Procedura analizy ryzyka

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Zagrożenie – Czynnik, działanie (zewnętrzne lub wewnętrzne, wywołane lub samoistne), poszukujące możliwych do wykorzystania podatności określonego składnika aktywów.
3. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Incydent jest istotny, gdy narusza lub może naruszać prawa i wolności osób, których dane dotyczą, w kontekście poufności, integralności i dostępności.
4. Skutki - rezultaty niepożądanego incydentu (stopień naruszenia praw i wolności osób, których dane dotyczą)
5. Ryzyko – Wartość stanowiąca iloczyn prawdopodobieństwa i skutku.

1 WYZNACZENIE ZBIORÓW DO ANALIZY RYZYKA Z AKTYWAMI

1. Analizie ryzyka poddawane są czynności (procesy) przetwarzania

Czynności przetwarzania często odpowiadają obecnym zbiorom danych osobowych (np. Zbiór Zleceniodawców i Zamawiających), ale już proces „Przetwarzanie danych osobowych występujących w tłumaczonych dokumentach" stanowi odrębną czynność (proces) przetwarzania, choć nie jest zbiorem danych z uwagi na brak struktury i uporządkowania.

2. Do analizy wymagane jest zidentyfikowanie aktywów i uwzględnienie ich w opisie zagrożeń. To aktywa są miejscem, gdzie występują podatności (luki), które są wykorzystywane przez zagrożenia. Aktywów należy poszukiwać w następujących grupach:
    a. Infrastruktura twarda (budynek, pomieszczenie, samochód)
    b. Media (prąd, Internet)
    c. Infrastruktura IT (sieć, WiFI)
    d. Sprzęt (komputer, router, telefon, drukarka)
    e. Oprogramowanie (System operacyjny, aplikacja)
    f. Ludzie (tłumacz, asystent)
    g. Outsourcing (informatyk, księgowa, inny tłumacz)

2 WYZNACZENIE ZAGROŻEŃ

1. Administrator jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do podatności rozmaitych aktywów, w kontekście potencjalnego naruszenia poufności, integralności lub dostępności. W praktyce są to *czarne scenariusze* w odniesieniu do danych osobowych.

3 WYLICZENIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń (w kontekście potencjalnych podatności konkretnych aktywów w procesie przetwarzania).
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając stopień naruszenia praw i wolności osób, których dane dotyczą.
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (**R**) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A - PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B - SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe	1
średnie	2
duże	3

4 PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZYKIEM

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

5 REAKCJA NA WARTOŚĆ RYZYKA

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)
    c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę)

6 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

7 PONOWNA ANALIZA RYZYKA

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 3 lata.