PROCEDURA

ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

Szkoły Podstawowej nr 1 w Bytowie,

ul. Mierosławskiego 7, 77-100 Bytów

Data wprowadzenia:	
Wersja:	**1**
Data utworzenia:	**05.03.2026 r.**
Opracował:	**Piotr Przyborowski (IOD)**
Zatwierdził:	

SPIS TREŚCI:

1. Wprowadzenie 3
2. Opis analizy ryzyka 3
3. Dane projektu 5
4. Lista aktywów 5
5. Lista zagrożeń 5
6. Lista podatności 5
7. Skala skutków i prawdopodobieństw 5
8. Skala ryzyka 6
9. Ryzyko akceptowalne 6
10. Lista zabezpieczeń 7
11. Macierz ryzyka po wdrożeniu zabezpieczeń 7
12. Ocena ryzyka 7
13. Wnioski 7
14. Ocena skutków dla ochrony Danych Osobowych (DPIA) 7
15. Załączniki 8

1. Wprowadzenie

Analiza ryzyka przetwarzania danych osobowych wykonywana jest przy użyciu programu komputerowego ARDO SMALL 2.0, firmy F-tec. F-tec jest firmą doradczą, specjalizującą się w świadczeniu usług z zakresu bezpieczeństwa informacji, oraz producentem specjalistycznego oprogramowania z zakresu bezpieczeństwa informacji niejawnych oraz danych osobowych.

2. Opis analizy ryzyka

W dokumencie przedstawiono wyniki procesu szacowania ryzyka dla bezpieczeństwa danych osobowych. W trakcie szacowania ryzyka przeprowadzono analizę ryzyka i ocenę ryzyka, czyli określono, które ryzyka są akceptowalne poprzez porównanie ich z wyznaczonym poziomem ryzyka, które można zaakceptować. W trakcie analizy ryzyka przeprowadzono identyfikację ryzyka i określono wielkości ryzyk.

1) Cechy informacji:
- Dostępność jest to właściwość określająca, że zasób jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony.
- Integralność jest to właściwość określająca, że zasób nie został zmodyfikowany w sposób nieuprawniony.
- Poufność jest to właściwość określająca, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym.

2) Zarządzanie ryzykiem:
Proces zarządzania ryzykiem prowadzi się w celu zapewnienia i utrzymania na poziomie akceptowanym przez kierownictwo organizacji bezpieczeństwa danych osobowych przetwarzanych w organizacji.
Zarządzanie ryzykiem składa się z następujących procesów:
- szacowanie ryzyka,
- postępowanie z ryzykiem,
- akceptacja ryzyka,
- przegląd, monitorowanie i informowanie o ryzyku.

3) Proces szacowania ryzyka składa się z:
- analizy ryzyka,
- oceny ryzyka.

4) Proces postępowania z ryzykiem:
- wybór sposobu działania z otrzymanym ryzykiem. Ryzyko możemy obniżyć wdrażając środki ochrony, pozostawić na wyliczonym poziomie, uniknąć ryzyka nie podejmując ryzykownych działań lub przenieść ryzyko na inny podmiot.

5) Proces akceptacji ryzyka:
- zatwierdzenie przez kierownictwo organizacji aktualnego stanu jako wystarczającego do ochrony danych osobowych.

6) Proces przeglądu, monitorowania i informowania o ryzyku:

- bieżąca analiza wdrożonych środków ochrony, otoczenia prawnego, środowiska eksploatacji systemu, zmian organizacji. Informowanie osób odpowiedzialnych za zarządzanie ryzykiem o zmianach ryzyka i nowych ryzykach.

7) Szacowanie ryzyka:
Szacowanie ryzyka jest to proces analizy ryzyka i oceny ryzyka. Analiza ryzyka jest to proces identyfikacji ryzyka i określenia wielkości ryzyk.

8) Analiza ryzyka:
- identyfikacja aktywów, czyli informacje, osoby, usługi, oprogramowanie, dane i sprzęt, a także inne elementy mające wpływ na bezpieczeństwo informacji,
- identyfikacja zagrożeń, czyli niepożądane zdarzenia, mogące mieć wpływ na dane osobowe,
- identyfikacja podatności, czyli słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie,
- identyfikacja zabezpieczeń, czyli środki o charakterze fizycznym, technicznym lub organizacyjnym,
- identyfikacja skutków, czyli wyników działania zagrożenia,
- określenie wielkości ryzyk, czyli wyznacza się poziomy zidentyfikowanych ryzyk.

9) Ocena ryzyka:
- porównanie wyznaczonych poziomów ryzyk z tymi, które można zaakceptować. Na podstawie oceny podejmuje się decyzję co do dalszego postępowania z ryzykami.

10) Szacowanie ryzyka przeprowadza się:
- przed podjęciem decyzji o wprowadzeniu niezbędnych zabezpieczeń,
- w przypadku wprowadzania zmian, które mogą mieć wpływ na bezpieczeństwo informacji
- po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka,
- w przypadku zaistnienia istotnego incydentu bezpieczeństwa,
- jeżeli zmianie lub rozszerzeniu uległo przeznaczenie, zadania lub funkcjonalność systemu,
- okresowo, przy czym częstotliwość określa się w polityce bezpieczeństwa.

11) Opis metodyki:
Metodyka użyta w analizie ryzyka jest to metodyka jakościowa. W metodyce wartość ryzyka naruszenia bezpieczeństwa wyliczana jest jako iloczyn skutków działania zagrożenia (następstw) i prawdopodobieństwa tego zagrożenia.

RYZYKO = SKUTEK x PRAWDOPODOBIEŃSTWO

Na podstawie szacowania ryzyka dokonujemy wyboru środków ochrony, określamy zabezpieczenia które należy wdrożyć w celu zapewnienia ochrony danych osobowych. Szacowanie ryzyka pozwala zidentyfikować ryzyka naruszenia bezpieczeństwa, na jakie narażone są informacje przetwarzane w systemie, pozwala dobrać adekwatne zabezpieczenia, efektywnie chroniące zasoby, a przede wszystkim informacje składowane w tym systemie. Na podstawie szacowania ryzyka dokonujemy wyboru środków ochrony, określamy zabezpieczenia które należy wdrożyć w celu zapewnienia ochrony danych osobowych.

12) Cel szacowania ryzyka:
- określenie zagrożeń i podatności systemów na te zagrożenia,
- identyfikacja obszarów, dla których należy wdrożyć zabezpieczenia i środki zaradcze,
- określenie istniejącego ryzyka,
- określenie skuteczność istniejących zabezpieczeń,
- zgromadzenie informacji potrzebnych do wyboru efektywnych i niezbędnych zabezpieczeń.

Przedstawiona metodyka określa ryzyka naruszenia bezpieczeństw na podstawie macierzy ryzyk. Macierz ryzyka obrazuje działania zagrożeń na zasoby. Działania te są opisane w postaci prawdopodobieństwa wystąpienia zagrożenia i skutków wystąpienia zagrożeń. Na podstawie prawdopodobieństwa i skutków otrzymujemy ryzyka. Każde ryzyko naruszenia bezpieczeństwa otrzymuje się z pary zasób i zagrożenie. Prawdopodobieństwa i skutki przedstawione są za pomocą skal liczbowych, a ich iloczyn stanowi ryzyko.

3. Dane projektu

1) Nazwa jednostki organizacyjnej:
2) Opis systemu – zawarty w Raporcie analizy ryzyka.

4. Lista aktywów

Zasobem nazywamy informacje, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji. W ramach identyfikacji ryzyka określono następujące zasoby - spis w Raporcie analizy ryzyka.

5. Lista zagrożeń

W ramach identyfikacji ryzyka określono zagrożenia. Poprzez zagrożenie należy rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach - spis w Raporcie analizy ryzyka.

6. Lista podatności

W ramach identyfikacji ryzyka określono podatności zasobów. Podatność należy rozumieć jako słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie – spis podatności w Raporcie analizy ryzyka.

7. Skala skutków i prawdopodobieństw

SKUTKI

Skutki ustalono dla każdego atrybutu informacji: poufności, dostępności i integralności. Przyjęto 10-stopniową wartość skali. Im większa wartość, tym większy skutek działania zagrożenia na zasób.

Skutek utraty poufności / zachowanie poufności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

Skutek utraty integralności / zachowanie integralności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

Skutek utraty dostępności / Zachowanie dostępności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

PRAWDOPODOBIEŃSTWA

Prawdopodobieństwa przyjmują wartości od 0 do 1. Im większa wartość tym większe prawdopodobieństwo wystąpienia zagrożenia.

Podatność systemu

Wartość	Poziom
0	Brak
0,1 - 0,2	Bardzo niskie
0,3 - 0,4	Niskie
0,5 - 0,6	Średnie
0,7 - 0,8	Wysokie
0,9 - 1	Bardzo wysokie

8. Skala ryzyka

Ryzyko wyliczono ze wzoru: Ryzyko = Skutek * Prawdopodobieństwo. W związku z tym, że skala skutków jest 10-stopniowa, skala prawdopodobieństwa jest ułamkowa od 0-1 to skala ryzyka po wymnożeniu skutków i prawdopodobieństwa jest 10-stopniowa. Przyjęto następujące poziomy ryzyka dla obliczonych wartości liczbowych ryzyka.

(R)yzyko = (P)rawdopodobieństwo * (S)kutek

Ryzyko utraty poufności, dostępności i integralności

Poziomy ryzyk	
Wartość ryzyka	**Poziom ryzyka**
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

9. Ryzyko akceptowalne

Przyjęto następującą wartość ryzyka akceptowalnego. Jest to poziom akceptowalny, powyżej którego należy zmniejszyć ryzyko.

Ryzyko akceptowalne: 4 (Średnie)

10. Lista zabezpieczeń

W ramach identyfikacji ryzyka wdrożono poniższe zabezpieczenia. Zabezpieczenie jest to środek o charakterze fizycznym, technicznym lub organizacyjnym zmniejszający ryzyko. Poprzez wdrożenie poniższego zbioru zabezpieczeń zapewniono bezpieczeństwo danych osobowych.

11. Macierz ryzyka po wdrożeniu zabezpieczeń

Po zastosowaniu zabezpieczeń nastąpiło obniżenie ryzyk naruszenia bezpieczeństwa. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.

12. Ocena ryzyka

Na etapie oceny ryzyka określa się, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyk z ryzykiem, które można zaakceptować. W przypadku, gdy ryzyka są większe od ryzyka akceptowalnego, wprowadza się działania zaradcze (proces postępowania z ryzykiem). Dla ryzyk, które nie mogą być zaakceptowane ze względu na ich zbyt wysoki poziom, proces postępowania z ryzykiem przeprowadza się ponownie. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.
Ryzyka naruszenia bezpieczeństwa zostały posortowane od największego do najmniejszego. Poniżej przedstawiono 100 największych wartości w tabeli oceny ryzyka dla poufności, dostępności i integralności.
Ryzyko akceptowalne: 4

13. Wnioski

Wszystkie ryzyka utraty poufności, dostępności i integralności zasobów i danych osobowych są akceptowalne. Kierownictwo organizacji akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa danych osobowych. Kierownictwo organizacji akceptuje ryzyka szczątkowe wraz z jego ewentualnymi konsekwencjami.

14. Ocena skutków dla ochrony Danych Osobowych (DPIA)

1) Jeżeli w wyniku przeprowadzonej analizy ryzyka dany rodzaj przetwarzania, ze względu na swój charakter, zakres, kontekst i cele powoduje nieakceptowalne wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator dokonuje oceny skutków operacji przetwarzania dla ochrony danych osobowych.

2). Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

3). Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych;

b) Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki;
c) Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące

elementy rozpoznawania cech lub właściwości obiektów, które znajda się w monitorowanej przestrzeni.
Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa.

d) Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29);

e) Dane przetwarzane na dużą skale, udzie pojęcie dużej skali dotyczy:
- liczby osób, których dane są przetwarzane,
- zakresu przetwarzania,
- okresu przechowywania danych oraz
- geograficznego zakresu przetwarzania;

f) Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
g) Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi;
h) Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych;
i) Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.

4). Dokument DPIA zawiera co najmniej:
- opis operacji przetwarzania;
- opis celów przetwarzania;
- oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- opis podatności;
- opis możliwych skutków;
- ocenę ryzyka przed zastosowaniem zabezpieczeń;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.
- ocenę ryzyka po zastosowaniu zabezpieczeń.

15. Załączniki

Załącznik PAR 1 – Raport Analiza ryzyka
Załącznik PAR 2 – Formularz oceny skutków dla ochrony danych

RAPORT

ANALIZA RYZYKA

dla bezpieczeństwa danych osobowych

Szkoły Podstawowej nr 1 w Bytowie,

ul. Mierosławskiego 7, 77-100 Bytów

Data wprowadzenia:	
Data utworzenia:	
Opracował:	**Piotr Przyborowski (IOD)**
Zatwierdził:	

Organizacja:	**Ocena skutków dla ochrony danych (DPIA)**						
	Czynność …..			**Cel przetwarzania: …..**			
OCENA RYZYKA NARUSZENIA PRAW I WOLNOŚCI	**PODATNOŚCI**	**MOŻLIWE SKUTKI**	**WAGA (liczba)**	**PRAWDOPODOBIEŃSTWO (liczba)**	**RYZYKO (iloczyn Wagi i Prawdopodobieństwa)**	**REKOMENDACJE ZABEZPIECZEŃ**	**OCENA PO ZAST. REK. ZABEZPIECZEŃ**
Jakie jest ryzyko kradzieży tożsamości lub oszustwa dotyczącego tożsamości?							
Jakie jest ryzyko naruszenia zakazu dyskryminacji?							
Jakie jest ryzyko szkody finansowej dla osób, których dane dotyczą?							
Jakie jest ryzyko szkody wizerunkowej dla osób, których dane dotyczą?							
Jakie jest ryzyko złamania tajemnicy zawodowej, mającej chronić osoby, których dane dotyczą?							
Wszelkie inne naruszenia praw i wolności osób fizycznych							
Wynik DPIA (akceptowalne = 40%)	SUMA	0			Suma przed zabezpieczeniami=	0	Suma po zabezpieczeniach=
	OCENA RYZYKA	Ryzyko dla procesu przed zastosowaniem zabezpieczeń:				Ryzyko dla procesu po zastosowaniu zabezpieczeń:	