ANALIZA RYZYKA

PRZETWARZANIA DANYCH

OSOBOWYCH

DLA

Zawartość

I. INFORMACJE OGÓLNE

Niniejsza analiza odnosi się zarówno do danych zwykłych jak i danych wrażliwych, przetwarzanych przez Administratora dla działalności

---

Mając na uwadze Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L. Nr 119, str. 1, dalej jako RODO), w szczególności art. 24 ust. 1 RODO, art. 32 ust. 1, 2 i 4 RODO, oraz Motywy 74-78 RODO każdy Administrator danych osobowych, w celu zachowania bezpieczeństwa

i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem, **musi samodzielnie oszacować ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą,** oraz wdrożyć środki bezpieczeństwa minimalizujące to ryzyko**.**

Przyjmuje się, że Administrator przetwarzając dane powinien stosować podejście oparte na ryzyku (*risked base approach*).

Zgodnie z nią, Administrator powinien uwzględnić ryzyko naruszenia praw lub wolności podmiotów danych i jego wpływ na prywatność w zależności od charakteru, zakresu, kontekstu i celów przetwarzania danych, a także ryzyko wpływające na interesy Administratora. Zasada ta jest stosowana względem przetwarzania już w fazie projektowania (*privacy by design)* wraz z domyślną ochroną danych (*privacy by default)*, co pozwala na właściwą ocenę zagrożeń i skupienie się na najbardziej ryzykownych operacjach przetwarzania danych. Podejście oparte na ryzyku rozpoczyna się od analizy ryzyka ogólnego, które pozwala określić konieczność przeprowadzenia pełnej oceny skutków dla ochrony danych.

Ogólne rozporządzenie o ochronie danych (RODO) nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników. Wskazuje się jednak na konieczność zapewniania m. in. poufności, integralności oraz dostępności systemów, w których przetwarza się dane osobowe.

Odnosząc się do ww. czynników, odwołać należy się do szacowania ryzyka w procesie dotyczącym przetwarzania informacji. W normie dotyczącej systemowego zarządzania bezpieczeństwem informacji ISO/IEC 27005 definiuje się bezpieczeństwo informacji jako zachowanie trzech cech, tj. poufności, spójności (inaczej integralności) oraz dostępności informacji. Zatem, biorąc pod uwagę brak regulacji dotyczących szczegółów ogólnego szacowania ryzyka związanego z przetwarzaniem danych osobowych za podstawę można przyjąć elementy metod i norm stosowanych w systemach dot. zarządzania bezpieczeństwem informacji.

W związku z powyższym, Administrator dokonuje samodzielnie oceny ryzyka dla praw i wolności osób fizycznych w zakresie bezpieczeństwa przetwarzania danych osobowych, stosując podejście oparte na ryzyku „*risked base approach*”, a w sytuacji, gdy pojawi się

wysoki stopień ryzyka naruszenia praw i wolności osób, których dane dotyczą, Administrator dokona oceny skutków dla ochrony danych zgodnie z art. 35 RODO (*DPIA - data protection impact assesment*).

ETAP 1: USTALENIE KONTEKSTU

Ustanowienie kontekstu to określenie wszystkich informacji i uwarunkowań związanych z działaniem organizacji.

W ramach przeprowadzanego audytu dokonana została analiza w celu określenia informacji i uwarunkowań związanych z działaniem organizacji w zakresie przetwarzania danych osobowych, biorąc pod uwagę informacje wewnętrzne i zewnętrzne [patrz dokument „Identyfikacja danych osobowych" oraz „Lista kontrolna - pomocnicze pytania audytowe"].

ETAP 2: MECHANIZMY KONTROLNE

W ramach tego etapu, Administrator zidentyfikował zastosowane środki bezpieczeństwa i mechanizmy kontrolne mające na celu spełnienie wymagań biznesowych, prawnych i innych ograniczeń dla procesów przetwarzania danych, w tym danych osobowych.

Dla każdego zidentyfikowanego procesu przetwarzania, Administrator sprawdził czy dane osobowe są przetwarzane:

- zgodnie z zasadami wyrażonymi w art. 5 RODO, a w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych w art. 44-49 RODO,
- na podstawie jednej z przesłanek wskazanych w art. 6-10 RODO,
- przy zapewnieniu osobom, których dane dotyczą, możliwości realizacji ich praw wskazanych w art. 12-22 RODO.

W tym celu określił:

- cele przetwarzania danych osobowych oraz podstawy prawne,

- wymagania dotyczące przejrzystości informacji udzielanych osobom, których dane dotyczą, na temat przetwarzania ich danych osobowych oraz ułatwiania im wykonania ich praw,
- źródła i sposoby pozyskiwania danych oraz przepływy danych w czasie ich przetwarzania,
- wymagania w zakresie jakości przetwarzanych danych oraz weryfikacja tej jakości,
- czas przez jaki dane będą przetwarzane.

ETAP 3: SZACOWANIE RYZYKA

oraz

ETAP 4: POSTĘPOWANIE Z RYZYKIEM

W ramach szacowania ryzyka, dla każdego zidentyfikowanego zagrożenia, wykonywana jest ocena prawdopodobieństwa jego zajścia oraz szacowanie skutków jego zmaterializowania się. Mając wyznaczone prawdopodobieństwo wystąpienia określonego zdarzenia oraz straty, jakie mogą być nim spowodowane, wyznacza się wartość ryzyka jako iloczyn prawdopodobieństwa wystąpienia danego zdarzenia i jego skutku.

1. **SKUTKI WYSTĄPIENIA RYZYKA ZE WZGLĘDU NA FINANSE I REPUTACJĘ/ WIZERUNEK FIRMY – Oszacuj co się stanie, gdy to się zdarzy**

Skutek	Poziom	Wartość/ finanse/ strata finansowa	Wpływ na reputacje
Bardzo wysoki	5	Powyżej 1 mln zł	Negatywne opinie w mediach międzynarodowych, stale pojawiają się negatywne opinie

			klientów lub pracowników w mediach o dużym zasięgu
Wysoki	4	W zakresie 500 tys. Zł – 1 mln zł	Negatywne opinie w mediach krajowych, bardzo często pojawiają się negatywne opinie klientów lub pracowników o zasięgu krajowym, w mediach społecznościowych, lokalnych
Średni	3	W zakresie 100- 500 tys. zł	Negatywne opinie w mediach lokalnych, często zdarzają się negatywne opinie klientów lub pracowników
Niski	2	W zakresie 5 – 100 tys. zł	Negatywne opinie bez udziału mediów, mogą pojawić się negatywne opinie klientów lub pracowników
Bardzo niski	1	Poniżej 5 tysięcy zł	Brak wpływu na reputacje

2. <u>OCEŃ PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZDARZENIA – Na ile jest to realne?</u>

Prawdopodobieństwo	Poziom	Skala
Nieprawdopodobne	1	Zdarzenie jest nieprawdopodobne – zdarzenie, nie wystąpiło w ogóle lub występuje rzadziej niż raz w roku
Mało prawdopodobne	2	Zdarzenie jest mało prawdopodobne – zdarzenie występuje co najmniej raz na rok
Możliwe	3	Zdarzenie jest możliwe – zdarzenie występuje co najmniej raz na kwartał
Prawdopodobne	4	Zdarzenie jest prawdopodobne – zdarzenie występuje co najmniej raz w miesiącu
Bardzo prawdopodobne	5	Zdarzenie jest bardzo prawdopodobne – zdarzenie występuje co najmniej raz w tygodniu

LEGENDA:

P - Prawdopodobieństwo incydentu (skala od 1 do 5)

S - Skutki wystąpienia incydentu (skala od 1 do 5)

R – Ryzyko wystąpienia incydentu (Niskie, Średnie, Wysokie, Krytyczne), R = P*S

Gdzie:

1. **Prawdopodobieństwo niskie / Skutki bardzo niskie**
2. **Prawdopodobieństwo mało prawdopodobne / Skutki mało prawdopodobne**
3. **Prawdopodobieństwo możliwe / Skutki średnie**
4. **Prawdopodobieństwo prawdopodobne / Skutki wysokie**
5. **Prawdopodobieństwo bardzo wysokie / Skutki bardzo wysokie**

3. **<u>POZIOM RYZYKA – Ustal za pomocą macierzy (skutek x prawdopodobieństwo)</u>**

RYZYKO			SKUTKI				
			Bardzo niskie	Mało prawdo-podobne	Średnie	Wysokie	Bardzo wysokie
			1	2	3	4	5
PRAW-DOPO-	Niskie	1	Niskie	Niskie	Średnie	Wysokie	Wysokie
	Mało prawdopodobne	2	Niskie	Średnie	Średnie	Wysokie	Wysokie

	Możliwe	3	Niskie	Średnie	Wysokie	Wysokie	Krytyczne
	Prawdopodobne	4	Średnie	Wysokie	Wysokie	Krytyczne	Krytyczne
	Bardzo wysokie prawdopodobieństwo (prawie pewne)	5	Średnie	Wysokie	Krytyczne	Krytyczne	Krytyczne

4. **POZIOM RYZYKA I POSTĘPOWANIE Z RYZYKIEM ORAZ MOŻLIWE REAKCJE – Ustal plan**

POZIOM RYZYKA	PODEJMOWANE DZIAŁANIE
Niski (N)	Działania podejmowane są w zależności od dostępności zasobów i nakładów – poziom ryzyka akceptowalny
Średni (Ś)	Działanie może zostać przesunięte w czasie, ale ryzyko wymaga okresowego monitorowania – poziom ryzyka nieakceptowalny
Wysoki (W)	Działanie może zostać przesunięte w czasie, ale ryzyko wymaga stałego monitorowania – poziom ryzyka nieakceptowalny
Krytyczny (K)	Działanie jest wymagane natychmiast – wymaga natychmiastowego działania

Przejdź do tabeli poniżej.

Lp.	Obszar/ aktywa	Zagrożenie *(„Z powodu …”)*	Opis zagrożenia, po datności i/lub skutków *(„… istnieje ryzyko, że … wskutek czego …”)*	Prawdopodo-bieństwo (w skali od 1 do 5)	Skutki (w skali od 1 do 5)	Ryzyko (ocena według macierzy ryzyka)	Zabezpieczenia i po stępowanie z ryzykiem (opis)
1.	Sprzęt	Złamanie haseł do nośników danych osobowych np. komputer, tablet, smartfon, baza danych w „chmurze”, pendrive, dyski ze wnętrzne.	Zagrożenie to może nastąpić w sytuacji używania mało skomplikowanych haseł, zbyt rzadkiego zmieniania haseł, braku kontroli nad użytkownikami. Powoduje brak dostępu do danych, ryzyko ich ewentualnej modyfikacji przez osoby trzecie, ryzyko braku możliwości realizacji usług.				**Procedura:** Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym **Zabezpieczenia:** Polityka czystego pulpitu / ekranu, Polityka zmiany haseł zawarta w Instrukcji Zarządzania Systemem Informatycznym, Szyfrowanie danych, Zastosowanie certyfikatu SSL,

							Stosowanie programów antywirusowych.

2.	Pomieszczenia/ Sprzęt	Nieograniczony dostęp do danych lub włamanie do pomieszczeń	Zagrożenie to może nastąpić w sytuacji używania mało skomplikowanych haseł, zbyt rzadkiego zmieniania haseł, braku kontroli nad użytkownikami. Powoduje brak dostępu do danych, ryzyko ich ewentualnej modyfikacji przez osoby trzecie, ryzyko braku możliwości realizacji usług.				**Procedura:** Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym **Zabezpieczenia:** Polityka czystego pulpitu/ ekranu, Polityka zmiany haseł zawarta w Instrukcji Zarządzania Systemem Informatycznym, Regularne wykonywanie kopii zapasowych przechowywanych w zamkniętej *metalowej/ niemetalowej* szafie, Stosowanie programów antywirusowych.

3.	Pomieszczenia/ Sprzęt	Zalanie	Ryzyko trwałej utraty wszystkich danych lub danych niezapisanych trwale na dysku, brak możliwości realizacji usług, brak możliwości odzyskania danych.				**Procedura:** Instrukcje postępowania BHP **Zabezpieczenia:** Wprowadzenie zakazu spożywania posiłków na biurku, Niepozostawianie urządzeń narażonych na zalanie otwartych po zakończeniu pracy, Szkolenie BHP, Instruktaż stanowiskowy.
4.	Pomieszczenia/ Sprzęt	Pożar/ eksplozja	Ryzyko trwałej utraty wszystkich danych lub danych niezapisanych trwale na dysku, brak możliwości realizacji usług, brak możliwości odzyskania danych.				**Procedura:** Instrukcje postępowania BHP **Zabezpieczenia:** Szkolenie BHP, Instruktaż stanowiskowy, Wyposażenie przeciwpo-

							żarowe np. wolnostojąca gaśnica,
5.	Pomiesz-czenia/ Sprzęt	Awarie zasilania, uszkodzenia elementów IT	Ryzyko trwałej utraty wszystkich danych lub danych niezapisanych trwale na dysku, brak możliwości realizacji usług, brak możliwości odzyskania danych.				**Procedura:** Instrukcje postępowania BHP **Zabezpieczenia:** Szkolenie BHP, Instruktaż stanowiskowy

6.	Procedury	Nieprzestrzeganie procedur	Ryzyko naruszenia ochrony danych osobowych, ich utraty, wykradnięcia i innych przypadków sprzecznych z Polityka Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informa tycznym.				**Procedura:** Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym **Zabezpieczenia:** Okresowe szkolenia w zakresie ochrony danych osobowych i zapoznanie z przepisami, Szkolenia zewnętrzne w zakresie ochrony danych osobowych, Szkolenia w zakresie zabezpieczeń systemu informatycznego.

7.	Personel	Wykradnięcie lub wyniesienie danych przez pracowników	Pracownicy lub osoby zatrudnione na podstawie umów cywilnoprawnych mogą wykraść dane klientów/ pracowników/ dostawców Administratora i wykorzystać je w celach własnych. Ryzyko sprzedaży tych danych osobom trzecim, przekazanie danych do konkurencji, wykorzystanie danych dla własnych korzyści, Naruszenie praw osób, których dane dotyczą.				**Procedury:** ….. **Zabezpieczenia:** Każda osoba, poza Administratorem, jest zobowiązana do przestrzegania ww. procedur. Zobowiązana jest do podpisania oświadczenia o poufności, oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych, podpisania stosownych upoważnień. Niektóre osoby zobowiązane są dodatkowo do podpisania umowy o poufności. Okresowe szkolenia w zakresie ochrony danych osobowych i zapoznanie z przepisami,

							Szkolenia zewnętrzne w zakresie ochrony danych osobowych, Szkolenia w zakresie zabezpieczeń systemu informatycznego. Pomieszczenia wyposażone są w system alarmowy antywłamaniowy, Szyfrowanie danych.

8.	Personel/ Podmioty trzecie	Wyciek danych klientów i/ lub pracowników przekazywanych do „chmury”, w tym dostarczanej przez podmioty trzecie, z państw trzecich.	Dane klientów utrwalane są w pliku elektronicznym, w tzw. „chmurze”, dostarczanej przez korporacje międzynarodowe. Istnieje ryzyko niewłaściwego zabezpieczenia tych danych i ich wycieku.				**Procedura:** Polityka bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym **Zabezpieczenia:** Ograniczanie przechowywania danych w „chmurze”, Wybieranie sprawdzonych dostawców „chmury”, Szczegółowa analiza regulaminu dostawcy usługi „chmury” .

9.	Sprzęt/ Podmioty trzecie	Utrata urządzenia zawierającego dane zwykłe i wrażliwe, pozostawienie urządzenia bez nadzoru, kradzież urządzenia, zagubienie	Osoby, które mogą odnaleźć urządzenie/ które ukradną urządzenie będą mieć nieograniczony dostęp do wszystkich danych na nim zgromadzonych, utrata tych danych przez Administratora, ujawnienie ich osobom trzecim.				**Procedura:** Polityka bezpieczeństwa – procedura używania urządzeń mobilnych **Zabezpieczenia:** Szyfrowanie dysku, Zakaz przetwarzania danych na urządzeniach mobilnych. Regularne wykonywanie kopii zapasowych, Szyfrowanie danych.
10.	Pomieszczenia	Pojawienie się osób nieupoważnionych w obszarze przetwarzania danych osobowych i uzyskanie dostępu do danych osobowych	Osoby, które mogą znaleźć się w obszarze danych lub uzyskać do nich dostęp będą mieć nieograniczony dostęp do wszystkich danych na nim zgromadzonych. Istnieje ryzyko utraty tych danych przez Administra-				**Procedura:** Procedura zgłaszania naruszeń ochrony danych **Zabezpieczenia:** Wykonanie szkoleń pracowników Dalsze monitorowanie

			tora, czy ujawnienie ich osobom trzecim.				ryzyka Dalsze utrzymanie monitoringu lub ochrony.
	Sieć	Phishing, cybersquatting (podrabianie stron)					**Procedura:** Procedura zgłaszania naruszeń ochrony danych Polityka bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym **Zabezpieczenia:** Utrzymywanie świadomości pracowników o zagrożeniach z sieci. Możliwe skorzystanie z metod prowadzenia tzw. symulacji phishingowych. Wdrożenie pro-

							cedury zgłaszania naruszeń ochrony danych osobowych.
		Inne – jakie?					**Procedura:** ….. **Zabezpieczenia:**
		Inne – jakie?					**Procedura:** ….. **Zabezpieczenia:**
		Inne – jakie?					**Procedura:** ….. **Zabezpieczenia:**

ETAP 5: USTALENIE CZY PRZEPROWADZENIE OCENY SKUTKÓW JEST WYMAGANE

Przepisy Ogólnego rozporządzenia o ochronie danych (RODO) nie wymagają przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do każdej operacji przetwarzania, która może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe wyłącznie w przypadku, gdy przetwarzanie „może powodować wysokie ryzyko naruszenia prawi i wolności osób fizycznych", zgodnie z art. 35 ust. 1,3 i 4 RODO.

Administrator dokonuje oceny czy przeprowadzenie oceny skutków dla ochrony danych jest konieczne na podstawie art. 35 ust. 1,3 i 4 RODO oraz na podstawie Motywu 75 RODO.

Przesłanka	**Czy występuje u Administratora?**	**Czy wskazuje na konieczność przeprowadzenia oceny skutków dla ochrony danych?**
Dany rodzaj przetwarzania został wskazany w przepisie prawa, np. w art. 35 ust. 3 RODO	NIE	NIE
Dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust. 4 RODO	NIE	NIE
Poziom ryzyka określony został jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, kontekstu i celów przetwarzania	NIE	NIE

Z analizy dokonanej przez Administratora wynika, iż nie ma on obowiązku przeprowadzenia oceny skutków dla ochrony danych w swojej działalności

---

[data i podpis Administratora Danych]