I. I. Spis treści

II. 1. Cel

Celem procedury jest ujednolicenie sposobu identyfikacji, szacowania i traktowania ryzyk w obszarze bezpieczeństwa informacji dla usług i systemów ICT organizacji, z zapewnieniem udokumentowania wyników, powiązania ryzyk z czynnościami przetwarzania danych osobowych ujawnionymi w rejestrze czynności przetwarzania oraz cyklicznego przeglądu wyników analizy.

III. 2. Zakres stosowania

Procedura ma zastosowanie do wszystkich komórek organizacyjnych i użytkowników zaangażowanych w świadczenie usług ICT oraz do wszystkich systemów, produktów ICT, podprodukтów, zasobów i czynności przetwarzania danych osobowych objętych zadaniami związanymi z wypełnieniem arkusza „Analizy Ryzyka".

Procedura obejmuje ocenę wpływu zagrożeń na poufność, integralność i dostępność informacji, a także ocenę skutku wynikającego z niespełnienia wymogu prawnego, w szczególności wymogu wynikającego z RODO lub innych przepisów mających zastosowanie do danej usługi ICT albo czynności przetwarzania.

IV. 3. Odpowiedzialności

- Kierownik jednostki – zatwierdza wyniki analizy ryzyka oraz decyzje w sprawie postępowania z ryzykiem.
- Pełnomocnik ds. SZBI / IOD, jeżeli został wyznaczony – nadzoruje wykonanie analizy, spójność metody, rejestr ryzyk oraz zgodność identyfikacji czynności przetwarzania z rejestrem czynności przetwarzania.
- Właściciele usług, aktywów i procesów – identyfikują zagrożenia, wskazują powiązane czynności przetwarzania, oceniają wpływ, określają zabezpieczenia i proponują działania.
- Zespół IT/Bezpieczeństwa – zapewnia doradztwo merytoryczne, weryfikuje oceny techniczne, wspiera plany traktowania ryzyka oraz analizę podatności i zabezpieczeń.

V. 4. Opis postępowania

4.1. Identyfikacja

Dla każdej usługi ICT należy wskazać główne elementy wymagane do świadczenia danej usługi. Elementy te mogą obejmować aktywa osobowe, teleinformatyczne i organizacyjne, produkty ICT, podprodukty lub inne składowe, jeżeli mają wpływ na ocenę ryzyka.

W arkuszu należy wskazać, czy dana usługa, produkt ICT albo podprodukt bierze udział w czynnościach przetwarzania danych osobowych. W kolumnie „Bierze udział w czynnościach przetwarzania" należy wskazać nazwy właściwych czynności zgodnie z rejestrem czynności przetwarzania. Jeżeli dana pozycja nie bierze udziału w czynnościach przetwarzania, należy wpisać „nie dotyczy" albo równoważną informację.

Dla każdego zidentyfikowanego zagrożenia należy opisać skutki w polach „Wpływ na poufność", „Wpływ na integralność" i „Wpływ na dostępność". Dodatkowo należy wskazać, czy materializacja zagrożenia może skutkować niespełnieniem wymogu prawnego.

4.2. Ocena skutku

Dla każdego zagrożenia należy przypisać wartości liczbowe dla wpływu na atrybuty bezpieczeństwa informacji:

- Poufność (C) – możliwa wartość: 0/1.
- Integralność (I) – możliwa wartość: 0/1.
- Dostępność (A) – możliwa wartość: 0/1.

Wartość 1 oznacza istotny wpływ danego zagrożenia na dany atrybut bezpieczeństwa informacji, a wartość 0 oznacza brak istotnego wpływu.

Dodatkowo należy ocenić pole „Wymóg prawny". Wartość „TAK" oznacza, że materializacja zagrożenia może prowadzić do niespełnienia wymogu prawnego, w tym wymogu wynikającego z RODO, przepisów sektorowych, obowiązków dokumentacyjnych, terminów ustawowych, obowiązków zapewnienia rozliczalności albo innych wymogów mających zastosowanie do danej usługi lub czynności przetwarzania.

Skutek S należy ustalić według następującej zasady:

- jeżeli „Wymóg prawny" = „TAK", skutek S przyjmuje wartość 3, czyli WYSOKIE, niezależnie od wyniku C + I + A;
- jeżeli „Wymóg prawny" = „NIE", skutek S ustala się jako suma C + I + A.

Odwzorowanie wartości skutku na skalę opisową:

- 1 → MAŁE;
- 2 → ŚREDNIE;
- 3 → WYSOKIE.

Jeżeli suma C + I + A wynosi 0, pozycję należy zweryfikować pod kątem zasadności ujęcia w analizie ryzyka albo uzupełnić opis skutku, ponieważ zagrożenie ujęte w arkuszu powinno powodować co najmniej jeden istotny skutek dla bezpieczeństwa informacji, zgodności prawnej lub ciągłości działania.

Osoba odpowiedzialna za ryzyko może, na podstawie wiedzy eksperckiej i udokumentowanego uzasadnienia, dokonać korekty oceny w celu urealnienia poziomu zagrożenia. Korekta nie może obniżać skutku ustawionego na poziom 3 w przypadku niespełnienia wymogu prawnego.

4.3. Ocena prawdopodobieństwa

Określić wartość prawdopodobieństwa P na skali:

- MAŁE = 1 – zdarzenie sporadyczne albo mało realne;

- ŚREDNIE = 2 – zdarzenie możliwe;
- DUŻE = 3 – zdarzenie prawdopodobne.

Przy ocenie prawdopodobieństwa należy uwzględnić podatności, historię incydentów, w tym ujawnionych poza Organizacją/Urzędem, wiedzę ekspercką, charakter czynności przetwarzania, kategorie danych, skalę przetwarzania oraz wdrożone zabezpieczenia.

4.4. Ocena ryzyka

Posiadając wiedzę na temat skutków danego zdarzenia oraz prawdopodobieństwa jego wystąpienia należy wyliczyć wartość ryzyka R według następującego wzoru:

R = P × S

Następnie należy przypisać poziomy ryzyka:

- 1–2 → MAŁE;
- 3–4 → ŚREDNIE;
- 6–9 → WYSOKIE.

Macierz Ryzyka (P × S)

RYZYKO	1 - MAŁE	2 - ŚREDNIE	3 - WYSOKIE
1 - MAŁE	1 - MAŁE	2 - MAŁE	3 - ŚREDNIE
2 - ŚREDNIE	2 - MAŁE	4 - ŚREDNIE	6 - WYSOKIE
3 - DUŻE	3 - ŚREDNIE	6 - WYSOKIE	9 - WYSOKIE

Legenda macierzy: MAŁE – akceptowalne; ŚREDNIE – wymagają planu działań; WYSOKIE – wymagają natychmiastowych działań i nadzoru kierownictwa.

4.5. Właściciele ryzyka

Dla każdego ryzyka należy wskazać właściciela. Właściciel ryzyka bierze udział w analizie ryzyka oraz jest merytorycznie odpowiedzialny za obszar jego występowania, w tym za obszar biznesowy, usługę ICT, aktywo, produkt ICT albo czynność przetwarzania powiązaną z ryzykiem.

Właściciel ryzyka odpowiada za:

- udział w analizie ryzyka, w szczególności określenie zagrożeń i powiązanych czynności przetwarzania;
- weryfikację oceny ryzyka, w tym ocenę skutku prawnego;
- nadzór nad mechanizmami mitygacji ryzyka;
- zapewnienie, że działania ograniczające ryzyko są adekwatne do poziomu ryzyka oraz wymogów prawnych.

Zaleca się, aby właścicielem ryzyka był właściciel aktywa, usługi, procesu albo czynności przetwarzania, w ramach której występuje ryzyko.

4.6. Postępowanie z ryzykiem

Dla ryzyk ŚREDNICH i WYSOKICH należy określić działania, takie jak redukcja, unikanie albo przeniesienie ryzyka, ze wskazaniem właściciela ryzyka, terminu realizacji i miernika efektu lub postępu.

Ryzyka MAŁE można akceptować, przy czym akceptację należy odnotować w arkuszu.

W przypadku ryzyk, dla których skutek został ustawiony na poziom 3 z powodu niespełnienia wymogu prawnego, plan postępowania z ryzykiem powinien obejmować także działania zapewniające zgodność, na przykład aktualizację procedur, rejestru czynności przetwarzania, obowiązków informacyjnych, umów powierzenia, upoważnień, retencji danych, zabezpieczeń technicznych albo zasad dokumentowania rozliczalności.

Sposób postępowania z ryzykiem musi zostać zatwierdzony przez ……

4.7. Zatwierdzanie i przeglądy

Wyniki analizy zatwierdza …….. Przegląd skuteczności i aktualizacja ocen odbywa się co najmniej raz w roku oraz po istotnych zmianach, incydentach, zmianach w systemach ICT, zmianach w czynnościach przetwarzania albo zmianach wymogów prawnych mających wpływ na ocenę ryzyka.

4.8. Instrukcja wypełniania arkusza - wersja skrócona

1) Pola podstawowe

- Wypełnij kolejno: Lp., Usługa ICT, Proponowane produkty ICT, Podprodukty, jeżeli występują, Bierze udział w czynnościach przetwarzania, Zagrożenie.
- W polu „Bierze udział w czynnościach przetwarzania” wskaż nazwy czynności zgodnie z rejestrem czynności przetwarzania. Jeżeli nie dotyczy, wpisz „nie dotyczy”.
- Opisz krótko skutki w polach: „Wpływ na poufność”, „Wpływ na integralność”, „Wpływ na dostępność”.

2) Zaznacz wpływ CIA oraz wymóg prawny

- Dla poufności, integralności i dostępności wpisz 1, jeżeli wpływ jest istotny, albo 0, jeżeli brak istotnego wpływu.
- W kolumnie „Wymóg prawny” wybierz „TAK”, jeżeli zagrożenie może spowodować niespełnienie wymogu prawnego. W takim przypadku skutek zostaje ustawiony na 3, czyli WYSOKIE.
- Formuła stosowana w arkuszu: jeżeli „Wymóg prawny” = „TAK”, S = 3; w przeciwnym razie S = C + I + A.

3) Ustal prawdopodobieństwo (P)

- Wybierz z listy: MAŁE = 1, ŚREDNIE = 2, DUŻE = 3.

4) Oblicz ryzyko (R)

- Formuła: R = P × S.
- Poziomy: 1–2 → MAŁE, 3–4 → ŚREDNIE, 6–9 → WYSOKIE.

5) Działania

- W „Stosowane zabezpieczenia” wpisz istniejące środki.
- W „Mitygacja ryzyka” opisz plan działania: co należy zrobić, kto odpowiada, do kiedy oraz jaki miernik potwierdzi realizację.
- Ryzyka MAŁE można zaakceptować. Ryzyka ŚREDNIE i WYSOKIE wymagają zaplanowania redukcji, przeniesienia albo unikania ryzyka.
- Dla ryzyk wynikających z niespełnienia wymogu prawnego uwzględnij działania zapewniające zgodność z RODO, rejestrem czynności przetwarzania i innymi właściwymi przepisami.

6) Zatwierdzenie i przeglądy

- Przekaż analizę do zatwierdzenia Kierownikowi jednostki albo innej wskazanej osobie.
- Przegląd i aktualizacja: co najmniej raz w roku oraz po istotnych zmianach, incydentach lub zmianach wymogów prawnych.

VI.5. Dokumenty związane

- Polityka bezpieczeństwa informacji.
- Rejestr czynności przetwarzania.
- Dokumentacja ochrony danych osobowych, w tym dokumenty potwierdzające spełnienie obowiązków wynikających z RODO.

VII. 6. Załączniki

- Arkusz szacowania ryzyka (MS Excel).

VIII. II. KARTA ZMIAN

Wersja	Zmiana	Autor	Opis modyfikacji	Zaakceptował	Data
1	1		Dostosowanie procedury do arkusza: dodanie czynności przetwarzania zgodnie z RCP oraz zasady skutku S = 3 dla niespełnienia wymogu prawnego.		