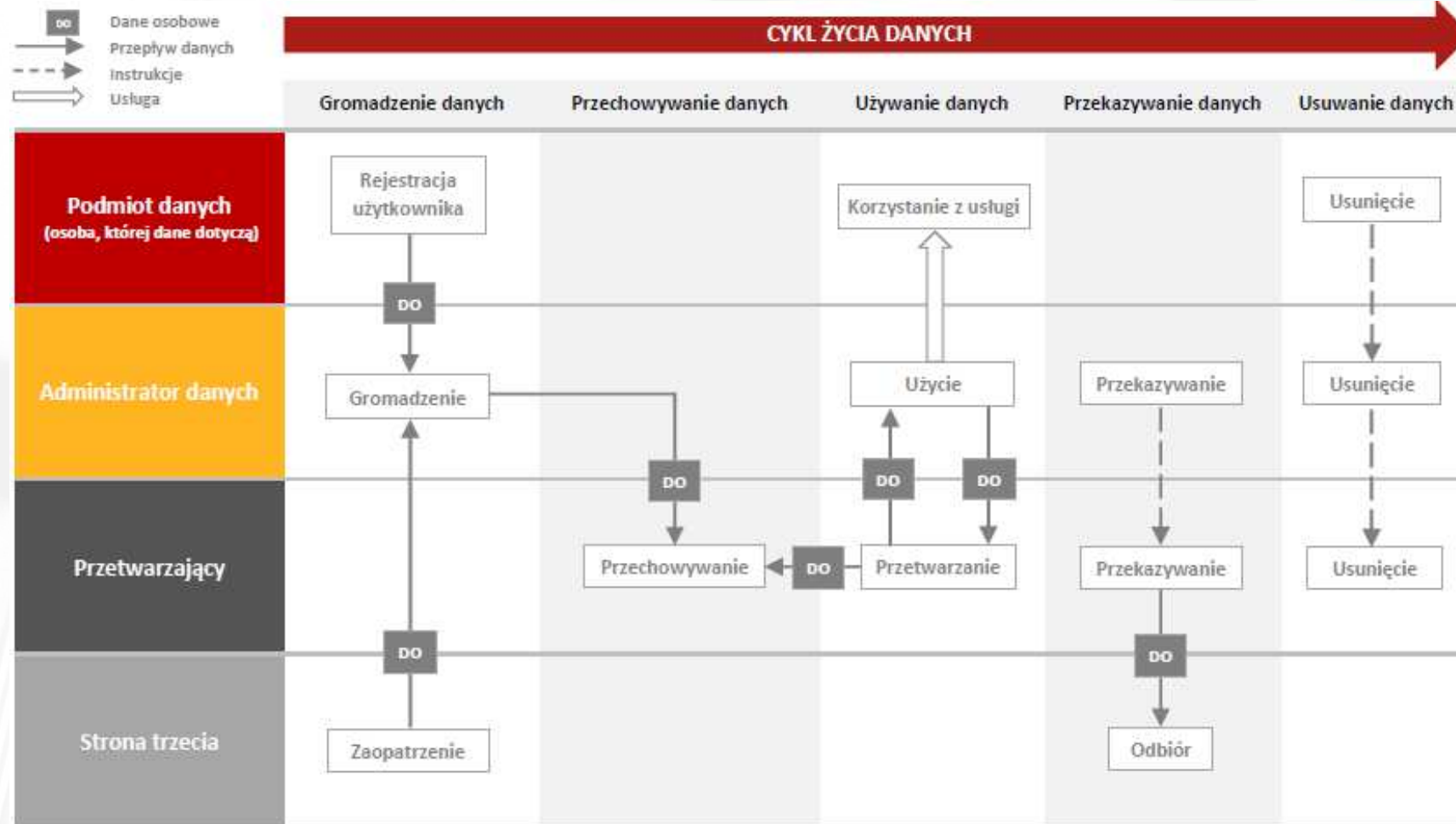
Identyfikacja i klasyfikacja aktywów w danej organizacji powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie szacowania ryzyka.



Podział aktywów wg PN-ISO/IEC 27005

Postępowanie z ryzykiem wg PN- ISO/IEC 27005

Kontekst – uwzględnienie całego cyklu przetwarzania



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

Kontekst – uwzględnienie zabezpieczeń i kontrol

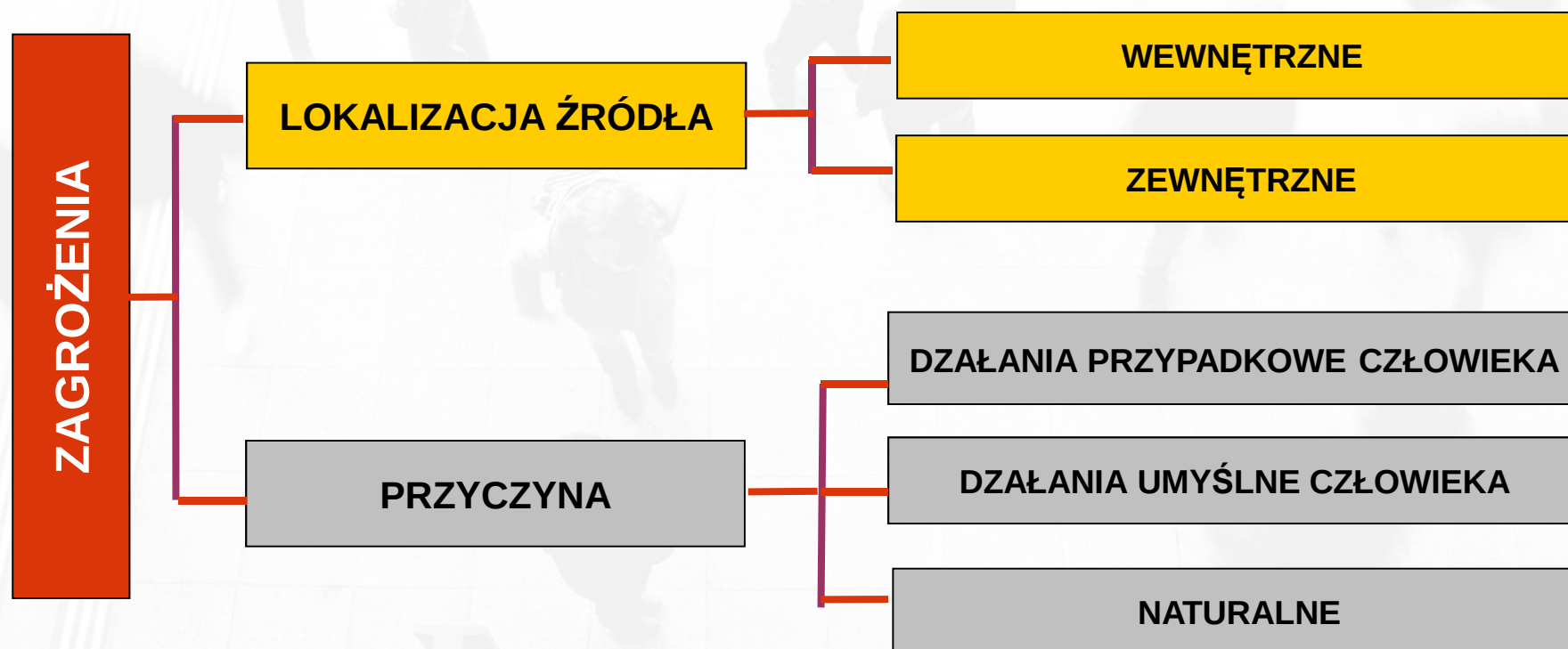
W celu określania istniejących zabezpieczeń można wykorzystać:

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

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

Identyfikacja zagrożeń

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



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

Identyfikacja podatności na urzeczywistnienie zagrożeń

Dla poszczególnych aktywów można wyróżnić wiele podatności.



Przykładowe podatności w normy PN-ISO/IEC 27005
Postępowanie z ryzykiem wg PN-ISO/IEC 27005

Ocena skutku dla poszczególnych zagrożeń

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

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

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

Ocena skutku dla poszczególnych kategorii (atrybutów bezpieczeństwa)

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

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

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

Ocena skutku dla poszczególnych kategorii (atrybutów bezpieczeństwa)

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

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

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

Wyliczanie poziomu ryzyka

Poziom ryzyka można wyliczyć według następującego wzoru:



R_p – pierwotny poziom ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,

Gdzie: ***P* ∈ {0,1,2,3,4}**

S_d – wartość przypisana skutkowi dla dostępności informacji,

S_i – wartość przypisana skutkowi dla integralności informacji,

S_p – wartość przypisana skutkowi dla poufności informacji,

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

0 – zdarzenie nie powoduje skutku (brak podatności),

1 – zdarzenie wywołuje niewielki skutek,

2 – zdarzenie wywołuje znaczący skutek,

3 – zdarzenie wywołuje bardzo znaczący skutek,

4 – zdarzenie wywołuje skutek katastrofalny.

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

Przykład

Grupa aktywów	Rodzaj aktywu	Zagrożenie	Podatność	Prawdopodobieństwo	Skutek	Wartość ryzyka	Poziom ryzyka
Systemy, programy, aplikacje	Poczta MS Exchange 2016	Utrata poufności	Słabość protokołu. Brak szyfrowania, brak cert. ID.	3	Sp = 3 Si = 2 Sd = 2	3x7 = 21	Ryzyko średnie
Systemy, programy, aplikacje	Windows Xp	Utrata poufności, Integralności, dostępności	Brak odporności na zagrożenia, Brak aktualizacji	4	Sp = 3 Si = 3 Sd = 3	4x9 = 36	Ryzyko wysokie
Systemy, programy, aplikacje	System obiegu dokumentów	Utrata dostępności, Nieuprawniony dostęp	Błąd konfiguracji. Złe uprawnienia.	2	Sp = 1 Si = 2 Sd = 2	2x5 = 10	Ryzyko niskie

Maks. wartość ryzyka = $4 \times (4 + 4 + 4) = 48$

Reguła Pereta 20%

$R < 9,6$ R. znikome

$9,7 < R < 19,2$ – niskie

$19,3 < R < 28,8$ – średnie

$28,9 < R < 38,8$ – **wysokie**

$38,9 < R < 48$ – **b. wysokie**

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

Uwzględnienie oceny skutków. Jak zrealizować?

Wskazówki dotyczące
oceny skutków dla
ochrony danych – motyw
75 RODO

**Ryzyko naruszenia
praw lub wolności.
Dotyczy sytuacji gdy:**

Przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą

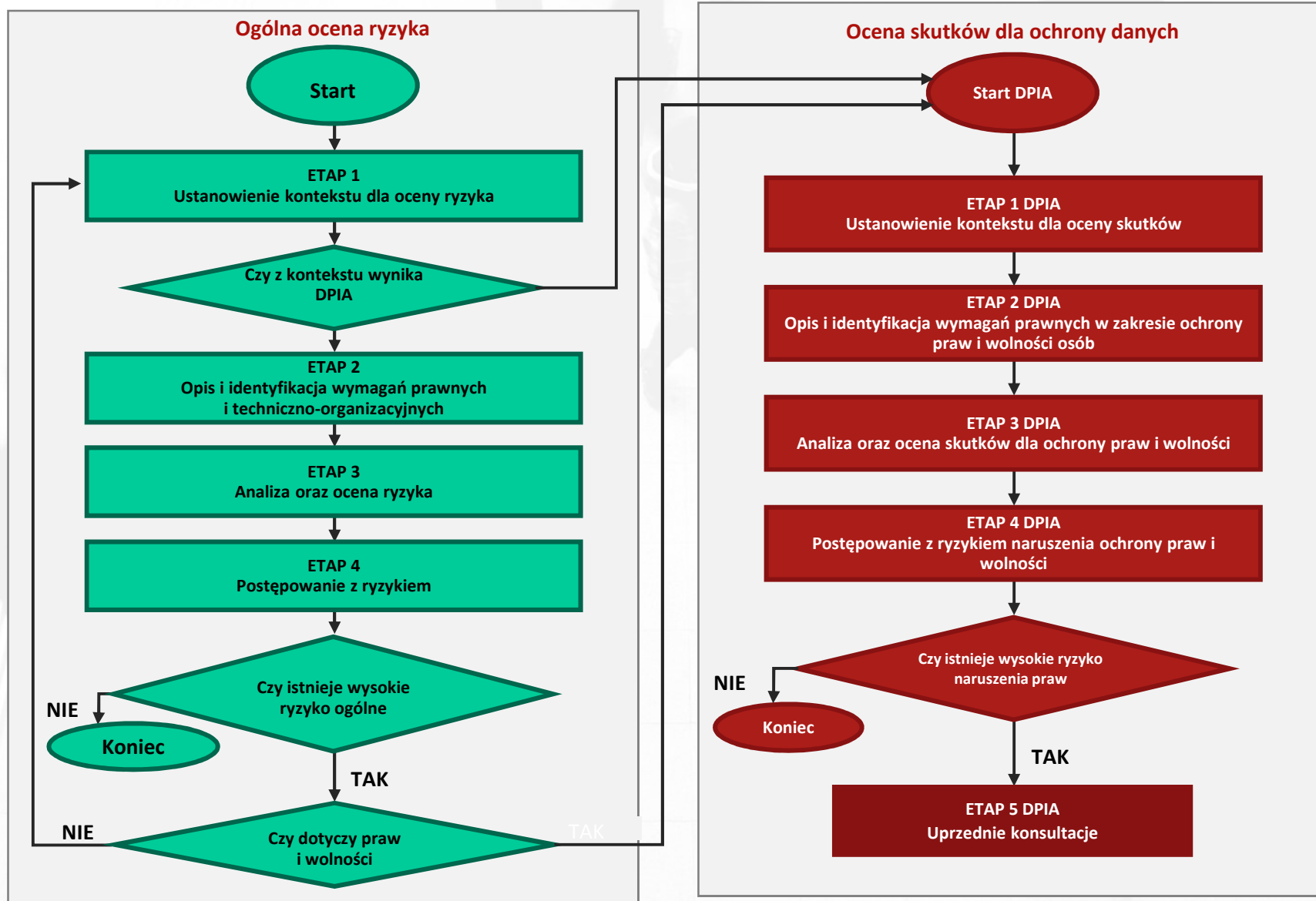
Osoby mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;

Przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia, seksualności lub wyroków skazujących

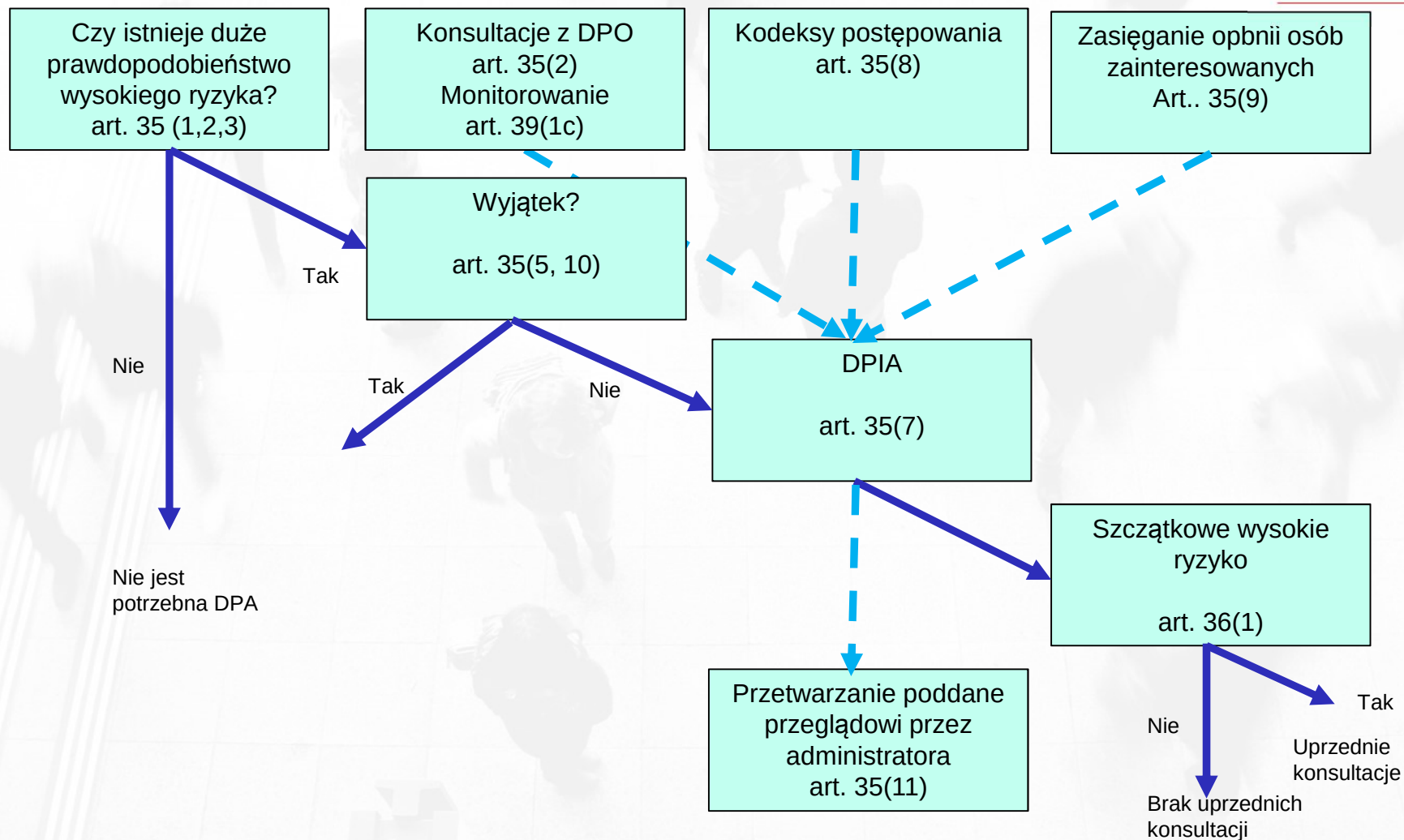
Oeniane są czynniki osobowe, np dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;

Przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Uwzględnienie oceny skutków. Jak zrealizować?



Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29



Uwzględnienie wskazówek zawartych w opinii Grupy Roboczej Art. 29



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

- 1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na **zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej;**
- 2) **przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 10)**