PROCEDURA ZARZĄDZANIA RYZYKIEM

BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w podmiocie

Gminna Biblioteka Publiczna w Grzmiącej

ul. Kolejowa 2,
78-450 Grzmiąca

Grzmiąca 2024-05-08

Zatwierdzone przez Administratora Danych

Jadwiga Kasztelan-Massopust

Pieczątka, podpis

1. WSTĘP

Jednym z kluczowych elementów ochrony danych osobowych jest analiza i oszacowanie ryzyka związanego z istniejącymi lub potencjalnymi zagrożeniami dla procesów przetwarzania danych funkcjonujących w organizacji oraz naruszenia ciągłości działania organizacji.

Celem niniejszego dokumentu jest przedstawienie metodologii zarządzania ryzykiem. Zakres dokumentu obejmuje wszystkie komórki organizacji. Przedstawia metodę tworzenia analizy i oceny ryzyka.

2. TERMINOLOGIA

Proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania ,

Poufność - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

Integralność danych - właściwość polegająca na tym, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Integralność systemu - właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.

Dostępność - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany (upoważniony) podmiot.

Podatność – cecha zasobu powodująca, że zasób jest narażony na działanie jednego lub wielu zagrożeń (np. podatnością serwerowni jest drewniana podłoga, zagrożeniem w tym przykładzie – pożar),

Punkt krytyczny – potencjalny negatywny czynnik poddawany ocenie będący podstawą do wyznaczenia ryzyka (zagrożenie lub podatność). Punkt krytyczny jest scharakteryzowany następującymi atrybutami:

- prawdopodobieństwo realizacji punktu krytycznego,
- skutek realizacji punktu krytycznego,
- wykrywalność,

Zabezpieczenie – rozwiązanie techniczne lub organizacyjne minimalizujące ryzyko,

Zagrożenie – niepożądane działanie lub sytuacja dotycząca procesów przetwarzania danych, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w organizacji.

3. METODA ZARZĄDZANIA RYZYKIEM

3.1. ZAŁOŻENIA

Skuteczne zarządzanie ryzykiem w obszarze bezpieczeństwa informacji wymaga od przyjętej metody liczenia ryzyka spełnienia następujących warunków:

- zapewnienia powtarzalności i porównywalności wyników,
- uwzględnienia stopnia poufności, dostępności i integralności,
- uwzględnienia prawdopodobieństwa wystąpienia zdarzenia (zagrożenia) i konsekwencji jego realizacji (skutków),
- uwzględnienia efektywności funkcjonujących zabezpieczeń, wpływających na prawdopodobieństwo zajścia zdarzeń, jak i na późniejsze ewentualne konsekwencje ich realizacji.
- określenie kryteriów oceny ryzyka i jego akceptacji.

3.2. PODSTAWY PROPONOWANEJ METODY SZACOWANIA RYZYKA

Zastosowano opracowaną do wielkości i charakteru organizacji metodę szacowania ryzyka spełniającą powyższe założenia. Jej najważniejszymi elementami są: ustalenie zgodnie z „Wykazem zbiorów danych" lub „Rejestrem czynności przetwarzania danych" wszystkich procesów zachodzących przy przetwarzaniu danych osobowych. Stanowi to punkt wyjściowy do identyfikacji ryzyka oraz wynikających z niego zagrożeń. Kolejnym elementem jest analiza zidentyfikowanych ryzyk, w której oceniamy prawdopodobieństwo wystąpienia zagrożenia Przyjmuje się, że ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż raz na 12 miesięcy.

4. OPIS METODY ANALIZY RYZYKA

4.1. Określenie ich wartości dla działalności organizacji następuje poprzez przydzielenie im odpowiednich ocen w obszarach poufności, dostępności i integralności. Kryteria opisane są w punktach 4.1.1, 4.1.2 oraz 4.1.3.

4.1.1. Poziom poufności

1	Informacje ogólnodostępne
2	Informacje chronione przede wszystkim ustawą o ochronie danych osobowych i RODO, informacje które przetwarzane są w wielu instytucjach (np. firmy telekomunikacyjne, dostawców mediów), również chronione informacje wewnętrzne organizacji, których ujawnienie nie wiąże się z sankcjami karnymi lub odszkodowawczymi, jednak może wiązać się z niewielkimi stratami podmiotu.
3	Informacje chronione zgodnie z RODO i ustawą o ochronie danych osobowych (tzw. wrażliwe), również informacje objęte tajemnicą, wynikającą z innych aktów prawnych (np. ordynacji podatkowej, tajemnicy bankowej, tajemnicy przedsiębiorstwa i pozostałych). Informacje, których ujawnienie może wiązać się z sankcjami karnymi lub odszkodowawczymi oraz mogą zagrozić istnieniu podmiotu.

4.1.2. Poziom dostępności

1	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich może być dłuższa niż 5-7 dni roboczych
2	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich nie może być dłuższa niż 3-5 dni roboczych
3	Informacje muszą być dostępne w sposób nieprzerwany, brak dostępu może w skrajnych okolicznościach skutkować sankcjami karnymi lub odszkodowawczymi.

4.1.3. Poziom integralności

1	Naruszenie integralności informacji jest łatwe do wykrycia i naprawienia, skutki wywołane nieprawidłową informacją są łatwe do przewidzenia i naprawienia
2	Naruszenie integralności informacji jest możliwe do wykrycia i naprawienia, skutki wywołane wadliwą informacją są możliwe do skorygowania, wymaga to jednak pewnego wkładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych
3	Naruszenie integralności informacji jest trudne lub wręcz niemożliwe do naprawienia, skutki wywołane wadliwą informacją wiążą się z poważnymi sankcjami (np. odszkodowawczymi lub karnymi), usunięcie lub skorygowanie skutków wiąże się z poniesieniem znaczących nakładów finansowych

4.2. IDENTYFIKACJA ZAGROŻEŃ

Dla każdego procesu określa się podatności i zagrożenia z nich wynikające. W analizie bierzemy pod uwagę trzy grupy zagrożeń dla zasobów informacyjnych organizacji, które rozważamy w kontekście określenia ryzyka związanego z przetwarzaniem informacji.

- Zagrożenia dla poufności informacji
- Zagrożenie dla dostępności informacji
- Zagrożenie dla integralność informacji

4.3. ANALIZA ODDZIAŁYWANIA ZAGROŻEŃ NA BEZPIECZEŃSTWO ZASOBÓW

Badane procesy analizowane są pod kątem wpływu typowych podatności i wynikających z nich zagrożeń. Każde zagrożenie analizowane jest na okoliczność utraty poufności, integralności i dostępności opisywanej grupy informacji.

4.4. ANALIZA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻEŃ

Każde z ocenianych zagrożeń jest oceniane pod kątem prawdopodobieństwa wystąpienia. Skala oceny jest trzystopniowa (od małego do dużego). Kryteria oceny znajdują się w „tabeli oceny prawdopodobieństwa". Prawdopodobieństwo wystąpienia ryzyka oceniamy uwzględniając funkcjonujące zabezpieczenia.

TABELA OCENY PRAWDOPODOBIEŃSTWA

Prawdopodobieństwo wystąpienia	Opis
Duże	Wydarzenie, którego zaistnienie jest dość prawdopodobne i można się go spodziewać kilka razy w roku
Średnie	Wydarzenie, którego zaistnienie jest względnie prawdopodobne, być może raz w roku
Małe	Zdarzenie, którego zaistnienie jest mało prawdopodobne, być może raz na 3 lata

4.5. WAGA RYZYKA

Waga ryzyka określana jest w skali pięciostopniowej (od bardzo małego do bardzo dużego). Wagę ryzyka ustala się na podstawie macierzy ryzyka, w której przyporządkowuje się ocenę prawdopodobieństwa do wpływu, jakie potencjalnie niesie ze sobą ryzyko.

TABELA MACIERZY RYZYKA

	Duże	3	4	5
	Średni	2	3	4
	Małe	1	2	3
		Małe	Średnie	Duże
		Prawdopodobieństwo		

4.6. KRYTERIA AKCEPTACJI RYZYKA

Otrzymany wynik w skali od 1 do 5 przekłada się na ocenę wagi ryzyka. Ogólne zasady postępowania ze zidentyfikowanym ryzykiem opisane są w tabeli ogólnych zasad wyznaczania ryzyka.

TABELA OGÓLNYCH ZASAD WYZNACZANIA DOPUSZCZALNOŚCI RYZYKA

Waga ryzyka wg macierzy	Oszacowanie ryzyka	Dopuszczalność ryzyka	Niezbędne działania
5	duże	Niedopuszczalne	Ryzyko krytyczne, działania mające na celu zmniejszenia ryzyka do poziomu dopuszczalnego należy podjąć natychmiast.
3,4	Średnie	Dopuszczalne	Zaleca się zaplanowanie i podjęcie działań, których celem jest zmniejszenie ryzyka.
1,2	Małe		Zaleca się rozważenie możliwości dalszego zmniejszania poziomu ryzyka lub zapewnienie, że ryzyko pozostaje najwyżej na tym samym poziomie.

5. PLAN POSTĘPOWANIA Z RYZYKIEM

Zaplanowane działania postępowania z ryzykiem zapisywane są w planie postępowania z ryzykiem. Dla wszystkich procesów, których poziom ryzyka będzie wyższy niż dopuszczalny, konieczne będzie wdrożenie środków ograniczających ryzyko lub zastosowanie jednej z następujących strategii postępowania:

- wdrożenie dodatkowych zabezpieczeń,
- świadome zaakceptowanie ryzyka na poziomie przekraczającym próg akceptowalności Administratora Danych,
- przeniesienie ryzyka na inny podmiot (np. ubezpieczenia),
- uniknięcie ryzyka (np. zaprzestanie przetwarzania danych osobowych w aktualny sposób np. zmiana programu bądź sposobu przetwarzania danych).

Po wdrożeniu środków ograniczających ryzyko, ich skuteczność powinno poddać się ocenie. Ze względu na to, że wprowadzanie środków kontroli ryzyka wiążę się z przeznaczeniem zasobów, plan postępowania z ryzykiem wymaga akceptacji Administratora Danych.

Tabela szacowania ryzyka

LP	Nazwa procesu	Poziom Poufności Str. 4	Poziom Dostępności Str. 4	Poziom Integralności Str. 4	Ryzyko Prawdopodobieństwo /Waga Str. 5	Działania związane z ryzykiem
1.	Dane pracownicze i powiązane z nimi dane – zatrudnienie na podstawie stosunku pracy	3	1	1	Średnie/ Dopuszczalne	Nie dotyczy
2.	Umowy cywilnoprawne – realizowanie umów cywilnoprawnych (umowa o dzieło, umowa zlecenia),	3	1	1	Średnie/ Dopuszczalne	Nie dotyczy
3.	Dane osób korzystających z placówki (uczestnicy zajęć, konkursów,czytelnicy itp.) i powiązane z nimi dane rodziców i opiekunów prawnych – realizowanie zadań podmiotu	3	1	1	Średnie/ Dopuszczalne	Nie dotyczy
4.	Dane stażystów i praktykantów – przyjmowanie osób praktykantów do odbycia stażu/praktyki	2	1	1	Małe/ Dopuszczalne	Nie dotyczy
5.	Dane finansowo-księgowe – realizowanie spraw księgowo – finansowych, płatności itd. Funkcjonowanie podmiotu w oparciu	2	1	1	Małe/ Dopuszczalne	Nie dotyczy

	o współpracę z kontrahentami (zawarcie i realizacja zawartej umowy) oraz powiązane z nimi dane kontrahentów					
6.	CV Rekrutacja - analiza dokumentów aplikacyjnych podczas poszukiwania nowego pracownika	2	1	1	Małe/ Dopuszczalne	Nie dotyczy
7.	Rejestr korespondencji – ewidencja poczty przychodzącej i wychodzącej	1	1	1	Małe/ Dopuszczalne	Nie dotyczy
8.	Archiwum zakładowe – archiwizowanie dokumentów	3	1	1	Średnie/ Dopuszczalne	Nie dotyczy
9.	Dokumenty związane z wprowadzeniem procedur Standardów ochrony małoletnich	3	1	1	Średnie/ Dopuszczalne	Nie dotyczy
10.	Dokumentacja związana z procedurą Pracy zdalnej	2	1	1	Małe/ Dopuszczalne	Nie dotyczy

PLAN POSTĘPOWANIA Z RYZYKIEM

Po wykonaniu Procedury Zarządzania Ryzykiem w związku z oceną wagi ryzyka i jej dopuszczalności w podmiocie wskazuje się następujące wyniki i postepowanie z nimi:

POZIOM DOPUSZCZALNOŚCI RYZYKA W PODMIOCIE = RYZYKO MAŁE/ DOPUSZCZALNE

Zbiory i czynności przetwarzania danych wymagające szczególnej uwagi Administratora Danych:
1. Dane pracownicze i powiązane z nimi dane – zatrudnienie na podstawie stosunku pracy
2. Umowy cywilnoprawne – realizowanie umów cywilnoprawnych (umowa o dzieło, umowa zlecenia),
3. Dane osób korzystających z placówki (uczestnicy zajęć,konkursów, czytelnicy itp.) i powiązane z nimi dane rodziców i opiekunów prawnych – realizowanie zadań podmiotu
4. Archiwum zakładowe – archiwizowanie dokumentów
5. Dokumenty związane z wprowadzeniem procedur Standardów ochrony małoletnich

Oszacowanie ryzyka	**Dopuszczalność ryzyka**	**Niezbędne działania**	**Plan postępowania z ryzykiem**
Średnie	Dopuszczalne	Zaleca się zaplanowanie i podjęcie działań, których celem jest zmniejszenie ryzyka.	1. Systematyczna analiza ryzyka poszczególnych zbiorów danych wskazanych wyżej. 2. Ciągłe budowanie świadomości pracowników poprzez aktualne szkolenia z zakresu ochrony danych osobowych. 3. Wykonywanie monitorowania bezpieczeństwa danych osobowych w ujęciu całościowym podmiotu.
Małe	Dopuszczalne	Zaleca się rozważenie możliwości dalszego zmniejszania poziomu ryzyka lub zapewnienie, że	1. Systematyczna analiza ryzyka poszczególnych zbiorów danych i oszacowanie ich ryzyka – sprawdzenie czy nadal klasyfikować je można jakie “małe”.

		ryzyko pozostaje najwyżej na tym samym poziomie.	2. Ciągłe budowanie świadomości pracowników poprzez aktualne szkolenia z zakresu ochrony danych osobowych.

AKCPETACJA PLANU POSTĘPOWANIA Z RYZYKIEM

Zatwierdzone przez Administratora Danych	Zatwierdzone przez Inspektora Ochrony Danych Osobowych
Podpis Jadwiga Kasztelan-Massopust	Podpis Sylwia Bołdak