……./……/2022

Katowice, dnia 17.11.2022r.

SUGESTIA Nr 21009
Inspektora Ochrony Danych

Dot. analiza ryzyka w czynności przetwarzania.

Zgodnie z przepisami ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 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) a szczególności art. 39 pkt 1 lit a oraz motywem (77) sugeruje się:

w procesie przeprowadzenia analizy ryzyka za część arkusza ***Matryca ryzyka XYZ*** *„czynności przetwarzania danych”* należy uwzględnić następujący proces obliczenia współczynnika prawdopodobieństwa:

etap 1

obejmuje opisane poziomy oddziaływania, które obejmują trzy poziomy: niski, średni i wysoki. Oceny dokonujemy w czterech głównych obszarach, jeżeli chodzi o bezpieczeństwo danych tj.

A. Sieci i zasoby techniczne;
B. Procesy i procedury;
C. Strony i ludzie zaangażowani w operację;
D. Sektor i skala działalności.

W odniesieniu do każdego z obszarów zadajemy pięć pytań a odpowiedź twierdząca oznacza jeden punkt. Pytania te są zawarte w tabeli:

A. Sieci i zasoby techniczne;	B. Procesy i procedury;	C. Strony i ludzie zaangażowani w operację;	D. Sektor i skala działalności
1.Czy jakakolwiek część przetwarzania danych odbywa się przez internet?	6.Czy rola i obowiązki dotyczące przetwarzania danych są niejednoznaczne lub niejasno zdefiniowane?	11.Czy przetwarzania danych wykonywane jest przez nieokreśloną liczbę pracowników lub więcej niż 1/3 stanu komórki organizacyjnej?	16.Czy uważasz swój sektor/obszar działalności za podatny na cyberataki?
2.Czy można zapewnić dostęp do wewnętrznego systemu przetwarzania danych osobowych przez internet (np. dla pewnych użytkowników lub grup użytkowników)?	7.Czy możliwe do zaakceptowania użytkowanie sieci, systemu i zasobów fizycznych w ramach organizacji jest dwuznaczne lub niejasno zdefiniowane?	12.Czy jakakolwiek część operacji przetwarzania danych wykonywana jest przez wykonawcę/stronę trzecią (podmiot przetwarzający dane)?	17.Czy twoja komórka/organizacja ucierpiała z powodu cyberataku lub innego naruszenia bezpieczeństwa w ciągu ostatnich dwóch lat?
3.Czy system przetwarzania danych osobowych jest powiązany z innym wewnętrznym (w ramach organizacji) lub zewnętrznym systemem lub serwisem informatycznym?	8.Czy pracownikom wolno wnosić i użytkować swoje własne urządzenia podłączone do systemu przetwarzania danych osobowych?	13.Czy obowiązki stron/osób uczestniczących w przetwarzaniu danych osobowych są niejednoznaczne lub niejasno ustalone?	18.Czy w ostatnim roku otrzymałeś zgłoszenia i/lub skargi dotyczące bezpieczeństwa systemu informatycznego (wykorzystywanego do przetwarzania danych osobowych)?
4.Czy nieupoważnione osoby mogą łatwo uzyskać dostęp do środowiska przetwarzania danych?	9.Czy pracownikom wolno przekazywać, przechowywać lub w inny sposób przetwarzać dane osobowe poza obiektami organizacji?	14.Czy pracownicy uczestniczący w przetwarzaniu danych osobowych nie znają zasad bezpieczeństwa informacji?	19.Czy operacja przetwarzania dotyczy dużej ilości jednostek i/lub danych osobowych?
5.Czy system przetwarzania danych osobowych został zaprojektowany, wdrożony lub jest utrzymywany bez przestrzegania odpowiednich dobrych praktyk?	10.Czy czynności przetwarzania danych osobowych mogą być wykonywane bez utworzenia plików dziennika/rejestr dokumentów?	15.Czy osoby/strony uczestniczące w operacji przetwarzania danych osobowych zaniedbują bezpieczne przechowywanie i/lub niszczenie danych osobowych?	20.Czy istnieją jakiekolwiek dobre praktyki z zakresu bezpieczeństwa dotyczące konkretnie twojego sektora /obszaru działalności, które nie są właściwie stosowane?

DZIAŁ ……

etap 2

Sumujemy punkty w każdym obszarze od A do D i określamy poziom oraz wynik zgodnie z tabelą:

Obszar oceny:	Liczba odpowiedzi „tak”	Poziom	Wynik
A. Sieć i zasoby techniczne:	0-1	Niski	**1**
	2-3	Średni	**2**
	4-5	Wysoki	**3**
B. Procesy i procedury:	0-1	Niski	**1**
	2-3	Średni	**2**
	4-5	Wysoki	**3**
C. Strony i ludzi zaangażowani w operację:	0-1	Niski	**1**
	2-3	Średni	**2**
	4-5	Wysoki	**3**
D. Sektor i skala działalności:	0-1	Niski	**1**
	2-3	Średni	**2**
	4-5	Wysoki	**3**

etap 3

Otrzymane **wyniki** w etapie 2 sumujemy i kwalifikujemy poziom współczynnika prawdopodobieństwa wystąpienia zagrożenia w zgodzie z tabelą:

Ogólna SUMA wyników:	Współczynnik prawdopodobieństwa	Wartość
4 - 5	Rzadkie i mało prawdopodobne	1
6 - 8	Możliwe	3
9 - 12	Pewne/prawie pewne	5

etap 4

Wartość współczynnika zapisujemy w arkuszu *Matrycy ryzyk „czynności przetwarzania danych”* kolumna E przy analizowanej czynności przetwarzania, bez zapisu zagrożenia kolumna B a w podatności kolumna D zapisujemy *zgodnie z sugestią nr 21009*, co przedstawiono na rysunku poniżej:

Nazwa czynności	Zagrożenie	Podatność (zaznacz pomocniczo, jeśli występuje)		Współczynnik prawdopodobieństwa	Współczynnik skutku	Współczynnik ryzyka	Zalecenia
Przeprowadzanie rekrutacji			Wyliczone zgodnie z Sugestią nr 21009	1	3	3	

Na tym kończymy czynność wyliczenia ***współczynnika prawdopodobieństwa*** dla czynności przetwarzania. Natomiast w przypadku otrzymania żółtych i czerwonych pól w kolumnie G *współczynnik ryzyka*, wpisujemy do kolumny H *Zalecenia* propozycje działań lub czynności w odniesieniu do wszystkich obszarów, których poziom oceniono na ***Średni*** lub ***Wysoki***. W przypadku kiedy wszystkie obszary dały ***Niski*** poziom, to *Zalecenia* ograniczają się tylko do wniosków z oceny współczynnika skutku.

Proces, opisany powyżej, należy powtórzyć dla wszystkich zdefiniowanych czynności przetwarzania, które oceniamy w analizie ryzyka. Przy obliczaniu parametrów czynności przetwarzania w odniesieniu do zidentyfikowanych zagrożeń korzystamy z arkusza. Wtedy możemy obliczyć wartość średnią z zagrożeń, co pokazano na rysunku:

Nazwa czynności	Zagrożenie	Podatność (zaznacz pomocniczo, jeśli występuje)		Współczynnik prawdopodobieństwa	Współczynnik skutku	Współczynnik ryzyka	Zalecenia
Przeprowadzanie rekrutacji			Wyliczone zgodnie z Sugestią nr 21009	1	3	3	
	Wartość średnia z zagrożeń 3,25 i 3			3	3	9	
	Może poskutkować dyskryminacją	X	przetwarzanie zdjęć w CV w czasie rekrutacji	3	3	9	wprowadzić instrukcje w tym zakresie

Brak zapisu oznacza, że w procesie oceny wykorzystano inny opisany w analizie ryzyka mechanizm.

Inspektor
Ochrony Danych

……