

SPIS TREŚCI.

1. Wstęp	2
2. Analiza ryzyka	2
2.1 Definicje	2
2.2 Rejestr czynności przetwarzania (inwentaryzacja danych osobowych)	2
2.3 Wyznaczenie zagrożeń	2
2.4 Wyliczenie ryzyka dla zagrożeń	2
2.5 Plan postępowania z ryzykiem	3
3. Upoważnienia	3
4. Środki techniczne i organizacyjne zabezpieczające dane osobowe	4
5. Regulamin Ochrony Danych Osobowych	4
6. Instrukcja postępowania z incydentami	4

1. Wstęp.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2. Analiza ryzyka.

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla grupy zbiorów dla procesów przetwarzania.

2.1 Definicje.

2.1.1 Aktywa - środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.

2.1.2 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.

2.1.3 Zagrożenie - potencjalne naruszenie (potencjalny incydent).

2.1.4 Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).

2.1.5 Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów.

2.2 Rejestr czynności przetwarzania (inventaryzacja danych osobowych).

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

2.3 Wyznaczenie zagrożeń.

2.3.1 Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.

2.3.2 Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów oraz procesów przetwarzania.

2.4 Wyliczenie ryzyka dla zagrożeń.

2.4.1 **Na podstawie „Arkusza analizy ryzyka RODO”** Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.

2.4.2 Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.

2.4.3 Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.

2.4.4 Proponowaną skalę skutków prezentuje Tabela B.

2.4.5 Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków wg formuły:

$$R = P * S.$$

Tabela A

PRAWDOPODOBIENSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B

SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10 000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

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 (akceptowalne)	1-2
ryzyko jest opcjonalne (akceptowalne albo należy obniżyć)	3-6
ryzyko jest nieakceptowalne (należy obniżyć)	9

Reakcja na wartość ryzyka.

1. Akceptacja ryzyka 0 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.
3. Redukcja - zastosowanie zabezpieczeń w celu obniżenia ryzyka.
4. Analizę ryzyka **odnotowuje się w „Rejestrze czynności przetwarzania”**.

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)

2.5 Plan postępowania z ryzykiem.

- 2.5.1 Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne. Informacje te zapisane są w planie postępowania z ryzykiem.
- 2.5.2 Administrator zobowiązany jest do **nadzorowania wdrożonych** zabezpieczeń.

3. Upoważnienia.

- 3.1 Administrator odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
- 3.2 Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
- 3.3 W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego.

4. Środki techniczne i organizacyjne zabezpieczające dane osobowe.

- 4.1 Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych opisanych w Instrukcji zarządzania RODO.
- 4.2 W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
- 4.3 Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

5. Regulamin Ochrony Danych Osobowych.

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności.

6. Instrukcja postępowania z incydentami.

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

- 6.1 Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego oraz Inspektora Ochrony Danych.
- 6.2 Do typowych podatności bezpieczeństwa danych osobowych należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekami, kradzieżami i utratą danych osobowych,
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
- 6.3 Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dyski, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych / sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
- 6.4 W przypadku stwierdzenia wystąpienia incydentu Inspektor Ochrony Danych Osobowych prowadzi postępowanie wyjaśniające w toku, którego:
 - a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
 - b. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
 - c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
- 6.5 Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

- 6.6 Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
- 6.7 W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu.

- KONIEC -