Załącznik nr 7 do Polityki Ochrony Danych Osobowych
Metodyka analizy ryzyka

1. Postanowienia ogólne

1.1. Niniejsza metodyka stanowi załącznik do Polityki ochrony danych osobowych. W celu określenia rekomendowanych minimalnych poziomów bezpieczeństwa danych posługujemy się niżej przedstawioną uproszczoną metodyką analizy ryzyka danych osobowych.

1.2. Z zastrzeżeniem pojęć zdefiniowanych w treści niniejszego dokumentu, pojęcia pisane z dużej litery mają znaczenie nadane im w Polityce.

1.3. Definicje:

1.3.1. **Metodyka** – oznacza niniejszy dokument stanowiący podstawę do przeprowadzenia uproszczonej metodyki analizy ryzyka danych osobowych.

1.3.2. **Polityka** – oznacza przyjętą w Spółce Politykę ochrony danych osobowych.

2. Ryzyko przetwarzania danych osobowych

2.1. Na potrzeby Metodyki ryzyko przetwarzania danych osobowych jest rozumiane jako ryzyko naruszenia praw lub wolności osób fizycznych przy przetwarzaniu danych osobowych. Przyjmuje się, że ryzyko przetwarzania danych osobowych ma dwa wymiary:

2.1.1. ryzyko nieupoważnionego dostępu lub wykorzystania danych osobowych (ryzyko naruszenia poufności), oraz

2.1.2. ryzyko niemożności wykorzystania danych w sposób przewidziany (ryzyko niedostępności danych i ryzyko wadliwości danych).

2.2. Przy szacowaniu ryzyka przetwarzania danych osobowych bierze się pod uwagę powagę potencjalne szkody dla osoby, zgodnie z motywem 75 preambuły RODO. Kwestia prawdopodobieństwa wystąpienia szkody jest uwzględniana w dalszej kolejności w sposób ilościowy/statystyczny – tzn. w oparciu o skalę przetwarzania, zgodnie z logiką art. 35 i 37 RODO.

3. Założenia Metodyki

3.1. Na potrzeby ustalenia poziomów ryzyka oraz zastosowania Metodyki brane są pod uwagi następujące czynniki:

3.1.1. branża (sektor), w tym o ile jest możliwy do wyodrębnienia, podsektor;

3.1.2. klientela (kategorie danych);

3.1.3. skala przetwarzanych danych oraz dodatkowo:

3.1.4. wysokość przychodów (obroty).

3.2. Łącznie czynniki branży (podsektoru) i klienteli wskazują na ogólne ryzyko prowadzonej działalności dla praw i wolności osób, których dane są przetwarzane. W tym celu, w pierwszej kolejności jest określane punktowo ryzyko branży oraz analogicznie ryzyko kategorii danych, przyjmując skalę od 1 do 3. Następnie wyniki tej punktacji są sumowane i wskazują one na ogólny poziom ryzyka naruszenia praw lub wolności osób fizycznych dla prowadzonej działalności.

3.3. W dalszej kolejności ogólny poziom ryzyka prowadzonej działalności jest zestawiany ze skalą działalności, dając łączny poziom ryzyka dla naruszenia praw lub wolności osób fizycznych, przy przetwarzaniu danych osobowych, który dodatkowo przez administratora przeszacowany jest wzwyż w przypadku dużego obrotu.

3.4. Metodyka ustalania poziomów ryzyka jest określana dla czynności przetwarzania stanowiących główny przedmiot działalności administratora, tj. wykonywanie czynności agencyjnych lub brokerskich na rzecz towarzystw ubezpieczeniowych.

3.5. Przyjmuje się, że ryzyko naruszenia praw i wolności dla czynności przetwarzania związanych z bieżącą działalnością organizacji (niestanowiących głównego przedmiotu działalności, tzw. core biznesu), tj. czynności przetwarzania z obszaru księgowości, prowadzenia kadr/HR lub bieżącej działalności, jest potencjalnie takie samo dla każdego rodzaju organizacji, i zostało ono zakwalifikowane do Poziomu I. Oznacza to, że Metodyka powinna znaleźć zastosowanie do czynności przetwarzania danych, które są wykonywane jako czynności związane z podstawową, zarobkową działalnością.

4. Branża

4.1. Przyjmuje się, że branża, w której dochodzi do przetwarzania danych osobowych, ma wpływ na ryzyko przetwarzania danych osobowych. Dla przykładu, działalność produkcyjna ma mniejsze ryzyko niż handel konsumencki. Działalność finansowa ma wyższe ryzyko niż transport. Przyjmujemy zatem, że poszczególne sektory gospodarki mają swoje „właściwe" / „natywne" ryzyko przetwarzania danych osobowych. W przypadku podmiotów wielobranżowych, gdy dane przetwarzane są tymi samymi zasobami (jak to zwykle bywa w przypadku mniejszych podmiotów), należy kierować się oceną ryzyka dla branży o najwyższym ryzyku właściwym. Gdy linie biznesowe są organizacyjnie i fizycznie rozdzielone, należy przeprowadzić dla nich odrębne oceny ryzyka.

4.2. Jeśli jest możliwe wyodrębnienie podtypu w ramach danej branży, należy ocenić na ile ten podtyp ma wpływ na ryzyko przetwarzania danych osobowych. Należy ocenić typ spraw, praktyki w ramach działalności.

5. Klientela

Klientela, czyli osoby lub podmioty, do których kierujemy ofertę usług lub produktów, także wpływa na ryzyko przetwarzania danych osobowych. Określa ona bezpośrednio (gdy klientami są osoby fizyczne) lub pośrednio (gdy naszymi klientami są przedsiębiorcy) kategorie osób i danych, które są przedmiotem przetwarzania. Należy więc zwrócić uwagę na to, do jakich klientów skierowana jest oferta organizacji. W tym miejscu uwzględniamy ryzyko kategorii danych, które przetwarzamy, gdy nie wynika to bezpośrednio z branży. Szczególnie istotne jest to w przypadku sektorów „wsparcia" biznesu (doradztwo, call center, informatyka itp.).

6. Skala przetwarzania danych

Skala przetwarzanych danych, czyli liczba rekordów danych osobowych (liczba klientów, pacjentów, pracowników itp.), bezpośrednio przekłada się na ryzyko przetwarzania danych osobowych. Im więcej osób „przetwarzamy", ale też im więcej osób po naszej stronie ma dostęp do danych, tym większe prawdopodobieństwo, że „coś pójdzie nie tak" oraz że wystąpią mniej prawdopodobne, ale bardziej dotkliwe w skutkach zdarzenia. Ryzyko naruszenia rośnie proporcjonalnie wraz ze wzrostem liczby (skali) przetwarzanych danych.

7. Wysokość przychodów

Możliwe, że nie ma związku przyczynowego pomiędzy tym, że zarabiamy więcej pieniędzy, a tym, że generujemy większe ryzyko przetwarzania danych osobowych. Uważamy jednak, że taka korelacja na ogół zachodzi, a co więcej, że im bogatsza firma (generująca wyższe przychody), tym jest większa tendencja, żeby przeciwko takiej firmie kierowane były roszczenia oraz działania kontrolne. Ponadto wysokość osiąganych przychodów jest pochodną skali prowadzonej działalności, a potencjalnie im wyższa skala działalności, tym większa liczba danych przetwarzamy. Dlatego wysokość przychodów uznajemy za czynnik mający wpływ na ryzyko przetwarzania danych.

8. Sposób ustalenia poziomów bezpieczeństwa

Krok 1 – Ryzyko branży

Spółka określa poziom ryzyka branży w skali 1–3

Ryzyko branży

Poziom ryzyka	Niskie	Średnie	Wysokie
Jaki poziom ryzyka (dla praw i wolności, osób, których dane przetwarza) przetwarzania danych generuje nasza branża? [Dokonując oceny, proszę wziąć pod uwagę nie tylko ogólnie branżę, lecz także charakter własnej działalności na tle branży]	1	2	3

	= Poziom ryzyka branży 1 (ryzyko niskie)
	= Poziom ryzyka branży 2 (ryzyko średnie)
	= Poziom ryzyka branży 3 (ryzyko wysokie)

Krok 2 - Ryzyko klienteli

Spółka określa ryzyko klienteli, mnożąc jego dwa wymiary – powagę ryzyka wycieku danych i powagę ryzyka niedostępności (lub niepoprawności danych)

Ryzyko klienteli (kategorii osób i danych)

	Jaki wpływ (jakie konsekwencje) na prawa i wolności osób, których dane przetwarzamy, miałoby naruszenie poufności danych (ich wyciek)?		
Jaki wpływ (konsekwencje) na prawa i wolności osób, których dane przetwarzamy, miałaby niedostępności lub wadliwość danych?	**Niskie 1**	**Średnie 2**	**Wysokie 3**
Niskie 1	1	2	3
Średnie 2	2	4	6
Wysokie 3	3	6	9

Interpretacja wyników

wynik mnożenia (1, 2, 3)	=	jasnoszary	=	Poziom ryzyka klienteli 1 (ryzyko niskie)
wyniki mnożenia (4, 6)	=	szary	=	Poziom ryzyka klienteli 2 (ryzyko średnie)
wynik mnożenia (9)	=	ciemnoszary	=	Poziom ryzyka klienteli 3 (ryzyko wysokie)

Krok 3 - Ryzyko działalności

Spółka określa ryzyko działalności mnożąc jego dwa wymiary ustalone w krokach 1 i 2 – ryzyko branży i ryzyko klienteli

Ryzyko działalności łącznie

	Ryzyko branży		
Ryzyko klienteli	Niskie 1	Średnie 2	Wysokie 3
Niskie 1	1	2	3
Średnie 2	2	4	6
Wysokie 3	3	6	9

Interpretacja wyników

wynik mnożenia (1, 2, 3)	=	jasnoszary	=	Poziom ryzyka klienteli 1 (ryzyko niskie)
wyniki mnożenia (4, 6)	=	szary	=	Poziom ryzyka klienteli 2 (ryzyko średnie)
wynik mnożenia (9)	=	ciemnoszary	=	Poziom ryzyka klienteli 3 (ryzyko wysokie)

Krok 4 - Ryzyko skali przetwarzania

Spółka określa ryzyko skali przetwarzania danych, mnożąc jego dwa wymiary – ilość osób, których dane przetwarzasz i ilość osób, którym dajesz dostęp do danych

Ryzyko skali

(uwaga: na potrzeby art. 35 i 37 RODO parametry dla średniej skali dla danych szczególnych kategorii zaliczono do dużej skali)

	Dane ilu osób przetwarzamy		
Ilu osobom dajemy dostęp do danych (pracownicy + inne osoby upoważnione)	Mało (do 6 tys. osób) 1	Średnio (do 50 tys. osób) 2	Wysoko (dużo) (powyżej 50 tys osób) 3
Mało (do 20 osób)	1	2	3
Średnio (21 do 249 osób)	2	4	6
Wysokie (ponad 250 osób)	3	6	9

wynik mnożenia (1, 2)	=	jasnoszary	=	Poziom ryzyka skali 1 (ryzyko niskie)
wyniki mnożenia (3, 4)	=	szary	=	Poziom ryzyka skali 2 (ryzyko średnie)
wynik mnożenia (6, 9)	=	ciemnoszary	=	Poziom ryzyka skali 3 (ryzyko wysokie)

Krok 5 - Ryzyko przetwarzania danych

Spółka określa ogólną wartość ryzyka przetwarzania danych, mnożąc jego dwa wymiary ustalone w krokach 3 i 4 – ryzyko skali i ryzyko działalności

	ryzyko skali		
ryzyko działalności	**Mała (1)**	**Średnia (2)**	**Wysoka (3)**
Małe 1	1	2	3
Średnie 2	2	4	6
Wysokie 3	3	6	9

wynik mnożenia (1, 2, 3)	=	jasnoszary	=	Poziom ryzyka przetwarzania 1 (ryzyko niskie) Środki Bezpieczeństwa Danych Poziom 1
wyniki mnożenia (4, 6)	=	szary	=	Poziom ryzyka przetwarzania 2 (ryzyko średnie) Środki Bezpieczeństwa Danych Poziom 2
wynik mnożenia (9)	=	ciemnoszary	=	Poziom ryzyka przetwarzania 3 (ryzyko wysokie) Środki Bezpieczeństwa Danych Poziom 3

Krok 6 – Obrót i budżet na ryzyko

Na końcu należy odpowiedzieć na pytanie jakie są roczne obroty?

Obroty roczne	Małe do 1 mln zł	Średnie 1-5 mln zł	Wysokie powyżej 5 mln zł

Jeżeli obroty są wysokie, to Spółka podwyższa ocenę ryzyka o jeden poziom.

9. Środki bezpieczeństwa danych

9.1. Poziom 1:

- kontrola dostępu do sprzętu elektronicznego, na którym gromadzone są dane osobowe (uniemożliwienie osobom nieuprawnionym dostępu do sprzęty używanego do przetwarzania),
- dostęp do elektronicznych nośników danych zabezpieczony hasłem,
- przechowywanie dokumentów zawierających dane osobowe w pomieszczeniach zamykanych na klucz uniemożliwiając dostęp osobom nieupoważnionym - zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
- pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów,
- zapobieganie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych,
- zapobieganie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych,
- zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników (w szczególności szyfrowanie i zabezpieczanie plików zawierających dane osobowe hasłem),
- hasła dostępowe do nośników zawierających dane osobowe powinny składać się z co najmniej 8 znaków (w tym co najmniej jednej małej litery, jednej wielkiej litery, jednej cyfry i jednego znaku specjalnego) oraz powinny być zmieniane przez użytkownika nie rzadziej niż raz w miesiącu,
- każdy pracownik posiada wyznaczone dla siebie stanowisko komputerowe, co zmniejsza ryzyko naruszenia integralności danych osobowych, jednak w przypadku pracowników pracujących na jednym stanowisku komputerowym każdy z nich posiada osobne konta użytkownika,
- stosowane są środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
- zapewnienie przywrócenia zainstalowanych systemów w razie awarii,
- zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu,
- przeprowadzanie szkoleń z zakresu ochrony danych osobowych nie rzadziej niż raz w roku,

- przeprowadzanie kontroli przetwarzania danych osobowych przez Zarząd lub Inspektora Ochrony Danych, jeśli został powołany nie rzadziej niż raz w roku,
- stosowanie zasady „czystego biurka" (tj. nie należy pozostawiać żadnych dokumentów z danymi osobowymi, podczas nieobecności pracownika przy stanowisku pracy, nie należy pozostawiać dokumentów zawierających dane osobowe podczas obsługi klienta, którego dane te nie dotyczą),
- stosowanie zasady „czystego ekranu" (tj. ustawienie monitorów w taki sposób, by uniemożliwić klientom, interesantom czy osobom trzecim wgląd w dane osobowe na nich wyświetlane. Zasada „czystego ekranu" obejmuje również pliki zamieszczone na pulpicie. Takie pliki mogą bowiem w samych nazwach zawierać dane osobowe, np. gdy aktualnie negocjowane umowy z poszczególnymi klientami nazywamy używając ich imienia i nazwiska. Odchodząc od komputera należy bezwzględnie pamiętać o jego blokowaniu - np. używając skrótu klawiszowego Windows+L oraz ustawienie automatycznej blokady komputera),
- stosowanie alarmu i monitoringu wizyjnego w budynku gdzie przechowywane są dane osobowe,
- do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie,
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
- opracowano i wdrożono politykę ochrony danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy,
- w lokalu przebywać muszą zawsze co najmniej dwie osoby upoważnione do przetwarzania danych osobowych, z wyjątkiem Członków Zarządu i Inspektora Ochrony Danych, który przebywać mogą samodzielnie.

9.1. Poziom 2:

Wszystkie zabezpieczenia stosowane przy poziomie 1, a ponadto:

- przeprowadzanie szkoleń z zakresu ochrony danych osobowych w odstępach nie dłuższych niż 6 miesięcy,
- przeprowadzanie kontroli przetwarzania danych osobowych przez Zarząd lub Inspektora Ochrony Danych, jeśli został powołany w odstępach nie dłuższych niż 3 miesiące,
- dane w formie papierowej przechowywane są w zamkniętej, niemetalowej/metalowej szafie lub sejfie, kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej/metalowej szafie lub sejfie,
- stosowane są mechanizmy wymuszające okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych,
- stosowane są mechanizmy automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika,
- w lokalu przebywać muszą zawsze co najmniej dwie osoby upoważnione do przetwarzania danych osobowych.

9.1. Poziom 3

Wszystkie zabezpieczenia stosowane przy poziomie 2, a ponadto:

- przeprowadzanie szkoleń i testów z zakresu ochrony danych osobowych w odstępach nie dłuższych niż 3 miesiące,
- przeprowadzanie kontroli przetwarzania danych osobowych przez Zarząd lub Inspektora Ochrony Danych, jeśli został powołany nie rzadziej niż raz w miesiącu,
- dane są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min,
- dane są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie – drzwi klasy C,
- dane są przechowywane w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,
- dostęp do pomieszczeń objęty jest systemem kontroli dostępu,
- dostęp do pomieszczeń jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.