

Analiza ryzyka dla bezpieczeństwa danych osobowych przetwarzanych w ramach

I. Wstęp

Analizę ryzyka przeprowadzono dla atrybutów bezpieczeństwa związanych z poufnością, integralnością, rozliczalnością i dostępnością danych przetwarzanych w ramach

Aktualizacja wyników analizy ryzyka będzie dokonywana zgodnie z ogólnymi zasadami zarządzania ryzykiem w Ministerstwie Finansów.

Ocena ryzyka została wyliczona zgodnie z niżej opisanymi parametrami:

Ocena ryzyka = Ocena prawdopodobieństwa x Ocena oddziaływania

Dla oceny oddziaływania zagrożenia z wykorzystaniem podatności należy przyjąć poniżej zamieszczoną skalę punktową:

- 1) nieznaczne – 1 punkt;
- 2) małe – 2 punkty;
- 3) średnie – 3 punkty;
- 4) poważne – 4 punkty;
- 5) katastrofalne – 5 punktów.

oddziaływanie zagrożenia	opis	wartość
nieznaczne	Utrata poufności, integralności, dostępności i rozliczalności informacji/danych, związana z pojedynczym incydem, która nie będzie miała większego wpływu na realizację zadań przez jednostkę organizacyjną ani nie będzie miała szkodliwego wpływu na interesy i prawa osób, których te informacje/dane dotyczyły.	1 punkt
małe	Utrata poufności, integralności, dostępności i rozliczalności informacji/danych, która może mieć wpływ na działalność jednostki organizacyjnej lub interesy lub prawa osób, których dane dotyczą; może się wiązać z pojedynczymi negatywnymi opiniami w mediach lokalnych.	2 punkty
średnie	Utrata poufności, integralności, dostępności i rozliczalności informacji/danych, która może mieć znaczący wpływ na działalność jednostki organizacyjnej lub interesy lub prawa osób trzecich oraz może spowodować narażenie na utratę wizerunku (negatywne opinie w mediach lokalnych i regionalnych) lub roszczenie ze strony pojedynczych osób.	3 punkty
poważne	Utrata poufności, integralności, dostępności i rozliczalności informacji/danych, która ma znaczący wpływ na działalność jednostki organizacyjnej i interesy lub prawa osób, których	4 punkty

	dane dotyczyły oraz skutkuje koniecznością poinformowania o zdarzeniu do organu nadzorczego ds. ochrony danych osobowych oraz osób, których te dane dotyczyły; powoduje utratę wizerunku (negatywne opinie w mediach ogólnopolskich/internecie) lub/i roszczenia ze strony niewielkiej grupy osób.	
katastrofalne	Utrata poufności, integralności, dostępności i rozliczalności informacji/danych, która może sparaliżować działalność organizacji, skutkująca wyjątkowo poważną szkodą dla organizacji, zagrażająca interesom i prawom osób, których te dane dotyczyły; skutkująca koniecznością poinformowania o zdarzeniu do organu nadzorczego ds. ochrony danych osobowych oraz osób, których te dane dotyczyły; wiążąca się z utratą wizerunku (negatywne opinie w mediach ogólnopolskich/internecie) lub/i roszczeniami ze strony dużej grupy osób, a także karami administracyjnymi ze strony organu nadzorczego ds. danych osobowych.	5 punktów

Dla oceny prawdopodobieństwa wystąpienia zagrożenia z wykorzystaniem podatności należy przyjąć poniżej zamieszczoną skalę punktową:

- 1) bardzo mało prawdopodobne – 1 punkt;
- 2) mało prawdopodobne – 2 punkty;
- 3) możliwe prawdopodobieństwo wystąpienia – 3 punkty;
- 4) duże prawdopodobieństwo – 4 punkty;
- 5) bardzo duże prawdopodobieństwo – 5 punktów.

prawdopodobieństwo wystąpienia zagrożenia	opis	wartość
bardzo mało prawdopodobne	nie ma realnej szansy wystąpienia zagrożenia (zagrożenie nigdy dotąd nie wystąpiło)	1 punkt
mało prawdopodobne	może wystąpić pojedynczy incydent raz na kilka lat	2 punkty
możliwe prawdopodobieństwo wystąpienia	może wystąpić pojedynczy incydent mniej więcej raz na rok	3 punkty
duże prawdopodobieństwo	zagrożenie występuje regularnie, z określoną częstotliwością, np. raz na kwartał, raz w miesiącu.	4 punkty
bardzo duże prawdopodobieństwo	może wystąpić w każdym momencie, występuje kilkanaście incydentów w miesiącu.	5 punktów

Kryteria oceny ryzyka

Poziom ryzyka	Opis	Wartość poziomu ryzyka
Niski – ryzyko akceptowalne	Ryzyka możliwe do zaakceptowania (świadomą decyzją kierownictwa)	1-6
Średni – ryzyko nieakceptowalne	Ryzyka nieakceptowane wymagające postępowania z ryzykiem (redukcja ryzyka,	8-12

	przeniesienie ryzyka, rezygnacja z działań powodujących występowanie ryzyk)	
Wysoki - ryzyko nieakceptowalne	Ryzyka nieakceptowane wymagające postępowania z ryzykiem z wysokim priorytetem (redukcja ryzyka, przeniesienie ryzyka, rezygnacja z działań powodujących występowanie ryzyka)	15-25

II. A. Ocena ryzyka dla grupy zagrożeń: zniszczenie fizyczne

LP	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdopodobieństwa [1 – 5]	Ocena oddziaływania [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczenia
1.1						
1.2						
1.3						
1.4						

Mapa ryzyka grupy zagrożeń: zniszczenie fizyczne

Ocena oddziaływania	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5

Ocena prawdopodobieństwa

II. B. Ocena ryzyka dla grupy zagrożeń: naruszenie bezpieczeństwa informacji
(ewentualnie podzielić ze względu na lokalizację, np: MF, CIRF, zewnętrzne..)

LP	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdopodobieństwa [1 – 5]	Ocena oddziaływania [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczenia
2.1						
2.2						
2.3						
2.4						
2.5						
2.6						
2.7						

Mapa ryzyka
dla grupy zagrożeń: naruszenie bezpieczeństwa informacji

Ocena oddziaływania	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5

Ocena prawdopodobieństwa

II. C. Ocena ryzyka dla grupy zagrożeń: awarie techniczne

LP.	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdopodobieństwa [1 – 5]	Ocena oddziaływania [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczenia
3.1						
3.2						
3.3						

Mapa ryzyka dla grupy zagrożeń: awarie techniczne

Ocena oddziaływania	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ocena prawdopodobieństwa				

II. D. Ocena ryzyka dla grupy zagrożeń: zjawiska naturalne

LP	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdopodobieństwa [1 – 5]	Ocena oddziaływania [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczenia
4.1						
4.2						
4.3						
4.4						

Mapa ryzyka dla grupy zagrożeń: zjawiska naturalne

Ocena oddziaływania	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ocena prawdopodobieństwa				

II. E. Ocena ryzyka dla grupy zagrożeń: utrata podstawowych usług

LP .	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdo- podobień- stwa [1 – 5]	Ocena oddzia- ływania [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczenia
5.1						
5.2						
5.3						
5.4						
5.5						

Mapa ryzyka dla grupy zagrożeń: utrata podstawowych usług

Ocena oddziaływania	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ocena prawdopodobieństwa				

III. F. Ocena ryzyka dla grupy zagrożeń: nieautoryzowane działania

LP.	Zagrożenie	Zastosowane zabezpieczenia	Ocena prawdopodobieństwa [1 – 5]	Ocena oddziaływan [1 – 5]	Ocena ryzyka [1 – 25]	Planowane / wdrażane dodatkowe zabezpieczeni a
6.1						
6.2						
6.3						
6.4						
6.5						
6.6						
6.7						
6.8						
6.9						
6.10						

Mapa ryzyka dla grupy zagrożeń: nieautoryzowane działania

Ocena oddziaływan ia	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ocena prawdopodobieństwa				

III. Podsumowanie

Przeprowadzona analiza ryzyka i przyjęte środki mitygujące pozwalają określić całkowite ryzyko i prawdopodobieństwo jego wystąpienia na poziomie **akceptowalnym/nieakceptowalnym** dla realizacji

.....
Należy monitorować ryzyko zgodnie z zasadami określonymi w wewnętrznych przepisach Ministerstwa Finansów dotyczących zarządzania ryzykiem teleinformatycznym, w szczególności po ujawnieniu się zdarzeń mogących wskazywać na zmaterializowanie się ryzyka

IV. Plan postępowania z ryzykiem

Lp.	Nr ryzyka	Poziom ryzyka	Sposób postępowania z ryzykiem	Opis działań	Poziom ryzyka po uwzględnieniu sposobu postępowania z ryzykiem (planowanych zabezpieczeń)	Właściciel ryzyka	Osoba/komórka organizacyjna odpowiedzialna za realizację	Planowany termin realizacji