Ocena ryzyka

1. W celu zminimalizowania ryzyka, czyli możliwości wykorzystania podatności przez zagrożenie w celu spowodowania utraty zachowania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności danych osobowych, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na jednostkę dokonano oceny poziomu ryzyka.

2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

3. Sposób oceny prawdopodobieństwa wystąpienia zdarzenia:

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysokie	5	Przewiduje się, że zdarzenie objęte ryzykiem będzie powtarzalne w ciągu roku.
Wysokie	4	Przewiduje się, że zdarzenie objęte ryzykiem wystąpi kilkakrotnie w ciągu roku.
Średnie	3	Przewiduje się, że zdarzenie objęte ryzykiem będzie występowało okazjonalnie, bądź w wyniku równoczesnego występowania różnych problemów i okoliczności.
Niskie	2	Przewiduje się, że zdarzenie objęte ryzykiem wystąpi raz w ciągu roku.
Bardzo niskie	1	Przewiduje się, że zdarzenie objęte ryzykiem nie wystąpi w ciągu roku.

4. Ocena skutków dokonywana jest w skali od 1 do 5, oceniając niżej wymienione kryteria:

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki

Bardzo Duży	5	Bardzo duży i trwały wpływ na finanse. Utrata wizerunku i zaufania do jednostki organizacyjnej. Zdarzenie uniemożliwia realizację zadania, zagraża realizacji celu
Duży	4	Duży wpływ na finanse, którego zminimalizowanie wymaga zaangażowania znaczącego zasobu czasu lub środków. Sytuacje i zjawiska prowadzące do zmniejszenia zaufania w niektórych obszarach. Zdarzenie wpływa na przekroczenie mierników realizacji zadania.
Średni	3	Średni skutek finansowy. Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielki negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego.
Mały	2	Niewielki wpływ na finanse, wymagający podjęcia działań, w wyniku których zakłócenie w realizacji zadania zostanie zneutralizowane. Sporadyczne, krótkotrwałe sygnały dotyczące pojedynczych zdarzeń, niewpływające na wizerunek całej jednostki organizacyjnej. Zdarzenie utrudnia realizację zadania.
Bardzo mały	1	Znikomy wpływ na finanse, niewymagający podejmowania reakcji związanej z realizacją zadania. Brak negatywnych reakcji zewnętrznych na działania jednostki organizacyjnej. Zdarzenie nie wpływa na realizację zadania.

5. Poziom ryzyka to iloczyn prawdopodobieństwa wystąpienia zdarzeń określonych w § 6 oraz skali oddziaływania (skutków) w przypadku ich wystąpienia.

Prawdopodo-bieństwo	5 Bardzo wysokie	5	10	15	20	25
	4 Wysokie	4	8	12	16	20
	3 Średnie	3	6	9	12	15

	2 Niskie	2	4	6	8	10
	1 Bardzo niskie	1	2	3	4	5
		1 Bardzo mały	2 Mały	3 Średni	4 Duży	5 Bardzo duży
		Skutek				

Poziom ryzyka określa zależność:

R=P*O

gdzie:

R – poziom ryzyka,
P – prawdopodobieństwo wystąpienia zdarzenia,
O – skala oddziaływania w przypadku wystąpienia zdarzenia,

6. Poziom Istotności Ryzyka:

1) Z punktu widzenia jednostki najbardziej istotne są obszary, w których poziom ryzyka wynosi więcej niż 15. Jest to ryzyko nieakceptowalne, które musi zostać zmniejszone i stale monitorowane. W przypadku wystąpienia takiego poziomy przetwarzanie danych zostaje wstrzymane do momentu jego zmniejszenia.
2) Poziom ryzyka w skali od 4 do 14 oznaczono obszar średniego zagrożenia.
3) Poziom ryzyka od 1 do 3 to obszar ryzyka, w którym zmaterializowanie się zdarzeń jest mało prawdopodobne, lub ich wpływ na jednostkę jest niewielki.

Zagrożenie:	Prawdopodobieństwo:	Oddziaływanie:	Poziom ryzyka:
włamania od strony okien	1	3	3
włamania od strony drzwi	1	3	3
oddziaływanie czynników zewnętrznych	1	3	3
pozostawienie niezamkniętych drzwi	1	3	3
pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach	1	2	2
pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy	1	2	2
pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze	1	2	2
pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe	1	2	2
przechowywanie dokumentów w miejscach do tego nieprzeznaczonych	1	1	1
wyrzucanie dokumentów w stopniu zniszczenia	1	2	2

umożliwiającym ich odczytanie			
przetwarzanie danych przez osoby nieuprawione	1	2	2
nieuzasadnione sporządzanie kserokopii danych	1	2	2
dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych	1	2	2
dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią	1	1	1
sporządzanie kopii danych w sytuacjach niewynikających z zakresu obowiązków służbowych	1	2	2
utrata kontroli nad kopią danych osobowych	1	2	2
podmiana lub zniszczenie nośników z danymi osobowymi	1	2	2
pozostawienie zapisanego hasła dostępu do bazy danych	1	3	3
samodzielne instalowanie oprogramowania, którego instalacja nie jest wymagana w	1	2	2

celu umożliwienia wykonywania obowiązków służbowych			
obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	1	2	2
opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych	1	2	2
odczytywanie nośników przed sprawdzeniem ich programem antywirusowym	1	2	2
dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych	1	3	3
ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym	1	2	2
ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	1	2	2
dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	2	1	2

awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich	1	2	2
nieoczekiwane, niedające się wyjaśnić zmiany danych	1	2	2
niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych	1	2	2
próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej	1	2	2
dopuszczanie aby osoby inne niż ADO, ABI lub osoby przez nich uprawnione podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji	1	3	3
manipulacja przy układach sieci komputerowej lub komputerach	1	3	3
obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu	1	3	3

Jak przedstawia powyższa analiza, poziom ryzyka w jednostce jest niski (maksymalny poziom ryzyka wynikający z macierzy wynosi 3. Oznacza to więc, iż zastosowane środki techniczne oraz organizacyjne mające na celu zapewnienie bezpieczeństwa i ochronę danych osobowych są wystarczające.

Pomimo takiej oceny, nie należy zaprzestać analizowania jego poziomu. Trzeba aktualizować jego ocenę każdorazowo w przypadku jakiejkolwiek zmiany w sposobie przetwarzania danych osobowych lub zmianach spowodowanych wprowadzeniem nowych środków organizacyjnych lub technicznych określonych w niniejszej dokumentacji