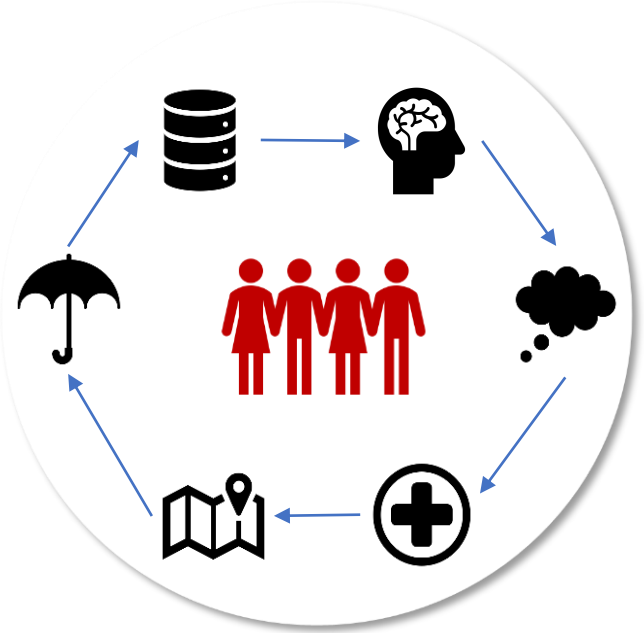
LexDigital

Metodyka przeprowadzenia oceny skutków dla ochrony danych w ujęciu praktycznym



Mariola Więckowska
Dyrektor ds. Innowacyjnych Technologii Ochrony Danych

UODO: Szkolenie dla Inspektorów Ochrony Danych
Warszawa, 19.12.2018

Agenda

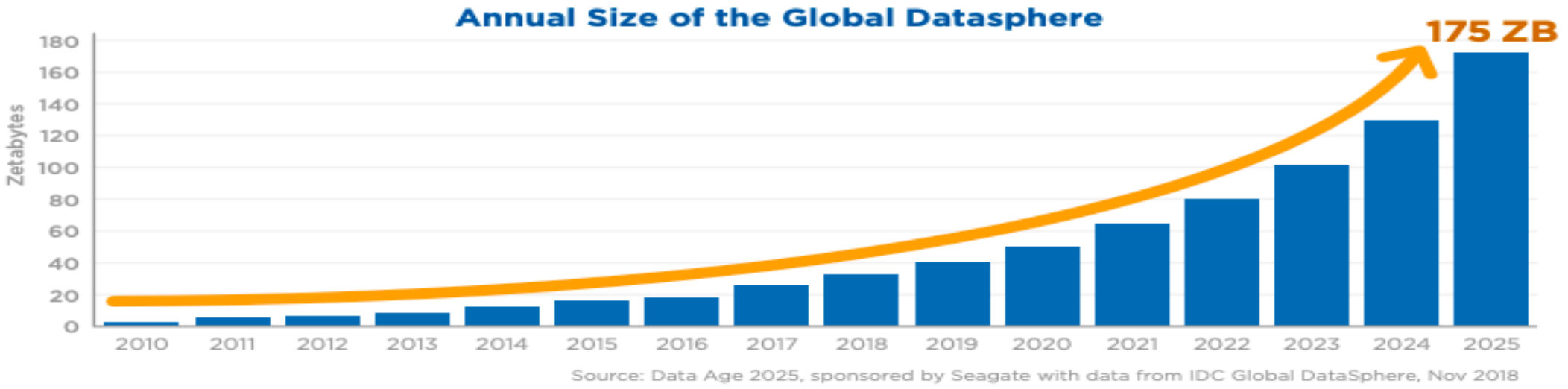
- Ryzyko ochrony danych vs. cyber-zagrożenia
- **O**cena **S**kutków dla **O**chrony **D**anych (OSOD) podstawy prawne i dostosowanie procesu do wymogów organizacji
- Analiza ryzyka jako podstawowe narzędzie w OSOD, czyli od czego warto zacząć oraz jakie elementy należy wziąć pod uwagę
- Dokumentowanie OSOD w celu wykazania obowiązków wynikających z RODO, w tym stosowania zasady ochrony danych w fazie projektowania i domyślnej ochrony danych oraz podejścia opartego na ryzyku
- Jak w praktyce prowadzić dokumentację oraz monitorować ustalenia OSOD?

O co tyle hałasu?

International Data Corporation

- **2017 = 23** Zettabytes (1 ZB = 931 322 574 615,48 GB)
- **2018 = 33** Zettabytes
- **2025 = 175** Zettabytes

Mniej niż 0,5% danych jest używana do podejmowania decyzji



LexDigital

Cyber-zagrożenia w Polsce

44% organizacji poniosło straty finansowe na skutek ataków

62% organizacji odnotowało zakłócenia i przestoje funkcjonowania

21% organizacji padło ofiarą zaszyfrowania dysku (ransomware)

46% **organizacji nie posiada operacyjnych procedur reakcji na incydenty**

Źródło: PWC - 5. edycja Badania Stanu Bezpieczeństwa Informacji

LexDigital

Naruszenia w organizacji

Aż **65%** uczestników badania zadeklarowało, że w ich organizacjach w ciągu ostatnich 12 miesięcy wykryto incydenty związane z naruszeniem bezpieczeństwa informacji lub systemów IT.

85% konsumentów twierdzi, że nie zamierza współpracować z organizacją, która nie będzie w stanie przekonać ich, że powierzone jej dane są odpowiednio zabezpieczone

Najbliższe otoczenie dalej najbardziej niebezpieczne

33% organizacji wskazało, iż głównym źródłem incydentów byli obecnie zatrudnieni pracownicy

Źródło: PWC - 5. edycja Badania Stanu Bezpieczeństwa Informacji

LexDigital

Statystyki 2017: naruszenia danych (wg Breach Level Index by Gemalto)

Co sekundę

- 122 rekordów danych ulega wyciekowi na świecie (nie wliczając danych z wycieku w Equifax)

Co minutę

- Ponad 7000 rekordów danych jest kradzione lub utracone na świecie, co daje więcej niż 10 milionów każdego dnia.

W pierwszej połowie 2017

- 1,9 miliarda rekordów danych wyciekło w wyniku naruszeń. To drastyczny wzrost o 164% w porównaniu z drugą połową 2016.

LexDigital

Statystyki 2018: naruszenia danych (wg Breach Level Index by Gemalto)

Co sekundę

- 291 rekordów danych ulega wyciekowi na świecie

Co minutę

- Ponad 17 000 rekordów danych jest kradzione lub utracone na świecie, co daje więcej niż 25 milionów każdego dnia.

W pierwszej połowie 2018

- 4,5 miliarda rekordów danych wyciekło w wyniku naruszeń. To wzrost o 133% w porównaniu z drugą połową 2017.

LexDigital

Art. 24 Obowiązki administratora

1. Uwzględniając **charakter, zakres, kontekst i cele** przetwarzania oraz **ryzyko naruszenia praw lub wolności** osób fizycznych o rożnym 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 przeglądom 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 postepowania**, o których mowa w art. 40, lub **zatwierdzonego mechanizmu certyfikacji**, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

LexDigital

Zasada rozliczalności

- Art.5 RODO wprowadza **zasadę rozliczalności**, zgodnie z którą Administrator będzie musiał wykazać przestrzeganie wypełniania rozporządzenia.
- I chociaż jednym z celów reformy ochrony danych osobowych w UE jest ograniczenie obciążeń biurokratycznych poprzez **wprowadzenie podejścia opartego na ryzyku** (tzw. „risk-based approach”), to wdrożenie zasad, które pozwolą na wykazanie stosowania przez firmę złożonych przepisów **nie jest łatwe.**

LexDigital

Stosowanie zasady rozliczalności

Prawne

- Umowy powierzenie/udostępnienie/współ administrowania
- Polityki / Procedury
- Zgody / Klauzule informacyjne
- Regulaminy / Polityki prywatności (transparentność)
- Śledzenie zmian w prawie, kodeksy postępowania ...

Organizacyjne

- Szkolenia/upoważnienia
- **Ocena skutków dla ochrony danych – stosowanie PbD**
- **Podejście oparte na ryzyku - przetwarzania i prywatności**
- Zarządzanie incydentami
- Środki ochrony fizycznej

Techniczne

- Dostosowanie systemów do wypełniania praw podmiotów danych
- Ochrona systemów, aplikacji i baz danych
- Środki sprzętowe oraz infrastruktura
- Stosowanie adekwatnych zabezpieczeń (Privacy by Design)
- Rejestrowanie czynności przetwarzania - dane klientów i pracowników -(nie)strukturalne

LexDigital

Artykuł 35: Ocena Skutków dla Ochrony Danych - OSOD

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem **nowych technologi**i – ze względu na swój **charakter, zakres, kontekst i cele** z dużym prawdopodobieństwem może powodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych (…) to przeprowadza się OSOD (...), w szczególności w przypadku:

- 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 osoby fizyczne;
- 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, o czym mowa w art. 10;
- **systematycznego monitorowania** na dużą skalę miejsc dostępnych publicznie.

LexDigital

OSOD: Motyw 84

Aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z **wysokim ryzykiem** naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania **oceny skutków dla ochrony danych** w celu oszacowania w szczególności **źródła, charakteru, specyfiki i powagi tego ryzyka**. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

LexDigital

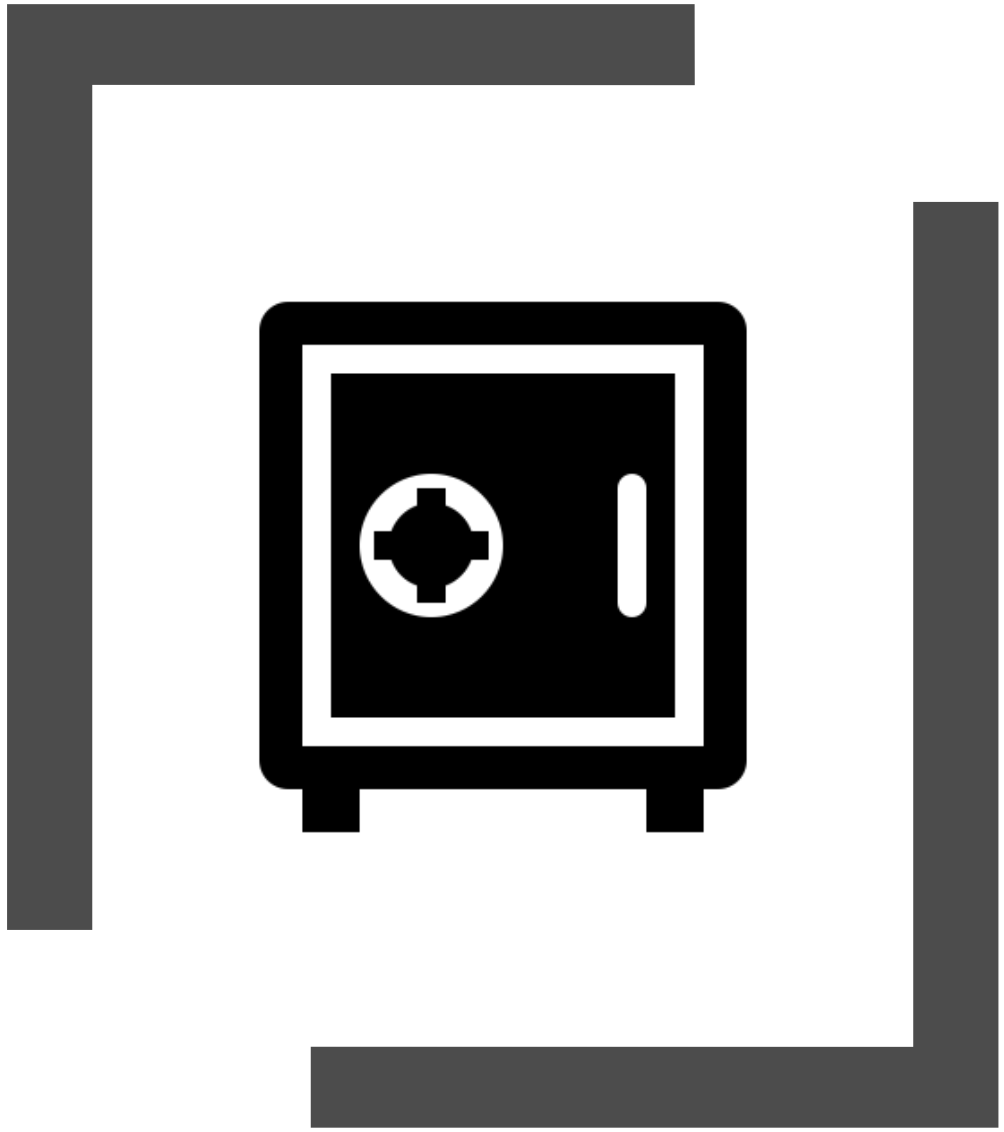
OSOD: Motyw 89

[…] obecnie obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je **skutecznymi procedurami i mechanizmami** koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój **charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**. Takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem **nowych technologii lub które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych** lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.

Artykuł 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

- Uwzględniając stan **wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele** przetwarzania oraz **ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża **odpowiednie środki techniczne i organizacyjne**, takie jak **pseudonimizacja**, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak **minimalizacja danych**, oraz w celu nadania przetwarzaniu **niezbędnych zabezpieczeń**, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.
- Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są **niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania**. Obowiązek ten odnosi się do **ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności**. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
- Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego **mechanizmu certyfikacji określonego w art. 42.**

LexDigital



PbD: Motyw 78

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich **środków technicznych i organizacyjnych**, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć **wewnętrzne polityki i wdrożyć środki**, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w **fazie projektowania oraz z zasadą domyślnej ochrony danych**. Takie środki mogą polegać m.in.

- na minimalizacji przetwarzania danych osobowych,
- jak najszybszej pseudonimizacji danych osobowych,
- przejrzystości co do funkcji i przetwarzania danych osobowych,
- umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych,
- umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

LexDigital

PbD: Motyw 78 c.d.

Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i **z należytym uwzględnieniem stanu wiedzy technicznej** zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych. **Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.**

LexDigital

Jak wdrożyć OSOD?

Podstawą jest budowanie świadomości osób, które uczestniczą w przetwarzaniu danych

OSOD to narzędzie, które odpowiednio wbudowane w kulturę organizacyjną zapewni wysoką ochronę danych i pozwoli na ich bezpieczne przetwarzanie, m.in. poprzez podjęcie kluczowych decyzji już w **fazie projektowania (privacy by design), domyślną ochronę danych (privacy by default**) oraz wczesne zaadresowanie i minimalizację potencjalnych **ryzyk prywatności**.

LexDigital

1

Etap 1: Wstępna ocena skutków dla ochrony danych –

ogólna ocena ryzyka

2

Etap 2: Ocena skutków dla ochrony danych -

ocena ryzyka prywatności i rekomendowane środki zaradcze

3

Etap 3: Przygotowanie raportu końcowego

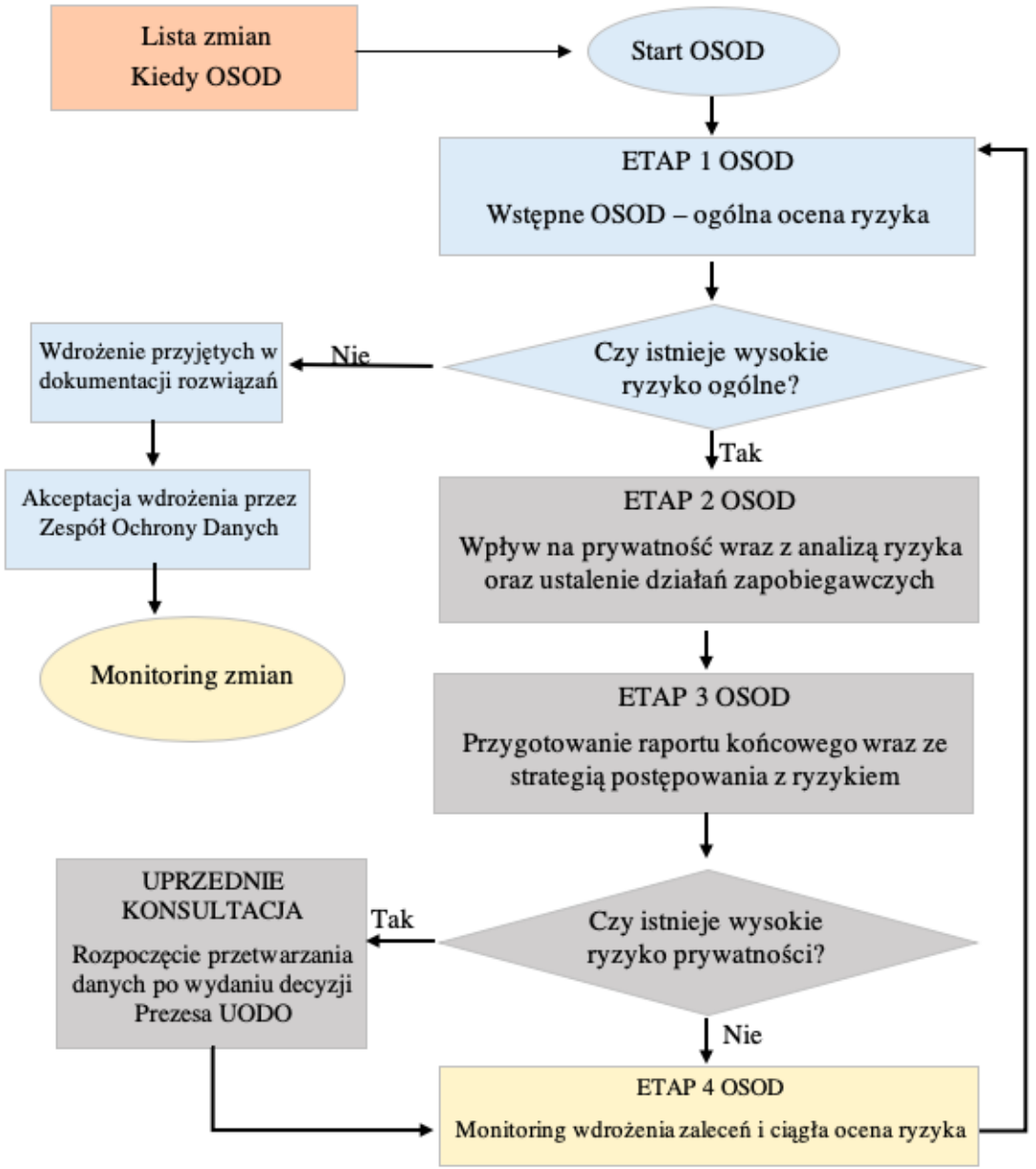
4

Etap 4: Monitoring wdrożenia

Etapy OSOD

LexDigital

Schemat OSOD



LexDigital

Ocena skutków dla ochrony danych

UWAGA: OSOD należy wypełnić w fazie projektowania zmiany/projektu.

- Powierzenia przetwarzania danych innym podmiotom
- Nowy system informatyczny/monitoringu
- Powstanie nowej bazy danych/mikro usługi
- Przekazanie danych do hurtowi danych lub innych wewnętrznych systemów
- Zastosowanie nowej technologii
- Przetwarzanie istniejących danych w nowym celu lub gdy dochodzi do profilowania podmiotu danych
- Udostępnienie danych/API innym podmiotom

LexDigital

UODO: wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

1. **Ewaluacja lub ocena, w tym profilowanie i przewidywanie** (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych
2. **Zautomatyzowane podejmowanie decyzji** wywołujących skutki prawne, finansowe lub podobne istotne skutki
3. **Systematyczne monitorowanie na dużą** skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni.
   Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa
4. **Przetwarzanie szczególnych kategorii** danych osobowych i dotyczących wyroków skazujących i czynów zabronionych

LexDigital

Wykazu rodzajów operacji przetwarzania c.d.

5. **Dane przetwarzane na dużą skalę**, gdzie pojęcie dużej skali dotyczyć liczby osób, których dane są przetwarzane w kontekście
   - zakresu przetwarzania,
   - okresu przechowywania danych oraz
   - geograficznego zakresu przetwarzania
6. **Przeprowadzanie porównań, ocena lub wnioskowanie** na podstawie analizy danych pozyskanych z różnych źródeł
7. Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są **uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi**
8. **Innowacyjne wykorzystanie lub zastosowanie** rozwiązań technologicznych lub organizacyjnych
9. Gdy przetwarzanie samo w sobie **uniemożliwia** osobom, których dane dotyczą, **wykonywanie prawa lub korzystanie z usługi lub umowy**

Etap 1: Wstępna ocena skutków dla ochrony danych – ogólna ocena ryzyka

Cel

- Ustalenie, czy w projekcie będzie dochodziło do przetwarzania danych osobowych oraz czy projekt będzie stwarzał z dużym prawdopodobieństwem **wysokie ryzyko** naruszenia praw lub wolności osób.
- Jeżeli ryzyko jest wysokie, to wtedy jest wymagane przeprowadzenie **dalszych etapów OSOD.**

LexDigital

Co należy rozważyć?

- Dlaczego wprowadzamy zmianę? (np. polepszenie usługi, zwiększenie wydajności, poprawa ochrony prywatności)
- Jaka jest podstawa prawna zmiany? (np. wymóg wynikający z przepisów prawa)
- Obecny i przewidywany zakres przetwarzanych danych wraz z ich celem i charakterem
- Kategorie przetwarzanych danych: ogólnie dostępne, zwykłe, szczególne
- Skutki łączenia informacji z innymi danymi
- Nośniki danych, np. papier, dane elektroniczne i ich rodzaj
- Użycie nowych technologii

LexDigital

Kontekst i wszystkie aspekty zmiany

Media, w których są zapisane dane, np. papier, wersje elektroniczne, w tym e-mail, wideo, nagrywane rozmowy telefoniczne, logi komputerowe
Łączenie pierwotnych informacji z innymi systemami/danymi. Połączone informacje mogą potencjalnie zwiększyć ryzyko zidentyfikowania osoby, nawet jeśli sama informacja nie jest uważana za dane osobowe
Czy dane osobowe będą udostępniane innym systemom informatycznym, instytucjom lub organizacjom działających na rzecz projektu
Czy strona trzecia, czyli spoza systemu lub organizacji będzie mogła zbierać, ujawniać, przechowywać, zabezpieczać lub zbywać dane osobowe
Czy projekt będzie obejmować dane osobowe, które są dostępne dla ogółu społeczeństwa, czy dane zwykłe, czy dane szczególne – jest to istotne dla ustalenia, czy należy kontynuować proces OSOD
Wpływ innych przepisów prawnych lub polityki prywatności, które muszą być przestrzegane

LexDigital

informacja chroniona

WOSOD: Wstępna Ocena Skutków dla Ochrony Danych - ogólna analiza ryzyka

Informacje o procesie przetwarzania oraz dane ADO	
Administrator	
Właściciel procesu	
Opiekun procesu	
Czynność przetwarzania/proces (numer procesu zgodnie z ankietą procesu)	Przykład: Rekrutacja

Cel procesu (po co go wykonujemy - np. pozyskanie nowych klientów, polepszenie usługi, poprawa ochrony prywatności)
Zakres przetwarzanych danych: Podaj kategorie danych osobowych, które będą przetwarzane w zmianie:
Opis: np. Dane podane podczas rejestracji konta (imię, nazwisko, adres do korespondencji, adres e-mail) oraz dane wytworzone podczas przetwarzania danych podczas korzystania z usługi/serwisu zgodnie z umową (IP, cookies).

Jaki jest kontekst przetwarzania danych? (zaznacz właściwe). Prosimy o wybranie jednego kontekstu wiodącego dla danego procesu. Jeżeli uważasz, że dane w procesie przetwarzane są w kilku kontekstach również je zaznacz		**Komentarz, uwagi, wątpliwości**
Administracyjny - wiązany m.in z czynnościami biurowymi dotyczącymi prowadzenia list obecności, zamówień sprzętu, przygotowywania wzorów umów, zakupów.	Tak	
Finansowy - związany m.in. ze sprawozdawczością finansową, procesami księgowymi, ofertowaniem, wyborem dostawców.	N/D	
Lokalny - związany ze środowiskiem wewnętrznym organizacji np. umieszczanie danych osobowych na tablicach informacyjnych.	N/D	
Pracowniczy - związany z czynnościami dotyczącymi m.in. rekrutacji, urlopów, zwolnień, szkoleń.	N/D	
Publiczny - związany z działalnością przetwarzania danych w sektorze publicznym.	N/D	
Reputacyjny - związany z działalnością odbywającą się na zewnątrz organizacji m.in udostępnianie danych osobowych na stronie www., prowadzenie profili na portalach społecznościowych.	N/D	
Wypełnianie umowy - związany z realizacją postanowień umowy np. z dostawcą.	N/D	
Zapewnienia bezpieczeństwa - związany z zastosowaniem środków służących zapewnieniu ochrony danych. np. zastosowanie środkow związanych z dostępem do pomieszczeń, ochrona przeciwpożarowa.	Tak	
Inny (podaj jaki)		

Jakie nośniki danych stosowane są w procesie?		Komentarz
papier	Tak	
nośniki elektroniczne	N/D	
Przechowywanie zgód		
udzielonych w formie pisemnej	Tak	
udzielonych w formie elektronicznej	N/D	
udzielonych w formie ustnej	N/D	
Typy danych		
Dane osobowe	Tak	
Dane szczególne	N/D	
Dane restrykcyjne, np. numer Pesel, skan DO, numer karty kredytowej	Tak	Skan DO
Charakter przetwarzanych danych		
Ciągły	Tak	
Sporadyczny	Nie	

Środki bezpieczeństwa

Jakie środki bezpieczeństwa są używane w obszarze przetwarzania danych osobowych?		Komentarze
Organizacyjne środki ochrony danych:		
Czy osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych?	Tak	
Czy przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego (budowanie świadomości konieczności regularnej zmiany haseł, zapewnieie bezpieczeństwa używania sprzętu poza obszarem przetwarzania)?	Nie	
Fizyczne środki ochrony danych:		
Czy wydzielono obszary bezpieczne, w tym dla miejsc gdzie przetwarzane są dane osobowe?		
Czy obszary zabezpieczono przed nieuprawnionym dostępem - stworzenie systemu kontroli dostępu zgodnie z ewidencją, np. poprzez karty magnetyczne?		

Rodzaje operacji przetwarzania danych	
Czy w procesie prowadzona będzie ewaluacja lub ocena, w tym profilowanie i przewidywanie w celach, które mogą wywołać negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych? (Np.tworzenie profili zachowań lub profili marketingowych, dopasowywanie reklamy produktu do danego użytkownika na podstawie analizy jego wcześniejszej internetowej aktywności).	Tak
Opis:	
Czy proces zakłada zautomatyzowane podejmowanie decyzji o skutku prawnym, finansowym lub podobnie znaczącym skutku? (Automatyczne podejmowanie decyzji to podejmowanie decyzji wobec konkretnej osoby tylko i wyłącznie przez system informatyczny (wynik działania określonego algorytmu) na podstawie uwzględnienia wybranych kryteriów. Podejmowanie decyzji w formie zautomatyzowanej dokonywane jest bez ingerencji człowieka np. przetwarzania mogące prowadzić do automatycznej blokady konta, usunięcia oferty, usunięcia danych, nieudzielenia kredytu, systemy profilowania klientów pod kątem zidentyfikowania preferencji zakupowych, ustalanie cen promocyjnych w oparciu o profil).	Nie

Weryfikacja wypełniania praw podmiotów danych zgodnie z RODO.

Należy zadbać w organizacji, aby dla każdego z praw wybrać odpowiednie rozwiązania techniczne i organizacyjne, które zgodnie z zasadą rozliczalności po analizie ryzyka zostaną udokumentowane i pozwolą na wykazanie wypełniania praw i wolności podmiotów danych.

Ważne staje się stosowanie zasady ochrony danych już w fazie projektowania i domyślnej ochrony danych.

Wypełniając prawa należy zapewnić weryfikację tożsamości podmiotu. Wykonanie niektórych praw może ze względów bezpieczeństwa wymagać dodatkowej weryfikacji podmiotu danych.

Nazwa procesu

Czy są wypełniane prawa podmiotów danych, zaznacz odpowiednie	Decyzja	Komentarze
Czy wypełniane jest prawo do informacji o (art. 13 i 14)? Prawo zostało rozszerzone o nowe kategorie informacji, które należy podawać podmiotowi danych w sposób przejrzysty, przy użyciu prostego i zwięzłego języka. Wymagane informacje są umieszczane w klauzulach informacyjnych, polityce prywatności, czy regulaminie. Spełnienie obowiązku informacyjnego wykonuje się podczas przekazywania danych do przetwarzania. Czy klauzule informacyjne i polityka prywatności zostały dostosowane do nowego zakresu informacji wymaganych przez rodo (pamiętaj o przejrzystej formie informacji).	Tak	
W jaki sposób prawo jest realizowane/dlaczego nie jest realizowane:		
Czy wypełniane jest prawo dostępu do danych osobowych oraz otrzymania kopii danych (art.15)? Podmioty danych mają prawo do uzyskania dostępu lub potwierdzenia, jakie ich dane są przetwarzane przez administratora. Zadbaj o poufność i bezpieczeństwo podczas dostarczania wymaganych informacji. Czy został wdrożony odpowiedni proces w organizacji na wypełnianie tego prawa? **Ważne: Nie jest wymagne przekazywanie kopii danych pretwarzanych w wersji papierowej.**	Nie	
W jaki sposób prawo jest realizowane/dlaczego nie jest realizowane:		

Przykład: Rekrutacja

Opis:

Decyzja dotycząca ryzyka	Decyzja
	Wysokie Ryzyko

	Tak	Nie	Wartość Sugerowana
Rodzaje operacji przetwarzania (lista UODO)	3	3	Wysokie Ryzyko
Prawa podmiotów	6	3	Wysokie Ryzyko
Ryzyko z RCP	0	1	Ryzyko
Typ danych	10	0	Wysokie Ryzyko

Data Wypełnienia

LexDigital

Etap 2: co rozważyć i udokumentować?

- Opis planowanych operacji i celów przetwarzania, w tym:
  - realizowanych przez administratora interesów prawnych;
  - jak, kto i z jakimi uprawnieniami będzie je przetwarzał;
  - jaka technologia będzie stosowana.
- W jaki sposób i kiedy dane osobowe będą mogły być przetwarzane poza organizacją, szczególnie czy w państwach trzecich.
- Przepływ danych osobowych przez istniejące i przyszłe systemy lub procesy biznesowe.
- Zidentyfikowanie zagrożeń prywatności i skutków odnoszących się do wszystkich aspektów projektu, w tym powiązań procesów biznesowych i użytych technologii.
- Istniejące środki ochrony prywatności dla planowanych działań, które mogą mieć zastosowanie do poszczególnych zagrożeń.

LexDigital

Identyfikacja zagrożeń i ich potencjalnych skutków dla prywatności

- Brak podstawy prawnej do zbierania, wykorzystywania lub ujawniania danych osobowych
- Przetwarzanie niekompletnych lub nieaktualnych danych
- Nieuzasadnione użycie lub ujawnienie danych, np. gdy spseudonimizowane lub anonimowe dane są wystarczające, aby osiągnąć cel
- Zbyt szeroki zakres przetwarzanych danych
- Przetwarzanie danych niezgodnie z pierwotnym celem
- Przetwarzanie danych po wygaśnięciu celu ich przetwarzania
- Ujawnienie danych nieuprawnionym podmiotom

LexDigital

Ryzyko w RODO

Ryzyko wiążące się z przetwarzaniem danych

- rodzące skutki finansowe, prawne i utraty reputacji w wyniku naruszenia prywatności;
- przypadkowe lub niezgodnego z prawem zniszczenie, utrata, modyfikacja, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Ryzyko naruszenia praw lub wolności osób, w tym

- braku wypełniania praw osób, możliwości kradzieży tożsamości, naruszenia dobrego imienia, dyskryminacji lub negatywnych skutków finansowych, pozbawienie przysługujących podmiotom danych ich praw.

LexDigital

Ocena ryzyka przetwarzania

- **Ryzyko przetwarzania danych określa miarę stopnia zagrożenia dla poufności, integralności i dostępności informacji, wyrażoną jako prawdopodobieństwa wystąpienia zagrożenie i szkodliwości jej skutków.**

- Art. 32 ust. 2 rodo
- (…) ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

LexDigital

Przykład atrybutów ryzyka przetwarzania

Kontrola zarządcza	• Brak kontroli zarządczej w obszarze ochrony danych osobowych. Niespełnianie wymagań zasad przetwarzania danych osobowych, w tym zasady bezpieczeństwa danych i wdrożenia procedur wymaganych przez RODO.
Legalność	• Brak spełnienia wymogów legalności przetwarzania w tym również transferu danych do państw trzecich (USA i kraje spoza UE) oraz powierzania przetwarzania danych osobowych wynikającego z RODO.
Poufność	• Brak zapewnienia poufności danych osobowych, polegające na tym, że informacja jest dostępna lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
Integralność	• Brak zapewnienia integralności danych – zapewnienie mechanizmów kontroli zmian danych oraz ich utraty w systemach IT.
Dostępność	• Ryzyko związane z brakiem zapewnienia odpowiedniego poziomu dostępności do danych, m.in. opracowania i testowania BCP.
Bezpieczeństwo	• Brak adekwatnego poziomu stosowanych zabezpieczeń w zakresie ochrony danych osobowych, w tym zapewnienie środków technicznych i organizowanych wynikających z polityki ochrony danych oraz wewnętrznych procedur.

LexDigital

Ocena ryzyka prywatności

- Podstawą oceny ryzyka prywatności jest zrozumienie **prawdopodobieństwa naruszenia praw i wolności osób, których dane dotyczą i wiążących się z tym potencjalnych skutków**. Ocena jest niezbędna do identyfikacji środków zaradczych i działań, i do wydania rekomendacji, co do sposobu realizacji projektu, które zminimalizują ryzyko prywatności i wzmocnią potencjalne korzyści z lepszej ochrony danych.

- Motyw 71: (…) zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiegający m.in**. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną** lub skutkujący środkami mającymi taki efekt.

LexDigital

Ocena ryzyka prywatności – motyw 75

- Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do **uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych**, w szczególności:
  - jeżeli przetwarzanie może poskutkować **dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną**;
  - jeżeli osoby, których dane dotyczą, mogą **zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi**;

LexDigital

Ocena ryzyka prywatności – motyw 75 cd.

- jeżeli przetwarzane są dane osobowe ujawniające **pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych** oraz
- jeżeli przetwarzane są **dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa** lub związanych z tym środków bezpieczeństwa;
- jeżeli oceniane są **czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania** się – w celu tworzenia lub wykorzystywania **profili osobistych**;
- lub jeżeli przetwarzane są dane **osobowe osób wymagających szczególnej opieki, w szczególności dzieci**;
- jeżeli przetwarzanie dotyczy **dużej ilości danych osobowych** i wpływa na dużą liczbę osób, których dane dotyczą.

LexDigital

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub zarządzania nimi

- **Obszar 1: Rzetelność, przejrzystość i legalność przetwarzania** (art. 5 ust 1. lit. a, art. 6 i 9) - ryzyko związane z podstawą prawną.

Ustal podstawę przetwarzania. Opisz sposób i podstawę zbierania danych i oceń, czy dane są przetwarzane zgodnie z prawem. Opis planowanych operacji przetwarzania i celów przetwarzania, w tym usprawiedliwionych interesów administratora;

- **Obszar 2: Proporcjonalność i minimalizacja przetwarzanych danych do celu** (art. 5) - ryzyko związane z zakresem przetwarzania danych.

Zbieraj tylko dane osobowe adekwatne do celu, minimalizuj zakres danych. Jaki jest cel gromadzenia danych osobowych? Zidentyfikuj każdą kategorię danych i upewnij się, że jest to konieczne dla celu. Jak to wpłynie na projekt i organizację? Czy zbierasz jedynie to, czego naprawdę potrzebujesz? Na przykład, czy potrzebujesz "datę urodzenia", czy "wiek" lub może "powyżej 18 lat" wystarczy?

- **Obszar 3: Transparentne wypełnianie obowiązku informacyjnego** (art. 13 i 14) - ryzyko związane z transparentnym informowaniem w zależności od źródła.

Podaj w trakcie zbierania danych transparentnie informacje wymagane przez rodo art. 13 albo 14. Jak będziesz przekazywał konieczne informacje? Jak zapewnisz transparentność? Co umieścisz w klauzuli informacyjnej, a co w polityce ochrony prywatności. Jeśli dane osobowe są zbierane z innego źródła, czy spełnione są wymogi prawne?

- **Obszar 4: Poprawność danych osobowych** (art. 5 ust. 1 lit. d) - ryzyko związane z poprawnością danych osobowych i krokami podejmowanymi w celu ich weryfikacji.

Upewnij się, że dane osobowe są poprawne i aktualne przed ich użyciem, ustal jakie kroki są podejmowane w celu ich weryfikacji. Rozsądne działania będą się różnić w zależności od kategorii danych. Istotne czynniki obejmują, np. jak proces ma sprawdzić, czy te informacje są poprawne? Czy informacje zostały dostarczone przez podmiot bezpośrednio, czy pozyskane z innego wiarygodnego źródła? Czy zostały sprawdzone z osobą bezpośrednio?

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub zarządzania nimi cd.

- **Obszar 5: Ograniczenie przechowywania danych** (art. 5 ust. 1 lit. e) - ryzyko związane z usuwaniem danych po wygaśnięciu celów i podstawy prawnej oraz zasadami przetwarzania do innych celów, np. archiwalnych po zastosowaniu odpowiednich środków bezpieczeństwa.

Usuwaj dane, gdy wszystkie cele i podstawy prawne wygasną. Opcjonalnie, ustal zasady przetwarzania do innych celów, np. archiwalnych po zastosowaniu odpowiednich środków bezpieczeństwa, np. szyfrowanie danych, pseudonimizacja. Jak długo zamierzasz przechowywać dane? Z jakiego prawa wynika obowiązek przechowywania danych? Jeżeli takie obowiązki nie istnieją, co uznać za rozsądny okres przechowywania danych? Jak dane zostaną usunięte? Jeśli informacje są udostępniane podmiotom trzecim, rozważ, jak długo będą one przetwarzane i jakie kroki trzeba przedsięwziąć, aby zapewnić usunięcie danych po zakończeniu celu przetwarzania.

- **Obszar 6: Integralność, poufność, dostępność danych oraz zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych** (art.5 ust. 1 lit. f oraz art. 32) - ryzyko związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa chroniącym przed utratą, nieupoważnionym dostępem, modyfikacją lub ujawnieniem oraz innymi nieuprawnionymi działaniami.

Mogą istnieć różne metody ochrony dany osobowe w celu ich ustalenia skorzystaj z kodeksów postępowania. Dobierz odpowiednie środki organizacyjne i techniczne.

Zabezpieczenia mogą obejmować: bezpieczeństwo fizyczne; bezpieczeństwo IT; szkolenie personelu; polityki, które muszą przestrzegać pracownicy; umowy powierzenia i klauzule poufności w umowach z dostawcami zewnętrznymi itp.

Zastanów się, czy w całej ścieżce przetwarzania danych nie występują luki w zabezpieczeniach - zidentyfikuj słabe punkty.

- **Obszar 7: Dostęp do danych osobowych** (art. 15) - ryzyko związane z zapewnieniem podmiotom dostępu do ich danych

Zapewnij podmiotom danych dostęp do kopii danych i wymaganych informacji. Opisz, jakie działania są podejmowane, aby umożliwić osobie uzyskiwanie dostępu do informacji i jej danych. Czy system zapewni udostępnianie podmiotom kopii przetwarzanych danych?

- **Obszar 8: Ujawnienie i przekazywanie danych osobowych** (art. 6 i 9) - ryzyko związane z ujawnianiem i przekazywaniem danych w przypadku braku uzasadnionej podstawy prawnej

Ujawnij dane tylko, jeśli masz uzasadnioną podstawę prawną. Ustal jasne zasady dotyczące ujawniania danych. Identyfikuj wszystkich, którym je przekazujesz. Jak poinformujesz podmiot o tym komu dane zostają ujawnione? Czy istnieje w systemie mechanizm pozwalający na rejestrację ujawnienia?

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub zarządzania nimi cd.

- **Obszar 9: Sprostowanie danych osobowych** (art. 16) - ryzyko związane z zapewnieniem podmiotom możliwości poprawiania swoich danych

Umożliwiaj podmiotom poprawianie swoich danych, jeśli są niepoprawne lub błędne. Rozważ, w jaki sposób organizacja zapewni prawo do sprostowania danych – czy osoba sama może zmienić dane, czy poprzez złożenie wniosku o aktualizację. Czy istnieją jakieś ograniczenia, które nie pozwalają za zmianę danych?

- **Obszar 10: Prawo do usunięcia - bycia zapomnianym** (art. 17) - ryzyko związane z zapewnieniem możliwości usunięcia danych na wniosek podmiotu

Zapewnij możliwość usunięcia danych na wniosek podmiotu. W jaki sposób prawo to będzie wypełniane? Czy system informatyczny spełni wymogi RODO?

- **Obszar 11: Prawo do ograniczenia przetwarzania danych** (art. 18) - ryzyko związane z oznaczeniem danych w celu ograniczenia ich przyszłego przetwarzania

Oznacz przechowywane dane w celu ograniczenia ich przyszłego przetwarzania. Zbadaj możliwości wypełniania prawa w przypadku:

  - kwestionowania prawidłowości danych,
  - gdy przetwarzanie jest niezgodne z prawem, a podmiot sprzeciwia się usunięciu danych i żąda ograniczenia przetwarzania,
  - po wygaśnięciu celu przetwarzania na prośbę osoby, której dane dotyczą
  - wniesiony jest sprzeciw zgodnie z art.21 rodo.

W jaki sposób będą weryfikowane oczekiwania podmiotu danych?

- **Obszar 12: Powiadomienie o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (art. 19)** - ryzyko związane z powiadamianiem każdego odbiorcy, któremu ujawniłeś dane o zmianie (możliwości techniczne i finansowe)

Powiadom każdego odbiorcę, któremu ujawniłeś dane w ramach możliwości technicznych i finansowych. Ustal w jaki sposób będziesz realizował ten obowiązek. Czy systemowo czy procesowo? Udokumentuj decyzję niewypełnienia tego prawa (dlaczego nie można go wypełnić lub uzasadnij niewspółmiernie duży wysiłek przy jego wypełnianiu).

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub zarządzania nimi cd.

- **Obszar 13: Zapewnienie przenoszenia danych (art. 20)** - ryzyko związane z przenoszeniem danych

Określ i przekaz podmiotom danych zasady dotyczące pobierania danych. Czy system pozwala na wypełnienie tego prawa? Jaki zakres danych przekazywać? Jak powinna wyglądać procedura bezpiecznego przekazania danych?

- **Obszar 14: Wypełnienie prawa sprzeciwu (art. 21)** - ryzyko związane ze sprzeciwem, dot. m.in. profilowania tzw. zwykłego oraz marketingu bezpośredniego

Jak zapewnić możliwość wniesienie sprzeciwu? W jaki sposób system ma zareagować? W jaki sposób poinformować podmioty danych? Jak zaimplementować opt-out?

- **Obszar 15: Podejście do zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania (art. 22)** - ryzyko związane z zautomatyzowanym podejmowaniem decyzji/profilowania i zbieraniem zgód

Zbadaj podstawę prawną i jeśli to konieczne zbieraj zgody. Dostosuj odpowiednio system. Ustal zasady postępowania w przypadku wycofania zgody. Zapewnij interwencję ludzką.

- **Obszar 16: Wykorzystanie unikalnych identyfikatorów** (art. 4 i motyw 30) - ryzyko związane z potencjałem używanych identyfikatorów do bycia danymi osobowymi, szczególnie w połączeniu z innymi danymi.

Ustal potencjał unikalnych identyfikatorów do bycia danymi osobowymi, szczególnie w połączeniu z innymi danymi. Określ, jakie unikalne identyfikatory są stosowane i ustal, dlaczego są potrzebne.

Metody szacowania ryzyka

Podczas szacowania ryzyka stosuje się najczęściej dwie metody:

• **Ilościowa** analiza ryzyka – opiera się na badaniu zdarzeń losowego. Wykorzystuje się w niej:

- plan zarządzania ryzykiem,
- lista zidentyfikowanych ryzyk,
- lista hierarchii ryzyk,
- lista ryzyk do dalszej analizy,
- dane historyczne,
- opinie ekspertów oraz rezultaty innych procesów planowania w danej realizacji.

• **Jakościowa** analiza ryzyka – opisowe miary wyrażające możliwość zajścia zdarzenia. Wykorzystuje się w niej:

- plan zarządzania ryzykiem,
- lista zidentyfikowanych ryzyk wraz z podziałem ich na kategorie,
- raport o stanie zaawansowania realizacji wytyczonych celów,
- przyjęta w firmie skala prawdopodobieństwa i mierników skutków wystąpień zagrożeń
- lista założeń które zostały przyjęte w procesie identyfikacji i oceny źródeł ryzyka.

• Najczęściej wyniki oszacowania ryzyka przybierają formę tabeli lub wykresu.

LexDigital

Poziom	Prawdopodobieństwo wystąpienia zdarzenia
5 - Bardzo Wysoki	Ryzyko wystąpi w większości okoliczności – prawie pewne zdarzenie.
4 - Wysoki	Ryzyko wystąpi prawdopodobnie w większości okoliczności. Znane są przypadki wystąpienia zdarzenia w ostatnim roku.
3 - Średni	Ryzyko wystąpi prawdopodobnie w niektórych okolicznościach. Znane są przypadki wystąpienia zdarzenia w ostatnich 3 latach.
2 - Niski	Ryzyko wystąpi z niskim prawdopodobieństwem. Brak przypadków wystąpienia zdarzenia w ostatnich 3 latach.
1 - Bardzo niski	Ryzyko praktycznie nie występuje. Brak przypadków wystąpienia zdarzenia w ostatnich 5 latach.

Poziom	Skutek
5 - Bardzo Wysoki	Krytyczny negatywny wpływ na podmioty danych, w tym utrata prywatności, życia, zdrowia, środków, reputacji.
4 - Wysoki	Znaczący negatywny wpływ na podmioty danych, w tym częściowa utrata prywatności, zdrowia, środków, reputacji.
3 - Średni	Średni negatywny wpływ na podmioty danych.
2 - Niski	Niski wpływ na podmioty danych.
1 - Bardzo niski	Bardzo niski wpływ na podmioty danych.

Prawdopodobieństwo wystąpienia zdarzenia oraz skutek jego zaistnienia

LexDigital

Macierz poziomu ryzyka oraz działania względem jego poziomu

Matryca ryzyka			Skutek				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
Prawdopodobieństwo	Bardzo wysokie	5	5 - Ś	10 - W	15 - W	20 - K	25 - K
	Wysokie	4	4 - N	8 - Ś	12 - W	16 - W	20 - K
	Średnie	3	3 - N	6 - Ś	9 - Ś	12 - W	15 - W
	Niskie	2	2 - N	4 - N	6 - Ś	8 - Ś	10 - W
	Bardzo niskie	1	1 - N	2 - N	3 - N	4 - N	5 - Ś

Poziom ryzyka	Konieczne działania
Niski (N)	Ryzyko akceptowalne – działania podejmowane w zależności od priorytetów i możliwości finansowych
Średni (Ś)	Ryzyko nieakceptowalne – wymagane okresowe monitorowanie, działanie może zostać przesunięte w czasie
Wysoki (W)	Ryzyko nieakceptowalne – wymagane stałe monitorowanie, działanie może zostać przesunięte w czasie
Krytyczny (K)	Ryzyko nietolerowalne – wymagane natychmiastowe działanie

LexDigital

Dokumentacja

Dobierz adekwatne środki zaradcze, opierając się na ocenie skuteczności poszczególnych rozwiązań. Wybierz te, które są najbardziej korzystne dla podmiotów danych, projektu i administratora.

- **Numer referencyjny**: Unikalny nr ryzyka pozwala jasno się do niego odnosić, np. w planie działań. Numeruj też zaproponowane środki ograniczające ryzyko.
- **Źródło ryzyka** (z powodu…): Odnoszące się do obszarów ryzyka jego źródło wynikające z aspektów przetwarzania danych w zmianie (np. zbieranie, przechowanie oraz ujawnienie danych).
- **Opis ryzyka** (istnieje ryzyko, że …): Określenie podatności każdego z aspektów przetwarzania danych, np. nowe wymogi w zakresie klauzul informacyjnych, zbierania zgód, wymogów systemowych lub inne decyzje dotyczące zmiany, które o ile będą niewłaściwie uwzględnione, mogą wpłynąć na projekt.
- **Skutki ryzyka** (wskutek czego…): Jak mogą one negatywnie lub pozytywnie wpłynąć na przetwarzającego i podmioty danych?
- **Aktualne środki ograniczające ryzyko**: Jak mogą przyczyniać się do zminimalizowania lub właściwego zarządzania zidentyfikowanym ryzykiem?
- **Ocena obecnego ryzyka rezydualnego**: Poziom prawdopodobieństwa i wpływ skutków przy obecnych środkach bezpieczeństwa.
- **Rekomendowane środki zapobiegawcze** dla ograniczenia, wyeliminowania ryzyka lub zarządzenia nim.
- **Ocena ryzyka szczątkowego** pozostałego po zastosowaniu rekomendowanych środków zapobiegawczych.

Przykładowa tabela analizy ryzyka

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub zarządzania nimi

Obszar 1: Rzetelność, przejrzystość i legalność przetwarzania (art. 5 ust 1. lit. a, art. 6 i 9)
Ryzyko związane z podstawą prawną

Nr ref.:	Źródło ryzyka (z powodu…)	Opis ryzyka (istnieje ryzyko, że …)	Skutki ryzyka (wskutek czego …)	Aktualne środki ograniczające ryzyko	Skutek	Prawdopodobieństwo	Wartość ryzyka
1	Zbierania danych osobowych od podmiotów trzecich	Braku przejrzystego przekazywania informacji o przetwarzaniu danych.	Osoba nie będzie posiadała wymaganych przez rodo informacji	Zapis w regulaminie usługi obligujący podmiot podający dane o konieczności poinformowania osób, ktorych dane są udostępniane.	4	5	20
2	Niepełnej informacji o zasadach przetwarzania danych szczególnych.	Niewypełnienie pełnego obowiązku informacyjnego.	Brak możliwości wypełniania praw podmiotów, które im przysługują. Informacje nie są podawane zgodnie z zasadą przejrzystości.	Sprawdzenie Poliyki prywatności oraz regulaminu usługi	2	2	4
3	Powierzenia danych osbowych Smart Software.	Nie uwzględnienie oraz brak oceny ryzyka dla wszystkich podprocesowrów.	Braku nadzoru nad wszystkimi podmiotami przetwarzającymi dane	Weryfikacja zapisów umowy.	5	2	10
4	Oparcie profilowania na opt-out	Błędna podstawa prawna przetwarzania danych	Skargi podmiótów na zasady potyczące profilowania	Poinformowanie podmiotów o zasadach profilowania podczas zawierania umówy	5	4	20
5	Przetwarzanie danych dotyczących zdrowia	Błędna podstawa prawna przetwarzania danych	Osoba, której dane dotyczą nie wyraziła zgody na przetwarzanie danych jej dotyczących.	Informowanie osób, których dane dotyczą o prawach im przysługujących.	4	5	20
6	Proces płatności za usługę i udostępniania danych	Niewypełnienie pełnego obowiązku informacyjnego.	Osoba, której dane dotyczą nie wyraziła zgody na przetwarzanie danych jej dotyczących.	Informowanie osób, których dane dotyczą o prawach im przysługujących.	3	3	9
7	Ubezpieczenie i udostępnianie danych ubezpieczycielowi	Niewypełnienie pełnego obowiązku informacyjnego.	Osoba, której dane dotyczą nie wyraziła zgody na przetwarzanie danych jej dotyczących.	Informowanie osób, których dane dotyczą o prawach im przysługujących.	2	2	4
8	Współpraca ze szpitalami	Brak podstawy prawnej przetwarzania danych szczególnych	Osoba, której dane dotyczą nie wyraziła zgody na przetwarzanie danych jej dotyczących.	Informowanie osób, których dane dotyczą o prawach im przysługujących.	3	3	9

Przykład przetwarza obarczone wysokim ryzykiem: Konsumenckie badania sensoryczne

Analiza ruchu klientów w sieci dużych sklepów przy użyciu nowych technologii, m.in. czujników ruchu i kamer, które monitorują zachowani i poruszanie się po sklepie.

Czujniki są w stanie ustalić drogę klienta przez sklep, czas spędzony przy poszczególnych towarach, co go zainteresowało aż po jego listę zakupów.

Dlaczego wysokie ryzyko?

1. Przetwarzanie na dużą skalę
2. Przetwarzanie danych biometrycznych (możliwość identyfikacji danej osoby przy kolejnych wizytach)
3. Wykorzystanie nowych technologii

LexDigital

Ocena potencjalnego ryzyka i możliwych sposobów jego ograniczenia w celu zmniejszenia negatywnych konsekwencji lub

Obszar 1: Rzetelność, przejrzystość i legalność przetwarzania (art. 5 ust 1. lit. a, art. 6 i 9)
Ryzyko związane z podstawą prawną

Nr ref.:	Źródło ryzyka (z powodu…)	Opis ryzyka (istnieje ryzyko, że …)	Skutki ryzyka (wskutek czego …)	Aktualne środki ograniczające ryzyko	Wpływ	Prawdopodobieństwo	Wartość ryzyka rezydualnego
1	Innowacyjny sposób zbierania danych biometrycznych.	Przetwarzanie danych biometrycznych będzie oparte na usprawiedliwionym interesie art. 6(1)(f).	Brak legalności przetwarzanych danych.	Poinformowanie klientów o podstawie prawnej przetwarzania ich danych.	4	4	16
2	Przetwarzanie danych biometrycznych.	Niepełne wypełnienie obowiązku informacyjnego o przetwarzaniu danych biometrycznych.	Brak wypełniania prawa Klienta do informacji zgodnie z zasadą przejrzystości.	Przygotowanie obowiązku informacyjnego dostępnego przy wejściu do sklepu.	4	4	16
4	Oparcie profilowania na opt-out	Błędna podstawa prawna przetwarzania danych	Skargi Klientów na zasady dotyczące profilowania	Poinformowanie Klientów o zasadach profilowania w obowiązku informacyjnym	4	4	16

Obszar 5: Ograniczenie przechowywania danych (art. 5 ust. 1 lit. e)
Ryzyko związane z usuwaniem danych po wygaśnięciu celów i podstawy prawnej oraz zasadami przetwarzania do innych celów, np. archiwalnuch po zastosowaniu odpowiednich środków bezpieczeństwa
Określenie sposobu przechowywania i zabezpieczania danych osobowych.

Nr	Źródło ryzyka (z powodu…)	Opis ryzyka (istnieje ryzyko, że …)	Skutki ryzyka (wskutek czego …)	Aktualne środki	Wpływ	Prawdopodo	Ocena
20	Archiwizacji danych BI - statystycznych	Możliwość identyfikacji Klienta na podstawie jego zachować.	Potencjalne negatywne skutki dla Klienta.	Anonimizacja danych zgodnie z przyjętymi zasadami. Weryfikacja potrzeb archiwizacji danych.	3	2	6

Plan Mitygacji Ryzyka

Ref	Opis Ryzyka	Uzgodnione działanie	Wpływ	Prawdopodobieńst	Ocena ryzyka szczątkowego
1	Przetwarzanie danych biometrycznych będzie oparte na usprawiedliwionym interesie art. 6(1)(f).	Przygotowanie mechanizmu pozwalającego na zebranie zgód (przycisk przy wejściu, wejście inną bramkę)	3	3	9
2	Niepełne wypełnienie obowiązku informacyjnego o przetwarzaniu danych biometrycznych.	Opracowanie transparentnej klauzuli informacyjnej dla Klientów z wyszczególnioną informacją dotyczącą danych biometrycznych oraz umieszczenie jej w widocznym miejscu	3	2	6
4	Błędna podstawa prawna przetwarzania danych.	Profilowanie wykonywane jest jedynie w celu marketingu bezpośredniego. Nie będzie dochodziło do profilowania preferencji żywnościowych, stylu życia i zdrowia Klientów.	2	2	4

Obszar 6: Integralność, poufność, dostępność do danych oraz zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych (art.5 ust. 1 l

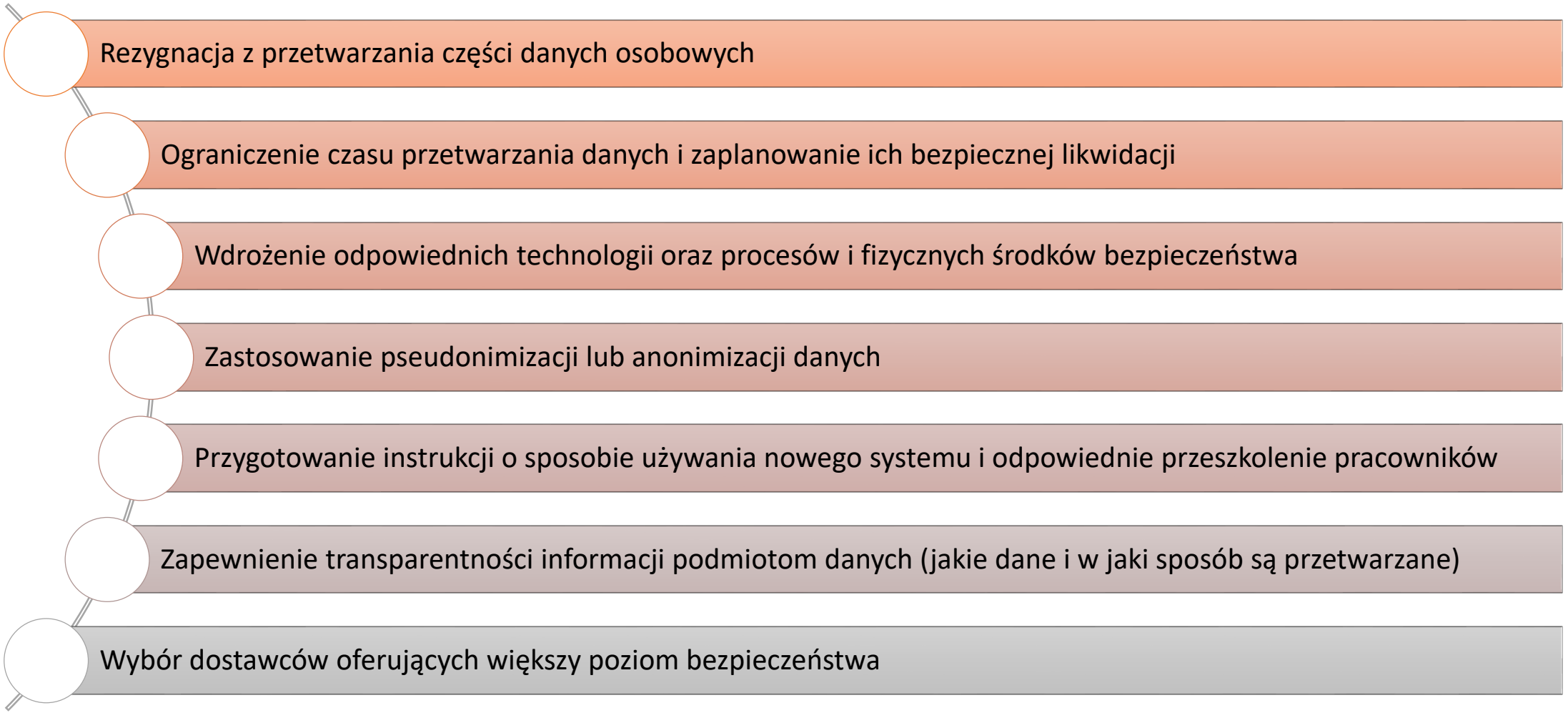
Nr	Źródło ryzyka (z powodu…)	Opis ryzyka (istnieje ryzyko, że …)	Skutki ryzyka (wskutek czego …)	Aktualne środki	Wpływ	Prawdopodo	Ocena
23	Wybór odpowiedniego dostawcy rozwiązania IT	Brak odpowiedniego poziomu bezpieczeństwa gwarantującego integralność, poufność i dostępność danych w systemie informatycznym	Może dojść do naruszenia prywatności danych Klientów.	Ogólne zapisy dotyczące bezpieczeństwa w umowie z dostawcą.	5	3	15
24	Zbieranie danych z czujników i kamer, które podlegają innowacyjnym algorytmom analitycznym	Brak wdrożenia odpowiednich zabezpieczeń technicznych w systemie informatycznym	Utrata poufności danych powodujących naruszenie praw Klientów.	Ograniczony dostęp do baz danych.	5	4	20
30	Regularne mierzenie i testowanie skuteczności środków technicznych i organizacyjnych mających zapewnić odpowiedni poziom bezpieczeństa	Ryzyko braku stosowania odpowiednich zasad przeprowadzania testów środków bezpieczeństwa przez podmiot przetwarzający.	Brak dostępności do danych.	Ogólne zapisy dotyczące testowania w umowie z dostawcą.	3	4	12

Obszar 7: Dostęp do danych osobowych (art. 15)
Ryzyko związane z zapewnieniem podmiotom dostępu do ich danych.
Odpowiadanie na wniosek podmiotu danych o dostęp do danych lub ich korektę.

Nr	Źródło ryzyka (z powodu…)	Opis ryzyka (istnieje ryzyko, że …)	Skutki ryzyka (wskutek czego …)	Aktualne środki	Wpływ	Prawdopodo	Ocena
33	Przetwarzanie danych z czujników i kamer	Nie będzie technicznej możliwości przekazania danych w ramach prawa dostępu	Przekazane dane w ramach wypełniania prawa dostępu nie będą zawierały danych z centalnego systemu rejestracji danych	Poinformowanie Klientów o zakresie danych zawartych w kopii danych	3	5	15
35	Niewłaściwej weryfikacji Klienta	Błędna identyfikacja podmiotu danych	Udostępnienie danych osobie nieupoważnionej. Naruszenie poufności danych i ich wykorzystanie niezgodnie z prawem.	Klient może złożyć prośby o kopię danych jednynie w przypadku podania dodatkowych informacji dotyczących wizyty w	3	3	9

Plan Mitygacji Ryzyka

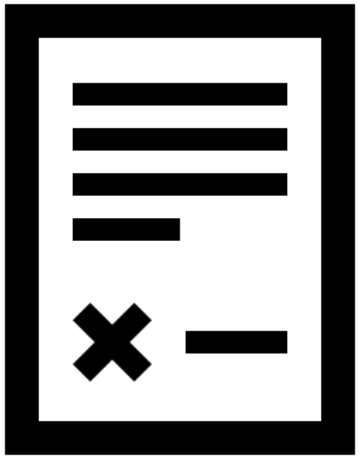
Ref	Opis Ryzyka	Uzgodnione działanie	Wpływ	Prawdop odobieńst	Ocena ryzyka szczątkowego
23	Brak odpowiedniego poziomu bezpieczeństwa gwarantującego integralność, poufność i dostępność danych w systemie informatycznym	Ustalenie z dostawcą systemu szczegółowych zasad stosowancyh zabezpieczeń w tym pseudonimizacji i szyfrowania danych podczas zbierania, transmisji i przetwarzania danych	2	2	4
24	Brak wdrożenia odpowiednich zabezpieczeń technicznych w systemie informatycznym	Dostosowanie zabezpieczeń używanych w czujnikach i kamerach do wymaganego poziomu - przeprowadznie testów	2	3	6
30	Ryzyko braku stosowania odpowiednich zasad przeprowadzania testów środków bezpieczeństwa przez podmiot przetwarzający.	Wprowadzenie zasad regularnego monitorowania i testowanie - składanie raportów do administratora. Prowadzenie audutów zewnętrznych	2	2	4
33	Nie będzie technicznej możliwości przekazania danych w ramach prawa dostępu	Poinformowanie osób o zasadach wypełniania prawa dostępu w zakresie tego procesu.	3	2	6



Dobór środków mitygujących ryzyko

LexDigital

Etap 3: Przygotowanie raportu końcowego



Wsparcie dla biznesu	Zadaniem OSOD jest wsparcie celów projektu i dostarczenie zarządowi i pozostałym kluczowym interesariuszom propozycji strategii ograniczenia ryzyka prywatności w celu podjęcia świadomych decyzji.
Rozliczalność	OSOD dokumentuje należytą staranność względem ochrony danych osobowych i wykazuje stosowanie ochrony danych w fazie projektowania oraz domyślną ochronę danych, przez co pozwala na wykazanie stosowania zasady rozliczalności.
Działania	Dla każdego rekomendowanego środka zaradczego, ograniczającego ryzyko, określa się konkretne działania, osobę odpowiedzialną i termin realizacji. Wszelkie decyzje dotyczące prywatności i wybranych działań powinny być odpowiednio udokumentowane i zaakceptowane.

LexDigital

Co powinno się znaleźć w raporcie końcowym?

A. Nazwa projektu, data przeprowadzania oraz osobę odpowiedzialną za OSOD

B. Wstępna ocena skutków dla ochrony danych – ocena ogólna ryzyka

C. Analiza projektu wraz identyfikacją zagrożeń i ich potencjalnych skutków dla prywatności oraz cena ryzyka prywatności i rekomendowane środki zaradcze

D. Streszczenie zarządcze - decyzje i zgody na wprowadzenie środków zaradczych lub akceptację ryzyka

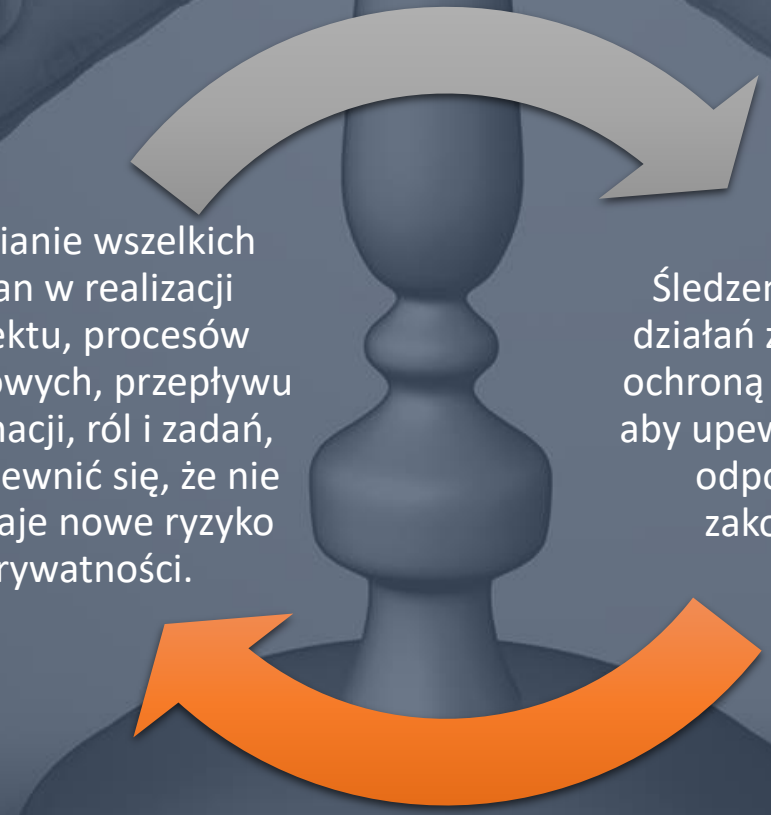
E. Dalsze działania, w tym konsultacje z organem nadzorczym w przypadku wysokiego ryzyka przed rozpoczęciem przetwarzania

F. Przypadki, w których należy dokonać przeglądu niniejszej oceny

G. Załączniki

LexDigital

Etap 4: Monitoring wdrożenia



Ocenianie wszelkich zmian w realizacji projektu, procesów biznesowych, przepływu informacji, ról i zadań, aby upewnić się, że nie powstaje nowe ryzyko prywatności.

Śledzenie postępu działań związanych z ochroną prywatności, aby upewnić się, że są odpowiednio zakończone.

LexDigital

W każdym etapie OSOD korzystaj z wiedzy ekspertów IT, zarządzania, ryzyka, bezpieczeństwa, prawa i prywatności oraz właścicieli biznesowych

Dla analogicznych operacji przetwarzania danych, wiążących się z podobnym ryzykiem, przeprowadź pojedynczą ocenę

To nie ma być ocena technicznych aspektów systemu, ale ocena skutków zmiany wobec ochrony danych osobowych

Dołóż starań, aby informacje były przedstawione w sposób prosty i zrozumiały dla odbiorcy, który nie posiada wiedzy na temat technologii, prawa lub tego systemu

Unikaj żargonów i skrótów, gdy nie są powszechnie zrozumiałe chyba, że je wyjaśnisz

Informacje powinny być zwięzłe, ale niezbędne do zrozumienia OSOD

Wskazówki

LexDigital

O czym warto pamiętać?

Minimalizacja danych to środek zmniejszający ryzyko przetwarzania danych

Łączone informacje mogą potencjalnie zwiększyć ryzyko zidentyfikowania osoby przez wnioskowanie, nawet jeśli sama informacja nie jest uważana za dane osobowe

Ocena ryzyka i potencjalnych środków zaradczych pozwala wybrać te, które są najbardziej korzystne dla podmiotów danych, projektu i administratora danych

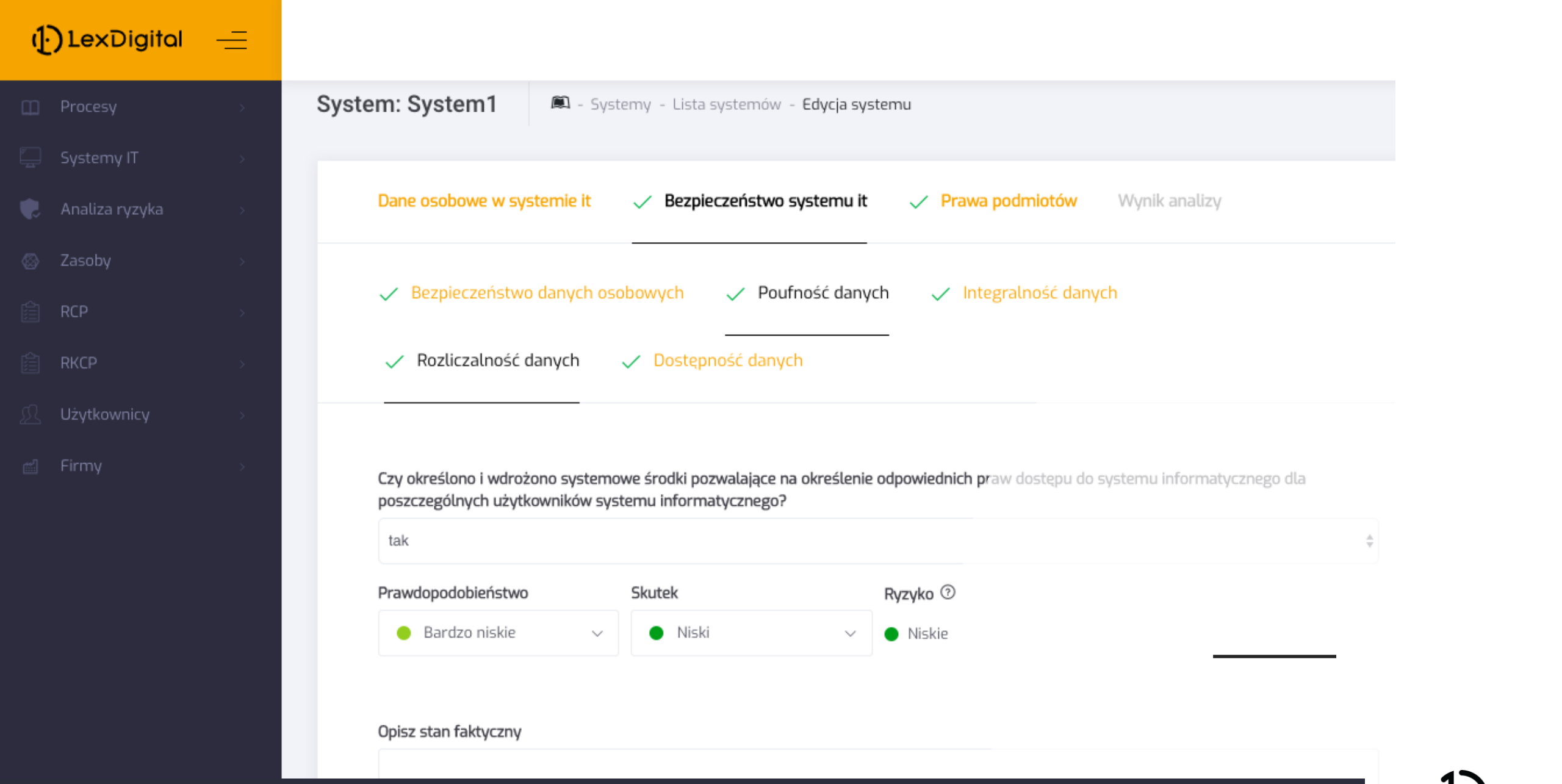
Udokumentuj etapy OSOD, aby zgodnie z zasadą rozliczalności móc wykazać przed organem nadzorczym wypełnienie obowiązku z RODO

LexDigital

OSOD:
DROGA DO ROZLICZENIA, CZYLI JAK KIEROWAĆ SIĘ RODO-WSKAZEM

Dostosowanie do wymogów RODO	Rozmowa	Zrozumienie	Adaptacja
Wypełniania praw podmiotów danych w	IT	Całej organizacji	
RODO-wita kultura i polityka organizacji	„Kieruj się RODOWSKAZEM"	**OSOD**	**POnR** (podejście oparte na ryzyku)

LexDigital



Przetestuj: https://lexdigital.pl/aplikacja-dla-iod

LexDigital

Dziękuję za uwagę

Mariola Więckowska
Dyrektor ds.
Innowacyjnych Technologii Ochrony Danych

LexDigital

ul. Zakręt 8
60-351 Poznań

www.LexDigital.pl
e-mail: biuro@lexdigital.pl