pieczątka

Załącznik nr 5

do Zarządzenia nr 5/2021
Przewodniczącego Zarządu
Związku Gmin Krajny
z dnia 2 listopada 2021 r.

Procedura analizy i szacowania ryzyka w zakresie bezpieczeństwa informacji i ochrony danych osobowych

Administrator Danych Osobowych *- Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów*

Instytucja objęta dokumentem*:*
Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów

Zgodnie z art. 32 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 (dalej RODO) oraz zgodnie z USTAWĄ z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)Administrator Danych Osobowych wdraża dokument o nazwie:
„Procedura analizy i szacowania ryzyka w zakresie bezpieczeństwa informacji i ochrony danych osobowych”.

- ***<u>Cel i przeznaczenie dokumentu</u>***

Celem niniejszej dokumentacji jest przedstawienie zasad i procedur dotyczących analizy szacowania ryzyka bezpieczeństwa informacji i danych osobowych.

Celem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowego szacowania ryzyka i opracowanie planów postępowania z ryzykiem.

Analiza uzyskanych wyników stanowi podstawę do podejmowania działań w zakresie doskonalenia ochrony aktywów.

Identyfikowanie ryzyka polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji.

Na szacowanie ryzyka składają się: analiza ryzyka (identyfikowanie, estymacja), ocena ryzyka. W szacowaniu ryzyka określa się wartość aktywów informacyjnych, identyfikuje się mające zastosowanie zagrożenia oraz istniejące (lub mogące zaistnieć) podatności, identyfikuje się istniejące zabezpieczenia i ich wpływ na

zidentyfikowane ryzyko, określa się możliwe następstwa oraz na końcu wskazuje się priorytety uzyskanych ryzyka i ustala ich kolejność zgodnie z kryteriami oceny ryzyka wyznaczonymi podczas ustanawiania kontekstu.

- **Nadrzędnym celem jest:**

1. Zapewnienie spełnienia wymagań prawnych.
2. Ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem.
3. Podnoszenie świadomości pracowników.
4. Zmniejszenie ryzyka utraty informacji.
5. Zaangażowanie wszystkich pracowników w ochronę informacji.
6. Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji.
7. Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji w Urzędzie Miejskim w Złotowie.

- **Zarządzanie ryzykiem, na które składa się:**

1. Klasyfikacja zasobów i ich zawartości.
2. Identyfikacja stopnia zagrożeń i ich następstw.
3. Określenie i wdrożenie działań zabezpieczających zasoby.

- **Zakres obowiązywania:**

1. Niniejszy dokument dotyczy wszystkich komórek organizacyjnych oraz wszystkich pracowników, a także innych osób mających dostęp do informacji chronionych.
2. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej lub innej).

- **Podstawy prawne i organizacyjne**

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (Dz. U. RPUE.L.2016.194.1),
2. Rozporządzenie 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) (Dz. U. UE.L.2016.119.1),
3. Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa -Zarządzanie ryzykiem w bezpieczeństwie informacji,
4. Norma PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania,

Podstawy prawne opracowanej dokumentacji – wg RODO

RODO - ROZDZIAŁ IV

Administrator i podmiot przetwarzający

Sekcja 1

Obowiązki ogólne

Artykuł 24

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Artykuł 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Każda organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia,
- utracenia,
- zmodyfikowania,
- nieuprawnionego ujawnienia,
- nieuprawnionego dostępu

Ocenę ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych przeprowadzamy biorąc pod uwagę potencjalnie negatywne skutki (straty,) zarówno dla administratora jak i dla osób, których dane dotyczą.

UWAGA! Gdyby istniało wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, wówczas należy dodatkowo przeprowadzić ocenę skutków dla ochrony danych osobowych.

Wymagania normy PN-ISO/IEC 27001:2014 w zakresie zarządzania ryzykiem w bezpieczeństwie informacji.

Punkt normy 6.1.1

Planując system zarządzania bezpieczeństwem informacji, organizacja powinna rozważyć czynniki wymienione w 4.1 oraz wymagania podane w 4.2, a także określić ryzyka i szanse, do których należy się odnieść, w celu:
a) zapewnienia, że system zarządzania bezpieczeństwem informacji może osiągnąć zamierzony (-e) wynik (-i);
b) zapobieżenia wystąpieniu niepożądanych skutków lub ich zredukowania;
c) ciągłego doskonalenia;
Organizacja powinna zaplanować:
d) działania odnoszące się do ryzyk i szans;
e) sposób: 1) ich zintegrowania i wdrożenia w procesach składających się na system zarządzania bezpieczeństwa informacji; 2)oceny ich skuteczności.

Punkt normy 6.1.2

Organizacja powinna opracować i wdrożyć proces szacowania ryzyka w bezpieczeństwie informacji, który:
a) ustanawia i utrzymuje kryteria ryzyka bezpieczeństwa informacji obejmujące:
1)kryteria akceptacji ryzyka;
2) kryteria szacowania ryzyka w bezpieczeństwie informacji;
b) zapewnia spójne, poprawne i porównywalne wyniki w kolejnych szacowaniach ryzyka;
c) identyfikuje ryzyka w bezpieczeństwie informacji;
d) analizuje poszczególne ryzyka w bezpieczeństwie informacji;
e) ocenia ryzyka w bezpieczeństwie informacji:
1) porównuje wyniki analizy ryzyka z kryteriami określonymi w 6.1.2 a);
2) nadaje analizowanym ryzykom priorytety dla celów postępowania z ryzykiem.
Organizacja powinna zachować udokumentowane informacje o procesie szacowania ryzyka w bezpieczeństwie informacji.

Punkt normy 6.1.3

Organizacja powinna opracować i wdrożyć proces postępowania z ryzykiem w bezpieczeństwie informacji w celu:
a)wyboru odpowiednich opcji postępowania z ryzykiem w bezpieczeństwie informacji z uwzględnieniem wyników szacowania ryzyka;
b) określeniu wszystkich zabezpieczeń niezbędnych do wdrożenia wybranej(-ych) opcji postępowania z ryzykiem w bezpieczeństwie informacji;
UWAGA: Organizacje mogą zaprojektować zabezpieczenia odpowiednie do swoich potrzeb lub wybrać je z dowolnego źródła.
c) porównania zabezpieczeń;
d) opracowania Deklaracji Stosowania w/w procedury;
e) sformułowaniu planu postępowania z ryzykiem w bezpieczeństwie informacji;
f) uzyskania zgody właścicieli ryzyka na plan postępowania z ryzykiem w bezpieczeństwie informacji i ich akceptacji dla rezydualnych ryzyk w bezpieczeństwie informacji.
Organizacja powinna zachować udokumentowane informacje o procesie postępowania z ryzykiem w bezpieczeństwie informacji.

Punkt normy 6.2c)

Organizacja powinna ustanowić cele bezpieczeństwa informacji dla odpowiednich funkcji i szczebli.
Cele bezpieczeństwa informacji powinny uwzględniać mające zastosowanie wymagania bezpieczeństwa informacji, wyniki szacowania ryzyka i postępowania z ryzykiem.

Punkt normy 8.2

Organizacja powinna szacować ryzyko w bezpieczeństwie informacji w zaplanowanych odstępach czasu lub wtedy, gdy proponowane jest wprowadzenie istotnych zmian, a także wtedy, gdy występują istotne zmiany z uwzględnieniem kryteriów określonych w 6.1.2 a).

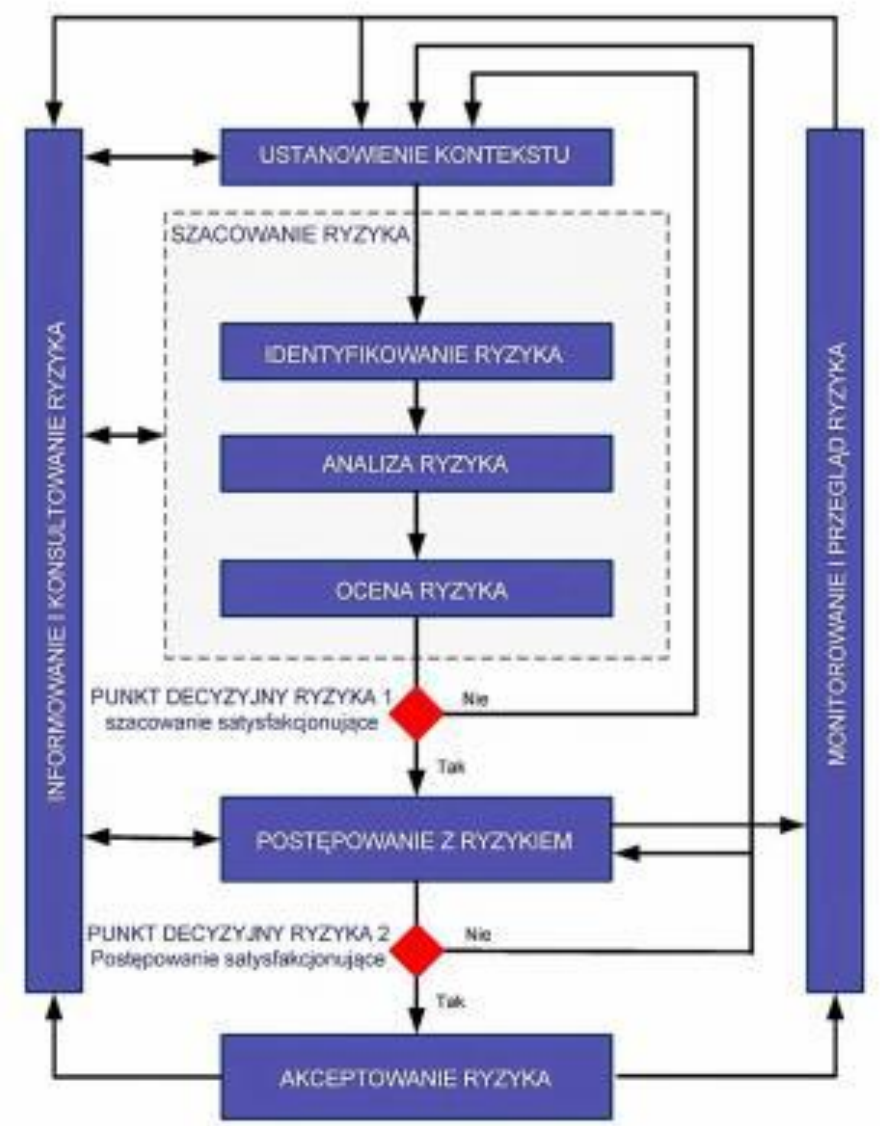
Punkt normy 8.3

Organizacja powinna wdrożyć plan postępowania z ryzykiem w bezpieczeństwie informacji.

Punkt normy 9.3e)

Przegląd zarządzania powinien uwzględniać wyniki szacowania ryzyka i stanów planów postępowania z ryzykiem;

ETAPY ZARZĄDZANIA RYZYKIEM



1. Ogólne wymogi bezpieczeństwa

Przetwarzanie danych osobowych odbywa się w postaci:

a) elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
b) papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

a) środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
b) środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

2. Ewentualne koszty związane z utratą aktywów

1) Koszty związane z odtworzeniem aktywów,
2) Koszty utraty zaufania do administratora danych osobowych,
3) Koszty związane z utratą:
   a) poufności,
   b) integralności,
   c) dostępności danych ,
4) Możliwość nałożenia kary przez organ nadzorczy,
5) Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych, np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

3. Zagrożenia dla systemu informatycznego

Podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

1) Utrata poufności (pozyskanie danych przez osoby nieupoważnione):
   a) nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki),
   b) nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
   c) nieuprawnione skopiowanie danych osobowych na inny nośnik,
   d) zgubienie nośnika zawierającego dane osobowe,
   e) niedostateczne zniszczenie wydruku zawierającego dane osobowe,
   f) klęska żywiołowa powodująca utratę poufności danych.
2) Utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):
   a) nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
   b) błędy ludzkie,
   c) działania wirusów (brak programów antywirusowych i firewalli),
   d) awarie oprogramowania komputerów.
3) Utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań):
   a) brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
   b) brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

4. Źródło zagrożenia, sposób zabezpieczenia

1) Siły wyższe – naturalne -niezależne od jednostki ludzkiej:

a) pożar np.: będący skutkiem uderzenia pioruna,
b) starzenie się sprzętu,
c) powódź,
d) katastrofa budowlana,
e) wilgoć, kurz,

Skutki zagrożeń wynikających z sił natury można starać się ograniczyć poprzez odpowiednie zabezpieczenie budynku, w którym znajdują się dane osobowe.

2) Działalność człowieka:
   a) błędy użytkowników,
   b) zgubienie nośnika informacji,
   c) niewłaściwe usunięcie danych z nośnika informacji,
   d) terroryzm,
   e) utrata prądu,
   f) szpiegostwo,
   g) kradzież,
   h) wandalizm,
   i) podsłuch,
   j) ataki socjotechniczne.

Zagrożenia wynikające z działalności człowieka mogą zostać ograniczone poprzez rygorystyczne przestrzeganie zasad ochrony danych osobowych obowiązujących oraz systematyczne szkolenia użytkowników.

5. Analiza zagrożeń i ryzyka

1) Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.

2) Zagrożenia i ryzyka w zakresie ochrony danych osobowych:
   a) niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
   b) brak procedur ochrony danych osobowych,
   c) niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
   d) brak aktualnego wykazu zbiorów będących w zasobach jednostki,
   e) brak lub wady upoważnień do przetwarzania danych osobowych,
   f) udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie,
   g) brak lub wady ewidencji wydanych upoważnień,
   h) brak lub wady szkoleń z zakresu ochrony danych osobowych,
   i) wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
   j) brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych,
   k) brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

6. Pojęcie i cele ryzyka

1) Ryzyko jest mierzone wpływem (skutkami) i „prawdopodobieństwem wystąpienia". Rozporządzenie w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:
   a) pseudonimizacja i szyfrowanie danych osobowych,
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2) W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy),

powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

7. Identyfikacja ryzyka

Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

a) jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
b) jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
c) jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
d) jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
e) lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
f) jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

8. Pomiar i analiza ryzyka

Prawdopodobieństwo w terminologii zarządzania ryzykiem to możliwość wystąpienia jakiegoś zdarzenia (np. jako prawdopodobieństwo lub częstość w określonym przedziale czasu).

Zdefiniowanie poziomu ryzyka realizujemy wykorzystując macierz ryzyka, która daje możliwość zobrazowania poziomu zagrożeń.

PRAWDOPODOBIEŃSTWO

NISKI	1-20
ŚREDNI	21-60
WYSOKI	61-80
KRYTYCZNY	81-100

POZIOM RYZYKA	*SPOSÓB DZIAŁANIA*
N - niski	Poziom ryzyka akceptowany Działania podejmowane są w zależności od wymaganych nakładów.
Ś - średni	Poziom ryzyka nieakceptowany Działanie może zostać przesunięte w czasie, lecz wymagany jest okresowy nadzór i monitorowanie.
W – wysoki	Poziom ryzyka nieakceptowany Działanie może zostać przesunięte w czasie, lecz wymagany jest stały nadzór i monitorowanie.
K – krytyczny	Poziom ryzyka nieakceptowany

Wymagana jest niezwłoczna reakcja i działanie

RYZYKO SZCZĄTKOWE:

Ryzyko szczątkowe – ryzyko, które pozostaje po wprowadzeniu zabezpieczeń, często zwane również ryzykiem pozostałym lub ryzykiem akceptowalnym.

Po analizie zagrożeń i podatności wszystkich czynników występujących czy też mogących wystąpić opisanych dotychczas, niewątpliwie istnieje jeszcze pewne ryzyko dla bezpieczeństwa przetwarzania danych osobowych. W celu bardziej przejrzystego zidentyfikowania pozostałego ryzyka niżej przedstawiono proces analizy ryzyka w oparciu o podaną macierz. W rzędach macierzy wyszczególnione są zasoby podlegające ochronie.

Analiza dotyczy ryzyk jakie zagrażają:

- INTEGRALNOŚCI,
- POUFNOŚCI ,
- DOSTĘPNOŚCI.

INTEGRALNOŚĆ - właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany – pożar, katastrofa budowlana, błąd ludzki przy przetwarzaniu danych osobowych, zniszczenie płyty zawierającej jedyną kopię danych osobowych.

POUFNOŚĆ - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom – nieuprawniony dostęp klientów do danych osobowych, zagubienie wydruku.

DOSTĘPNOŚĆ - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

Skutek - rezultat niepożądanego incydentu, następstwa zaistnienia zagrożeń, szkody mierzone wysokością strat, jakie poniosłaby jednostka organizacyjna w wyniku ujawnienia, utraty lub modyfikacji informacji lub zasobu systemu.

Podatność - słabość zasobów, która może być wykorzystana przez zagrożenie – charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę.

Ryzyko - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobów, aby spowodować ich straty lub zniszczenie.

RYZYKO (iloczyn) : PODATNOŚĆ X SKUTEK = RYZYKO

PRZYJĘTE WARTOŚCI ZWIĄZANE Z OCENĄ ZAGROŻENIA:

- 1 - 3 - nie ma realnej szansy wystąpienia zidentyfikowanego zagrożenia; zagrożenie nigdy nie wystąpiło,
- 4 - 7 - zagrożenie jest mało realne, jednak zagrożenie może się pojawić,
- 8 - 9- zagrożenie jest realne i może pojawić się w nieoczekiwanym momencie, pomimo iż nie wystąpiło w okresie ostatnich 24 miesięcy,
- 10 - zagrożenie jest realne lub bardzo realne; zagrożenie wystąpiło w okresie ostatnich 24 miesięcy.

9. Szacowanie ryzyka integralności

W analizie ustalono cztery poziomy zagrożeń dotyczących zachowania integralności oraz zakres wartości liczbowych (1-10) dla tych poziomów:

Poziomy zagrożeń	**Zakres wartości liczbowych skutków utraty integralności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie - **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA INTEGRALNOŚCI”

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**							
		Nielegalny dostęp	Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Wirusy	Personel	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	8	6	8	6	5	4	5	4
	PODATNOŚĆ	3	5	3	3	5	6	5	3
	RYZYKO	**24**	**30**	**24**	**24**	**25**	**24**	**25**	**12**
Zgromadzone dane – zbiory	SKUTKI	4	5	6	6	6	5	6	5
	PODATNOŚĆ	6	5	4	4	5	6	5	4
	RYZYKO	**24**	**25**	**24**	**24**	**30**	**30**	**30**	**20**
Oprogramowanie	SKUTKI	6	5	7	5	6	7	6	4
	PODATNOŚĆ	5	6	4	6	7	7	6	5
	RYZYKO	**30**	**30**	**28**	**30**	**42**	**49**	**36**	**20**
Sprzęt komputerowy	SKUTKI	6	6	5	6	6	7	6	4
	PODATNOŚĆ	6	5	4	5	6	7	5	4
	RYZYKO	**36**	**30**	**20**	**30**	**36**	**49**	**30**	**16**

OSZACOWANIE RYZYKA INTEGRALNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów, w ujęciu integralności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI 1-20

ŚREDNI 21-60

WYSOKI 61-80

KRYTYCZNY 81-100

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego.

10. Szacowanie ryzyka poufności

W analizie szacowania ryzyka przyjęto cztery poziomy zagrożeń zachowania „poufności" i 10 - cio stopniową skalę skutków utraty „poufności":

Poziomy zagrożeń	**Zakres wartości liczbowych skutków utraty poufności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA POUFNOŚCI"

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**									
		Nielegalny dostęp	Błędy, pomyłki	Pokonanie i omijanie zabezpieczeń	Nielegalne kopiowanie	Nieuprawnione naprawy	Rotacja personelu	Awarie	Klęski żywiołowe	Podsłuch i pogląd	Niedyskrecja
Nośniki informacji	SKUTKI	9	6	6	8	6	5	4	4	5	9
	PODATNOŚĆ	3	5	6	7	7	7	4	4	5	6
	RYZYKO	**27**	**30**	**36**	**56**	**42**	**35**	**16**	**16**	**25**	**54**
Zgromadzone dane	SKUTKI	8	8	8	7	8	6	6	3	7	8
	PODATNOŚĆ	6	5	7	6	5	4	5	3	3	5
	RYZYKO	**48**	**40**	**56**	**42**	**40**	**24**	**30**	**9**	**21**	**40**
Oprogramowanie	SKUTKI	8	8	9	9	7	5	5	4	6	6
	PODATNOŚĆ	3	6	6	5	3	4	4	4	4	4
	RYZYKO	**24**	**56**	**54**	**45**	**21**	**20**	**20**	**16**	**24**	**24**
Sprzęt komputerowy	SKUTKI	8	7	8	2	8	4	6	4	6	6
	PODATNOŚĆ	7	7	7	3	7	5	7	3	6	4
	RYZYKO	**56**	**49**	**56**	**6**	**56**	**20**	**42**	**12**	**36**	**24**

OSZACOWANIE RYZYKA POUFNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, poufności i dostępności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI 1-20

ŚREDNI 21-60

WYSOKI 61-80

KRYTYCZNY 81-100

Analizując otrzymane wyniki należy stwierdzić, że w instytucji nie zanotowano poziomu ryzyka wysokiego i krytycznego.

11. Szacowanie ryzyka dostępności

W analizie „ryzyka dostępności" przyjęto cztery poziomy zagrożeń zachowania „dostępności" i 10-cio stopniową skalę skutków utraty „dostępności":

Poziomy zagrożeń	**Zakres wartości liczbowych skutków utraty dostępności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA DOSTĘPNOŚCI"

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**						
		Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Infekcja wirusowa	Rotacja personelu	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	2	2	3	3	3	3	4
	PODATNOŚĆ	2	1	2	3	3	3	4
	RYZYKO	**4**	**2**	**6**	**9**	**9**	**9**	**16**
Zgromadzone dane	SKUTKI	6	6	6	6	6	6	6
	PODATNOŚĆ	7	3	3	5	2	2	2
	RYZYKO	**42**	**18**	**18**	**30**	**12**	**12**	**12**
Oprogramowanie	SKUTKI	3	4	2	2	3	3	2
	PODATNOŚĆ	2	3	2	3	2	3	4
	RYZYKO	**6**	**12**	**4**	**6**	**6**	**9**	**8**
Sprzęt komputerowy	SKUTKI	3	4	2	2	3	5	3
	PODATNOŚĆ	4	2	3	3	3	5	2
	RYZYKO	**12**	**8**	**6**	**6**	**9**	**25**	**6**

OSZACOWANIE RYZYKA DOSTĘPNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów i dostępności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI	1-20
ŚREDNI	21-60
WYSOKI	61-80
KRYTYCZNY	81-100

Analizując otrzymane wyniki szacowania ryzyka w instytucji w zakresie integralności, poufności, dostępności należy stwierdzić, że zanotowano średni poziom zagrożeń, natomiast nie zanotowano poziomu ryzyka wysokiego i krytycznego.

Postanowienia końcowe

W sprawach nieuregulowanych niniejszą procedurą odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych podmiotu.

Dokument wchodzi w życie z dniem podpisania.

Zapisy tego dokumentu wchodzą w życie z dniem 2 listopada 2021 r.

Sporządził: *Marcin Misztal – Inspektor Ochrony Danych Osobowych.*

Administrator Danych Osobowych: *Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów*

……...

Data, podpis i pieczątka