ZAŁĄCZNIK NR 12
do Polityki

Zasady i tryb zarządzania ryzykiem w ochronie danych osobowych

1.C e l

Administrator Danych Osobowych zapewnia warunki niezbędne do prawidłowego funkcjonowania procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w jednostce. Dlatego też w zgodnie z art. **5** ust **2** oraz Preambułą **75**, **76** i **85 RODO** –wprowadza zasady zarządzania ryzykiem ochrony danych osobowych.
Zasada podejścia opartego na ryzyku zobowiązuje administratora do przeprowadzania szczegółowej analizy prowadzonych procesów przetwarzania danych i dokonywania samodzielnej oceny ryzyka, na jakie przetwarzane dane w konkretnym przypadku są narażone. Zasada podejścia opartego na ryzyku **zobowiązuje Administratora Danych** do:

- ✓ respektowania ochrony praw i wolności osób, których dane dotyczą,
- ✓ dostosowania środków ochrony przetwarzania danych osobowych do skali ryzyka,
- ✓ poszukania środków redukujących prawdopodobieństwo wystąpienia zagrożeń najbardziej dotkliwych oraz środków redukujących skutki ich wystąpienia.

Celem niniejszego dokumentu jest ustanowienie metodyki zarządzania ryzykiem w zakresie zagrożeń wynikających z przetwarzania danych osobowych, z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą Analiza przeprowadzana jest w celu podjęcia decyzji o wymaganych środkach bezpieczeństwa w zidentyfikowanych procesach przetwarzania danych osobowych. Niniejsze zasady określają sposób przeprowadzania i dokumentowania procesu szacowania **ogólnej oceny ryzyka** naruszenia praw lub wolności osób fizycznych, oparte o materiały publikowane przez Urząd Ochrony Danych Osobowych, takie jak: *Jak rozumieć podejście oparte na ryzyku?* oraz *Jak stosować podejście oparte na ryzyku?*.

2.D e f i n i c j e

Administrator Danych - oznacza organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przewarzania danych osobowych;
Aktywa - kontrolowane przez jednostkę zasoby, są to środki materialne oraz personel umożliwiające dokonywanie operacji przetwarzania danych dla procesu przetwarzania danych;
Aktywa podstawowe - to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem jednostki (w tym, dane osobowe);
Aktywa wspierające – to środki umożliwiające korzystanie z aktywów podstawowych, np. sprzęt, oprogramowanie, sieć, pracownicy;
Akceptowanie ryzyka – decyzja, aby zaakceptować ryzyko;
Bezpieczeństwo danych osobowych - zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania;
Czynność przetwarzania – zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane;
Identyfikowanie ryzyka – szereg czynności polegających na określeniu sytuacji, które mogą się wydarzyć i spowodować straty/naruszenie;
Integralność :

a) danych – właściwość, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
b) systemu – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;

Kontekst – informacje wiążące się z działaniem jednostki, min. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych;
Kryteria akceptacji ryzyka – to kryteria, które określają dopuszczalność danego ryzyka;
Kryteria oceny ryzyka – to kryteria, które określają poziomy odniesienia, względem których określa się wartość ryzyka;
Akceptacja ryzyka – określenie dopuszczalności danego ryzyka, definiowane poprzez wartość progową, przy przedziałach ryzyka;
Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Ochrona danych osobowych – to bezpieczeństwo informacji, polegające na zabezpieczeniu poufności, integralności oraz dostępności informacji;
Ocena ryzyka – czynność polegająca na porównaniu wyników uzyskanych podczas analizy z kryteriami oceny ryzyka z kryteriami akceptacji ryzyka określonymi na etapie ustanowienia kontekstu działania jednostki; każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, **taka jak**: *zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, przeglądanie, ujawnianie poprzez przesyłanie, rozpowszechnianie , usuwanie, niszczenie;*
Operacja przetwarzania danych osobowych – każda czynność wykonywania na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, **taka jak:** *zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;*
Podatność – należy przez to rozumieć słabość - właściwość zapewniająca, ze informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
Poufność – właściwość zapewniająca, ze informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
Proces przetwarzania danych osobowych – to zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania;
Rejestr – rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 RODO;
Rozliczalność – właściwość zapewniająca, że działania podmiotu (np. użytkownika) mogą być jednoznacznie przyporządkowane tylko temu podmiotowi;
Ryzyko – według Rozporządzenia (RODO) – jako ryzyko rozumie się naruszenie praw i wolności osób fizycznych, których dane są przetwarzane; przez ryzyko należy rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów; ryzyko jest mierzone wpływem (skutkami) oraz prawdopodobieństwem wystąpienia;
Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka;
Właściciel ryzyka – właściciel procesu, czyli osoba odpowiedzialna za konkretny proces przetwarzania danych i mająca prawo podejmowania w tym zakresie decyzji , np. (osoba określona w strukturze regulaminu organizacyjnego);
Zagrożenie – to potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji;
Źródło ryzyka – potencjalna przyczyna niepożądanego incydentu, który może wywołać naruszenie praw lub wolności osób fizycznych;

3.Działania zmierzające do ustalenia kontekstu w związku z prowadzoną działalnością

Szkoła realizuje **cele i zadania** wynikające z przepisów prawa, (tj. art. 98 ust. 1 pkt. 4 – prawa oświatowego) oraz sposób ich wykonywania, w tym w zakresie udzielania pomocy psychologiczno-pedagogicznej, organizowania opieki nad dziećmi niepełnosprawnymi, umożliwiania uczniom podtrzymywania poczucia tożsamości narodowej, etnicznej, językowej i religijnej, z uwzględnieniem zasad bezpieczeństwa oraz zasad promocji i ochrony zdrowia.
Przedszkole realizuje cele i zadania wynikające z ustawy o systemie oświaty oraz z aktów wykonawczych do ustawy, w tym w szczególności z podstawy programowej wychowania przedszkolnego. Celem przedszkola jest, min. wspomaganie dzieci w rozwijaniu uzdolnień oraz kształtowania czynności intelektualnych potrzebnych im w codziennych sytuacjach i w dalszej edukacji.

4.Określenie informacji i uwarunkowań związanych z działaniem Administratora Danych oraz zakresu przetwarzanych danych

Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS, systemie teleinformatycznym System Informacji Oświatowej – danych osobowych uczniów/wychowanków, ich rodziców (opiekunów prawnych).
Przetwarzanie danych osobowych w **Zespole** odbywa się na serwerze i na stacjach roboczych użytkowników przy wykorzystaniu programów, systemów wspomagających pracę i oraz zarządzanie jednostką.

Z uwagi na rodzaj i charakter danych osobowych zawartych w zbiorach identyfikuje się następujące przypadki przetwarzania danych:

a) ***dane osobowe zwykłe*** – dane osobowe niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie (np. w przepisach kodeksu postępowania administracyjnego: dane osobowe stron postępowania, dane osobowe uczestników postępowania, dane osobowe uczniów itp.);

b) ***dane szczególnych kategorii danych osobowych i dane karne*** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, których przetwarzanie jest dopuszczalne w związku z art.9 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). Całość procesu przetwarzania opiera się o przesłanki określone w art. 9 ust. 2 i art. 10 RODO;

c) ***dane niezidentyfikowane*** - do głównych procesów przetwarzania danych niezidentyfikowanych dochodzi w ramach stosowanego monitoringu wizyjnego, którego reguły działania ustala odrębna instrukcja postępowania oraz oznaczono miejsca tabliczką informującą o objęciu terenu, czy pomieszczeń monitorowaniem.

Dane osobowe przetwarzane u administratora mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

5.Określenie procesów oraz aktywów (zasobów)

1. Procesy przetwarzania danych osobowych

Prawidłowe wyodrębnienie procesów jest niezbędne do zapewnienie skutecznej ochrony przetwarzanych danych oraz realizacji obowiązków wynikających z RODO. Posiadając wiedzę na temat przetwarzanych w organizacji danych osobowych oraz celach ich przetwarzania jesteśmy w stanie:

- ✓ zweryfikować, czy dysponujemy *odpowiednią podstawą prawną* do przetwarzania tych danych,
- ✓ ustalić, czy stosujemy się do jednej z kluczowych *zasad przetwarzania danych – minimalizacji,* czyli czy przetwarzamy wyłącznie te dane, które są niezbędne do realizacji celu w danym procesie,
- ✓ określić *retencje danych,* czyli okres przez jaki będziemy przechowywać dane osobowe przetwarzane w danym procesie,
- ✓ stworzyć i z powodzeniem *prowadzić rejestr czynności przetwarzania,*
- ✓ prawidłowo nadać pracownikom *upoważnienia do przetwarzania danych osobowych.*

Procesy związane z przetwarzaniem danych osobowych zostały opisane w rejestrze czynności przetwarzania danych osobowych, w ramach zapewnienia zgodności z art. 30 RODO, np. proces: **Bezpieczeństwo i Higiena Pracy,** cel przetwarzania danych: wypełnienie obowiązków przewidzianych w przepisach prawa, związanych z bezpieczeństwem i higieną pracy.

Aktywa (zasoby) związane z przetwarzaniem danych osobowych (wspierające realizację czynności przetwarzania)

Kategoria aktywów (zasobów)	Zasoby szczegółowe	Przykłady:
PODSTAWOWE		
PROCESY	Dokumentacja tradycyjna Systemy informatyczne	*ewidencja pracowników, rejestr wniosków o udostępnienie informacji publicznej; rejestr korespondencji (EOD)*
DZIAŁANIA BIZNESOWE	Działalność jednostki - obsługa spraw obywateli w ramach działalności statutowej, realizacji umów	*przyjmowanie wniosków i wydawanie decyzji zgłoszenia do ubezpieczeń społecznych ze środków publicznych, umowy o pracę*
DANE OSOBOWE (INFORMACJE)	1.Źródła pozyskiwania danych osobowych (dane zewnętrzne, wewnętrzne). 2.Kategorie osób i podmiotów, od których są pozyskane dane. 3.Rodzaj danych (dane osobowe zwykłe; szczególnej kategorii; dane niezidentyfikowane).	*informacje niezbędne dla funkcjonowania jednostki (w tym dane osobowe) - dane są zawarte w bazie danych : finansowe, pracowników, byłych pracowników, kontrahentów, obywateli załatwiających sprawy w jednostce.* *akta spraw, umowy, akta osobowe, książki adresowe, skorowidze zawierające dane osobowe itp.*
WSPIERAJĄCE		
PERSONEL	1.Użytkownicy systemów. 2.Pracownicy merytoryczni. 3.Użytkownicy sprzętu. 4.Administrator systemu. 5.Administrator Bazy Danych 6.Pracownicy obsługi 7.Współpracownicy (pracownicy zewnętrzni, stażyści, usługobiorcy).	*personel z pełnym lub ograniczonym dostępem do danych osobowych i uprawnieniami do ich przetwarzania*
SPRZĘT	1.Urządzenia do przetwarzania danych	*urządzenia automatycznego przetwarzania (np. systemy, macierze dyskowe*
	2.Urządzenia przenośne	*laptopy*
	3.Serwery	*serwery poszczególnych systemów*
	4.Urządzenia stacjonarne	*stanowiska komputerowe*
	5.Urządzenia	*drukarka, kopiarka, rutery, skanery*
	6.Nośniki danych elektroniczne	*CD-ROM, pendrive*
	7.Inne nośniki	*fax, slajd, wydruk*
OPROGRAMOWANIE	1.System operacyjny	*Windows,*
	2.Systemy informatyczne	*wspierające działalność np. finansowo-księgową*
	3.Baza danych	*finansowa, pracowników, byłych pracowników, kontrahentów, obywateli załatwiających sprawy w jednostce,*
	4.Pakiety oprogramowania lub oprogramowanie standardowe	*program kadrowy,* *pakiet biurowy (np. MS Office, przeglądarki)*
	5.Aplikacje stworzone na zamówienie	*SIO, VULCAN, UONET+*
SIEĆ	Okablowanie wewnętrzne Połączenie z siecią zewnętrzną (INTERNET)	*bezprzewodowy, szerokopasmowy*
SIEDZIBA	1.Budynki 2.Pomieszczenia biurowe 3.Pomieszczenia specjalne 4.Pomieszczenia będące w dyspozycji podmiotu	*stanowiska pracy, pracownia informatyczna, archiwum, pomieszczenia gospodarcze*
ORGANIZACJA	1.Struktura organizacyjna	*regulamin organizacyjny, procedury, dokumenty*
	2.Podwykonawcy	*dokumenty, procedury, umowy dot. przetwarzania danych osobowych*

2.**Wartość aktywów (zasobów):**

Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności.

Do istotności wartości aktywów (zasobów) należy przyjąć następujące wartości:

Ocena wpływu	Wartość	Opis
Krytyczne	**5**	Zasób jest krytyczny dla funkcjonowania organizacji, bez niego nie można realizować statutowych zadań (w tym czynności przetwarzania danych), może doprowadzić do przerwania ciągłości działania. Utrata danych osobowych szczególnej kategorii danych – utrata danych powoduje wysokie kary oraz odszkodowania.
Bardzo ważne	**4**	Zasób jest bardzo ważny dla funkcjonowania organizacji; utrata lub naruszenie bezpieczeństwa aktywa może powodować przerwanie procesów statutowych.
Duże	**3**	Zasób jest ważny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa może mieć wpływ na realizację zdań statutowych (w tym, czynności przetwarzania) - powoduje utrudnienia w normalnym funkcjonowaniu jednostki.
Umiarkowane	**2**	Zasób jest średnio ważny dla funkcjonowania organizacji, nieznacznie wpływa na realizację zadań statutowych (w tym czynności przetwarzania). utrata lub naruszenie bezpieczeństwa aktywa powoduje utrudnienia w normalnym funkcjonowaniu procesu biznesowego
Mało istotne	**1**	Zasób jest mało istotny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa nie ma wpływu na realizację statutowych zadań (w tym czynności przetwarzania).

6.Określenie właściciela ryzyka

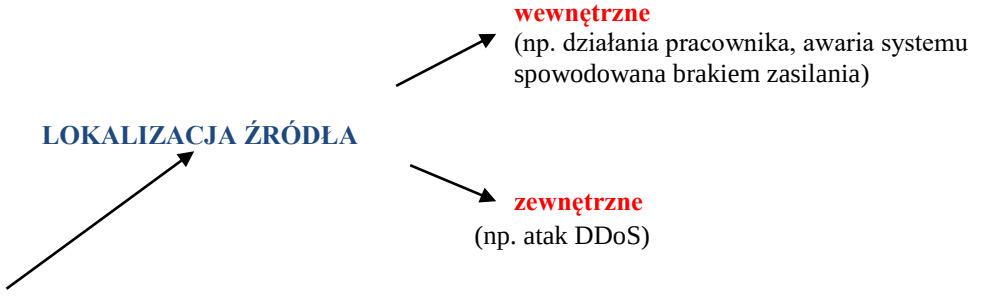
Właścicielem ryzyka w każdym przypadku jest osoba decyzyjna w komórce organizacyjnej za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. koordynator, samodzielne stanowisko pracy. Właściciel ryzyka został wskazany w rejestrze czynności przetwarzania danych osobowych.

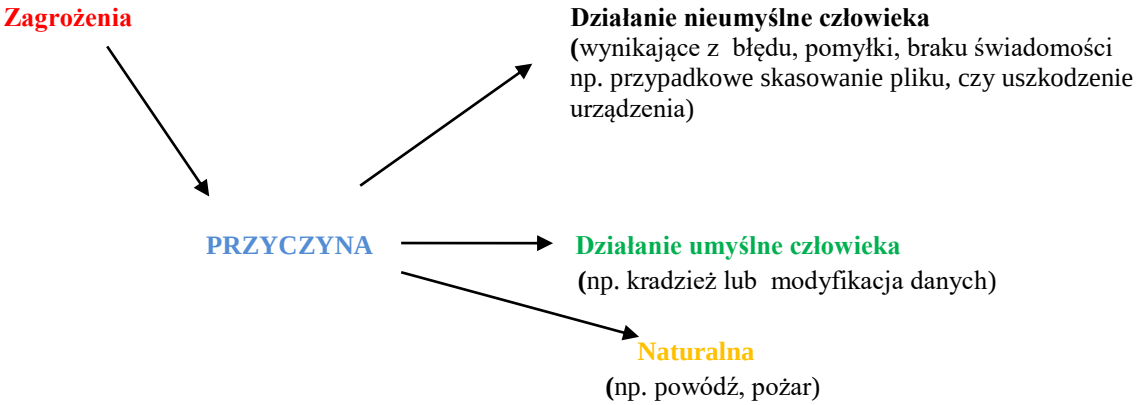
7.Identyfikacja zagrożeń na potrzeby szacowania ryzyka dla bezpieczeństwa danych

Zagrożenia możemy podzielić na **dwie grupy** :

1) **do pierwszej grupy** należy zaliczyć zagrożenia związane z **naruszeniem bezpieczeństwa i przetwarzania danych osobowych,** które można zidentyfikować w oparciu o normę PN-EN-150/IEC 27001. W tym obszarze znajdują się ryzyka związane z poufnością, integralnością oraz dostępnością przetwarzanych danych niezależnie od tego, czy te dane przetwarzane są w postaci elektronicznej, czy papierowej, czy przekazywane są ustnie. Zagrożenia te rodzą skutki: finansowe, prawne oraz utratę reputacji w wyniku naruszenia prywatności. **Bezpieczeństwo danych osobowych może zostać naruszone przypadkowo lub poprzez niezgodne z prawem zniszczenie, utratę, modyfikację, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych (np. kradzież).**

W najprostszym ujęciu zagrożenia można podzielić ze względu na lokalizację (umiejscowienie) ich źródła oraz przyczynę ich powstawania, co prezentuje **rysunek**.





2) **do drugiej grupy** należy zaliczyć zagrożenia związane z **naruszeniem praw lub wolności osób fizycznych,** związane z: profilowaniem danych; realizacją praw osób do usunięcia, przenoszenia lub wycofania zgody na przetwarzanie danych; możliwości kradzieży tożsamości, naruszenia dobrego imienia, dyskryminacji lub negatywnych skutków finansowych, nie wypełnienie obowiązku informacyjnego.

Zagrożenia scharakteryzowane w tej grupie można podzielić na:

a) organizacyjne (*np. brak polityki, regulaminów*)
b) personalne (*np. brak weryfikacji uprawnień, umów o zachowaniu poufności*)
c) fizyczne (*np. brak sytemu alarmowego, krat*)
d) techniczne (*np. brak zabezpieczenia systemem antywirusowym, firewall*).

W przypadku danych osobowych, zgodnie z RODO, należy przeprowadzić identyfikację zagrożeń dla każdej operacji przetwarzania danych osobowych *(zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie).*

Lista potencjalnych zagrożeń w obszarze przetwarzania danych znajduje się w Załączniku nr 1 do niniejszych zasad. Wskazany katalog zagrożeń nie jest listą zamkniętą.

8.Skutki wystąpienia zidentyfikowanych zagrożeń

Ocena skutku dla poszczególnych zagrożeń :

1) Skutki dla osób fizycznych, których prawa lub wolności zostały naruszone określa motyw 75 RODO:

- ✓ dyskryminacja osób, których dane dotyczą,
- ✓ kradzież tożsamości lub sfałszowanie (oszustwo) tożsamości osoby fizycznej,
- ✓ strata finansowa osób fizycznych, których dane dotyczą,
- ✓ naruszenie dobrego imienia osób fizycznych, których dane dotyczą,
- ✓ ograniczenie praw osób, których dane dotyczą,
- ✓ utrata kontroli nad własnymi danymi osobowymi,
- ✓ nieuprawnione odwrócenie pseudonimizacji danych osób fizycznych

Na potrzeby oceny ryzyka naruszenia praw lub wolności osób fizycznych każdy analizowany skutek zagrożenia należy oceniać (w skali od **0** do **3**) poprzez wykorzystanie skal opisanych w poniższej tabeli:

Ocena skutków naruszenia praw lub wolności osób fizycznych			**Skutki wystąpienia naruszenia** praw lub wolności osób fizycznych		
Wartość	**Nazwa**	**Opis**	**Skutek prawny**	**Skutek finansowy**	**Skutek wizerunkowy**
3	**wysokie**	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych	*bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych*	*wystąpienie zagrożenia spowoduje straty finansowe w wysokości powyżej 100 tys. zł*	*wystąpienie zagrożenia powoduje istotny lub duży negatywny wpływ na wizerunek jednostki, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w wysokości powyżej 100 tys. zł*
2	**średnie**	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie	*wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa, z wyłączeniem przepisów karnych, lub w przypadku niepodjęcia odpowiednich działań naprawczych naruszenie prawa zostanie nieuniknione*	*wystąpienie zagrożenia spowoduje straty finansowe w maksymalnej wysokości do 100 tys. zł*	*wystąpienie zagrożenia ma mało znaczący negatywny wpływ na wizerunek jednostki lub krótkoterminową utratę wizerunku, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w maksymalnej wysokości do 100 tys. zł;*
1	**niskie**	Identyfikuje się nieznaczne skutki mogące prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych	*wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa*	*wystąpienie zagrożenia nie spowoduje strat finansowych*	*wystąpienie zagrożenia nie ma wpływu na wizerunek ADO lub ten wpływ jest znikomy, nie wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku*
0	**nie dotyczy**	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*

Na potrzeby oceny ryzyka utraty **poufności, integralności lub rozliczalności** każdy analizowany skutek zagrożenia należy oceniać (w skali od **1**do **4**):

Podczas doboru wartości przypisywanej skutkowi utraty poufności (Sp) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli utrata poufności dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji
2	Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji
3	Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, wpływa w sposób znaczący na wizerunek urzędu i organu, który ten urząd obsługuje, jednak nie wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, jednak może wiązać się z odpowiedzialnością administracyjną
4	Jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i może prowadzić do roszczeń odszkodowawczych ze strony tych osób, a także do odpowiedzialności karnej osób odpowiedzialnych za zapewnienie ochrony takiej informacji

Podczas doboru wartości przypisywanej skutkowi utraty integralności (Si) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest łatwo wykrywalna i przywrócenie integralności nie powoduje nadmiernych kosztów
2	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych, jednak istnieje możliwość skorygowania decyzji
3	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych i nie istnieje możliwość skorygowania decyzji należy przyjąć
4	Jeżeli spowodowana zagrożeniem utrata integralności informacji może okazać się niewykrywalna należy przyjąć

Podczas doboru wartości przypisywanej skutkowi utraty dostępności (Sd) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany materializacją zagrożenia, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), a przywrócenie pełnego dostępu do informacji lub usług systemu nie wiąże się z dodatkowymi kosztami
2	Jeżeli okres czasu utraty dostępności informacji lub usług, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), ale przywrócenie dostępu do informacji wiąże się z dodatkowymi kosztami
3	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, znacząco nie mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO) należy przyjąć
4	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, wielokrotnie przekracza czas założony w planie zapewnienia ciągłości działania (RTO) lub jeżeli spowodowana zagrożeniem utrata dostępności informacji jest nieodwracalna należy przyjąć

9.Identyfikacja podatności (prawdopodobieństwa) wystąpienia zdarzenia

W przypadku zidentyfikowanych aktywów można wyróżnić następujące podatności:

- ✓ sprzęt *(wrażliwość na zmiany temperatury; wrażliwość na zmiany zasilania),*
- ✓ oprogramowanie *(brak mechanizmów uwierzytelniania; brak aktualnych poprawek bezpieczeństwa),*
- ✓ sieć *(brak szyfrowania transmisji; brak refundacji sprzętu),*
- ✓ personel *(brak procedur rekrutacji; praca bez nadzoru),*
- ✓ siedziba *(brak kontroli dostępu; brak fizycznej ochrony budynku),*
- ✓ struktura organizacyjna *(brak planów ciągłości; niewykonywanie audytów).*

Dla każdego zestawu „ czynność przetwarzania – zagrożenie – skutek" należy ocenić prawdopodobieństwo wystąpienia zagrożenia dla poszczególnych aktywów – według przyjętej poniżej tabeli:

Ocena prawdopodobieństwa wystąpienia zagrożenia dla poszczególnych aktywów		
Wartość	**Nazwa**	**Opis**
5	**bardzo prawdopodobne**	Istnieją racjonalne przesłanki by ocenić, ze zagrożenie wystąpi **(istnieje więcej niż 50% szans na wstąpienie)**. Zagrożenie miało miejsce w **przeciągu ostatniego roku.**
4	**prawdopodobne**	Wystąpienie zagrożenia jest realne, lecz **nie przekracza 50%** prawdopodobieństwa. Zagrożenie występuje sporadycznie i miało miejsce w **przeciągu ostatnich 2 lat.**
3	**możliwe**	Wystąpienie zagrożenia **jest możliwe**. Zagrożenie miało miejsce w **przeciągu ostatniego tygodnia.**
2	**mało prawdopodobne**	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest **znikoma (bliska zeru)**.
1	**rzadkie**	Zagrożenie występuje **raz w roku.**

10.Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych

Administrator danych określa :

a) akceptowany poziom zagrożenia (ryzyka) na poziomie nieznacznym (niskim).
b) do każdego nieakceptowanego poziomu zagrożenia podejmuje się decyzję określającą sposób reakcji tj. podjęcia działań zmierzających do zmniejszenia zagrożenia do poziomu akceptowalnego.

Ocena powagi ryzyka obliczana jest według poniższego wzoru:

$$\mathbf{R = P \times S}$$

gdzie:

R - ocena powagi ryzyka naruszenia praw i wolności osób fizycznych, lub ryzyka dla bezpieczeństwa przetwarzanych informacji

P - prawdopodobieństwo urzeczywistnienia się zagrożenia (od **0** do **5**)

S - skutek naruszenia praw lub wolności osób fizycznych (wartość przypisana od **0** do **3**); natomiast skutek dla poufności informacji, integralności informacji, dostępności informacji (należy przypisać wartość od **1** do **4**) ponadto należy sumować skutki według wzoru **S = Sp +Si +Sd.**

Oszacowaną wartość danego zagrożenia przyporządkowuje się odpowiedniemu poziomowi ryzyka według poniższej tabeli (matrycy budowy poziomu Ryzyka) :

SKUTEK (S)	**Krytyczne**	**10**	**30**	**60**	**80**	**100**
	Poważne	**8**	**24**	**48**	**64**	**80**
	Średnie	**6**	**18**	**36**	**48**	**60**
	Małe	**3**	**9**	**18**	**24**	**30**
	Nieznaczne	**1**	**3**	**6**	**8**	**10**
		Rzadkie	**Mało prawdopodobne**	**Możliwe**	**Prawdopodobne**	**Bardzo prawdopodobne**
		PRAWDOPODOBIEŃSTWO (P)				

gdzie :

Ryzyko	Opis reakcji na ryzyko
Ryzyko NISKIE	Poziom ryzyka akceptowalny, nie wymaga dalszego postępowania. Niskie szkody w przypadku wystąpienia zagrożeń.
Ryzyko ŚREDNIE	Poziom ryzyka umiarkowany. Wymaga stałego monitorowania. Działalnie ograniczające ryzyko do poziomu akceptowalnego. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot.
Ryzyko WYSOKIE	Poziom ryzyka nieakceptowany. Wymaga dalszego postępowania z ryzykiem oraz zaplanowanie ochrony danych osobowych. Należy dokonać wyboru wariantu postępowania z ryzykiem.
Ryzyko KRYTYCZNE	**Poziom ryzyka nieakceptowany** (maksymalny) – powoduje wysokie szkody i wymaga natychmiastowego działania.

W celu przeciwdziałania postępowania z ryzykiem Administrator Danych podejmuje decyzję, co do postępowania **z ryzykiem .** Reakcja Administratora na ryzyko może obejmować :

1) **działanie polegające na modyfikowaniu ryzyka (minimalizacja ryzyka)** – reakcje mające na celu wyeliminowanie danego ryzyka lub uwarunkowań z nim związanych w celu ochrony przed skutkami osób fizycznych,
2) **łagodzenie (czyli unikanie) ryzyka** – zmniejszenie prawdopodobieństwa lub skutków niekorzystnego zdarzenia do akceptowalnego poziomu,
3) **przeniesienie** – próba transferu skutków wystąpienia ryzyka na inny pomiot**,** np. przez wykupienie ubezpieczenia od jakiegoś ubezpieczenia lub scedowanie skutków ryzyka na firmę współpracująca (stosowny zapis w umowie powierzenia).
4) **akceptację** - aktywną (stworzenie planu działania na wypadek wystąpienia ryzyka) lub bierną (niepodejmowanie żadnych działań do momentu wystąpienia ryzyka)

11.Monitorowanie i przegląd ryzyka u administratora

1. Wprowadza się obowiązek oceny ryzyka i zarządzania ryzkiem w zakresie ochrony danych osobowych, która stanowi element kontroli zarządczej u administratora.
2. Monitorowanie i ocena ryzyk prowadzona jest w sposób ciągły.
3. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności jednostki, dokonywany jest przez IOD we współpracy osobami odpowiedzialnymi za poszczególne obszary działalności jednostki (właścicielami ryzyka) oraz informatykiem w zakresie systemu informatycznego.
4. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko.
5. **Kwestionariusz oceny ryzyka** (kwestionariusz samooceny) przygotowany przez Inspektora Ochrony Danych jest rozsyłany pracownikom komórki lub osobie kierującej dana komórką organizacyjną do wypełnienia.- **do dnia 30 kwietnia każdego roku.**
6. **Informatyk corocznie w terminie do 30 kwietnia każdego roku** przeprowadza regularnie analizę ryzyk w obszarze przetwarzania danych osobowych **w systemie informatycznym**.
7. Na podstawie otrzymanych wyników szacowania ryzyka ochrony danych osobowych przez poszczególnych właścicieli ryzyk – Inspektor Ochrony Danych dokonuje **w terminie do 30 czerwca każdego roku** szacowania ryzyka ochrony danych osobowych, który przedstawia do zatwierdzenia Administratorowi Danych Osobowych.

ZAŁĄCZNIK NR 1
do analizy ryzyka

Lista potencjalnych RYZYK w obszarze przetwarzaniu danych osobowych wynikających z ewentualnych zagrożeń :

1.Ryzyko dotyczące naruszeniem bezpieczeństwa i przetwarzaniem danych osobowych, wynikające z zagrożeń:

a) przypadkowe zniszczenie

- błędy i pomyłki użytkowników,
- samodzielne instalowanie oprogramowania niebędącego własnością administratora danych,
- samodzielne modyfikowanie parametrów systemu i aplikacji,

b) niezgodne z prawem zniszczenie

- błędy ludzkie (nieświadome lub celowe) błędy i pomyłki użytkowników,
- atak wirusa,
- wyrzucenie akt, dokumentów lub nośników elektronicznych zawierających dane osobowe w formie ich odczytania – niewłaściwe ich zniszczenie,
- zdarzenia zamierzone przez człowieka świadome i celowe np. kradzież danych lub sprzętu,

c) utrata danych :

- nie przestrzeganie zasady czystego biurka i czystego ekranu,
- celowe lub przypadkowe zniszczenie danych,
- zniszczenie danych osobowych poprzez błędy i omyłki użytkowników (przypadkowe lub celowe),
- podłączenie jakichkolwiek urządzeń obcych do sieci komputerowej, demontaż urządzeń ,
- przechowywanie danych (dokumentacji tradycyjnej) w sposób niezapewniający ich utraty oraz przed dostępem osób nieuprawnionych,
- pozostawienie akt i dokumentów zawierających dane osobowe bez nadzoru (np. w niezamkniętych pomieszczeniach lub w miejscach dostępnych przez osoby z zewnątrz), np. kradzież
- utrata kontroli nad kopia dokumentów zawierających dane osobowe,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- atak wirusa,
- klęska żywiołowa, wypadek, zdarzenie, w wyniku których utracono poufność danych osobowych,
- niezabezpieczenie danych w systemie przed utrata danych spowodowaną - awarią sprzętu, awarią zasilania lub zakłóceniami sieci zasilającej (odcięcie zasilania) np. niestosowanie UPS, generatora prądotwórczego.
- wadliwe działanie oprogramowania

d) modyfikacja:

- nieuzasadniona zmiana danych,
- uszkodzenie danych,
- celowe lub przypadkowe zniszczenie danych,
- samodzielne modyfikowanie parametrów systemu i aplikacji,
- włamanie do systemu komputerowego,
- błędy i pomyłki użytkowników,
- zignorowanie stwierdzenia śladów manipulacji przy elementach sieci komputerowej, komputerach lub programach komputerowych, poprzez:

✓ zignorowanie stwierdzenia obecności nowych kabli, urządzeń i programów o nieznanym pochodzeniu,

✓ zignorowanie niezapowiedzianych zmian w wyglądzie lub zachowaniu wykorzystywanych aplikacji komputerowych lub sprzętu,

✓ zignorowanie obecności na komputerze lub w systemie nieoczekiwanych nowych programów lub zmian konfiguracji oprogramowania.

- Zignorowanie śladów włamania do pomieszczeń,

e) nieuprawnione ujawnienie:

- osobom nieuprawnionym danych osobowych, sposobu ich zabezpieczenia lub stworzenie im warunków umożliwiających pozyskanie wiedzy w tym zakresie, poprzez**:**
- umożliwienie osobom nieupoważnionym (umyślnie lub nieumyślnie) odczytanie danych osobowych z ekranu monitora (niewłaściwe ustawienie stanowiska komputerowego - monitora),
- nieprzestrzeganie procedury postępowania w trakcie pacy oraz po jej zakończeniu (zasada czystego ekranu i czystego biurka),
- opuszczenie stanowiska pracy z pozostawieniem aktywnej aplikacji umożliwiającej dostęp do danych osobowych,
- dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania (aplikacji) osobie nieupoważnionej – osobie innej niż osoba, której został przydzielony identyfikator,
- pozostawienie obszaru przetwarzania bez nadzoru,
- pozostawienie w miejscu widocznym zapisanego identyfikatora i hasła dostępu do systemu, lub kont i haseł dostępu administratorów,
- ujawnienie osobie nieupoważnionej informacji dotyczących zabezpieczenia systemu informatycznego lub dokumentacji tradycyjnej,
- nie zachowanie w tajemnicy danych oraz sposobu ich zabezpieczenia (np. plotkarstwo osób upoważnionych do przetwarzania danych):
  - ✓ przechowywanie danych (dokumentacji tradycyjnej) w sposób niezapewniający ich utraty oraz przed dostępem osób nieuprawnionych,
  - ✓ pozostawienie akt i dokumentów zawierających dane osobowe bez nadzoru (np. w niezamkniętych pomieszczeniach lub w miejscach dostępnych przez osoby z zewnątrz),
  - ✓ wyrzucenie akt , dokumentów lub nośników elektronicznych zawierających dane osobowe w formie ich odczytania,
  - ✓ dopuszczenie do kopiowania dokumentów zawierających dane osobowe przez osoby nieuwapnione.

f) nieuprawniony dostęp

- osobom nieuprawnionym udostępnienie danych osobowych, sposobu ich zabezpieczenia lub stworzenie im warunków umożliwiających pozyskanie wiedzy, w tym zakresie, poprzez**:**
  - ✓ praca w systemie informatycznym na obcym koncie,
  - ✓ nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe,
- brak kontroli dostępu do aplikacji i systemów:
  - ✓ ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe.
  - ✓ nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
  - ✓ nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym,
- włamanie do systemu komputerowego - brak ochrony przed szkodliwym oprogramowaniem, którego celem jest uzyskanie dostępu do systemu informatycznego:
  - ✓ nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego lub urządzenia mobilnego,
  - ✓ brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika,
  - ✓ awaria sprzętu,
  - ✓ brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,

2.Ryzyko związane z bezpieczeństwem danych w związku z zagrożeniami utraty poufności, integralnością oraz dostępnością przetwarzanych danych :

a) zagrożenia związane z poufnością danych osobowych

- ✓ udostępnianie danych osobowych osobom nieupoważnionym,
- ✓ zabranie danych osobowych przez osobę nieuprawnioną,
- ✓ przełamanie zabezpieczeń fizycznych lub programowych,
- ✓ niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych,
- ✓ złamanie obowiązku zachowania tajemnicy przez osoby uprawnione do przetwarzania danych osobowych,
- ✓ nieuprawnione kopiowanie danych na zewnętrzne nośniki informacji (CD, DVD, pendrive, dyski w chmurze itp.), niekontrolowane kopiowanie danych,

- ✓ niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych,
- ✓ naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych,
- ✓ podsłuch lub podgląd danych osobowych,
- ✓ ujawnienie haseł dostępu do stanowiska komputerowego,
- ✓ klęska żywiołowa w wyniku, której utracono poufność danych,
- ✓ zdarzenia losowe wewnętrzne np. awaria sprzętu, błędy oprogramowania,

b)zagrożenia związane z brakiem integralności danych osobowych

- ✓ uszkodzenie celowe lub przypadkowe – systemu operacyjnego lub urządzeń sieciowych,
- ✓ celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
- ✓ infekcje wirusowe komputera, np. brak działania systemu operacyjnego,
- ✓ awaria sprzętu komputerowego,
- ✓ czynniki środowiskowe - pożar, zalanie, ekstremalna temperatura, itp.,
- ✓ zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny, włamanie, wirus),

c)zagrożenia związane z brakiem rozliczalności danych osobowych w systemie informatycznym

- ✓ nieprzydzielenie użytkownikom indywidualnych identyfikatorów,
- ✓ niewłaściwa administracja systemem informatycznym,
- ✓ niewłaściwa konfiguracja systemu informatycznego,
- ✓ zniszczenie/zafałszowanie logów systemowych,
- ✓ brak rejestracji udostępniania danych osobowych,
- ✓ podszywanie się pod innego użytkownika,
- ✓ niespełnianie przez system informatyczny wymogu odnotowania (daty pierwszego wprowadzenia identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
- ✓ źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
- ✓ informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,.

3.Ryzyko naruszenia praw lub wolności osób fizycznych – wynikających z RODO

- **a)** brak podstawy prawnej do zbierania, wykorzystywania lub ujawniania danych,
- **b)** przetwarzanie niekompletnych lub nieaktualnych danych,
- **c)** nieuzasadnione użycie lub ujawnienie danych,
- **d)** zbyt szeroki zakres przetwarzanych danych,
- **e)** przetwarzanie danych niezgodnie z pierwotnym celem,
- **f)** przetwarzanie danych po wygaśnięciu celu ich przetwarzania,
- **g)** przypadkowe lub niezgodne z prawem zniszczenie danych osobowych,
- **h)** ujawnienie danych nieuprawnionym podmiotom.

ZAŁĄCZNIK NR 2
do analizy ryzyka

Ankieta dotycząca bezpieczeństwa danych osobowych

1. Czy w jednostce wdrożona jest dokumentacja ochrony danych osobowych, w tym:
   a) Polityka bezpieczeństwa
      ☐ TAK ☐ NIE
   b) Instrukcja zarządzania systemem informatycznym?
      ☐ TAK ☐ NIE
2. Czy zatrudnione u Państwa osoby, które mają dostęp do danych osobowych, dysponują odpowiednimi upoważnieniami do ich przetwarzania?
   ☐ TAK ☐ NIE
3. Czy brali Państwo kiedykolwiek udział w szkoleniach z zakresu ochrony danych osobowych?
   ☐ TAK ☐ NIE
4. Czy w codziennej pracy zdarzają się Państwu problemy, wynikające z niewłaściwego zabezpieczenia danych lub nienależytej kontroli nad obiegiem dokumentów w Państwa jednostce?
   ☐ TAK ☐ NIE
5. Czy w Państwa jednostce zabezpiecza się dane osobowe poprzez środki ochrony fizycznej takie jak: zamykane pomieszczenia, zamykane szafy, biurka, strefy dostępu, instalację alarmową, monitoring, kraty lub żaluzje antywłamaniowe?
   ☐ TAK ☐ NIE ☐ CZĘŚCIOWO
6. Czy system informatyczny służący w Państwa jednostce do przetwarzania danych osobowych spełnia wymogi określone w przepisach prawa?
   ☐ TAK ☐ NIE
7. Czy rejestrowali Państwo jakiekolwiek zbiory danych osobowych w rejestrze prowadzonym przez GIODO?
   ☐ TAK ☐ NIE
8. Czy w Państwa strukturze wyznaczony został Inspektor Ochrony Danych?
   ☐ TAK ☐ NIE
9. Czy spełniają Państwo obowiązek informacyjny wobec:
   a) Swoich pracowników
   ☐ TAK ☐ NIE
   b) Swoich kontrahentów
   ☐ TAK ☐ NIE
   c) Swoich klientów
   ☐ TAK ☐ NIE
10. Czy potrafią Państwo wskazać, które z danych osobowych przetwarzanych w Państwa jednostce, należą do danych zwykłych, a które do danych wrażliwych?
    ☐ TAK ☐ NIE
11. Czy potrafią Państwo wskazać cel przetwarzania danych w odniesieniu do poszczególnych zbiorów danych, w których przetwarza się dane osobowe w Państwa jednostce?
    ☐ TAK ☐ NIE
12. Czy dysponują Państwo umowami powierzenia przetwarzania danych osobowych, podpisanymi przez Państwa jako Administratora Danych?
    ☐ TAK ☐ NIE
13. Czy osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania poufności tych danych?
    ☐ TAK ☐ NIE
14. Czy Państwa firma zajmuje się przetwarzaniem danych osobowych klientów zamieszkujących UE (wyłączając Polskę), czy też są to klienci spoza UE? *[Można zakreślić więcej niż jedną odpowiedź]*
    ☐ Tak, przetwarzamy dane osobowe jednostek zamieszkujących kraje UE
    ☐ Tak, przetwarzamy dane osobowe jednostek spoza UE (np. USA, kraje w Azji, czy Afryce)
    ☐ Nasza firma przetwarza dane osobowe klientów wyłącznie z Polski
    ☐ Nie wiem/ Nie dotyczy
15. Czy na Państwa stronie internetowej (jeśli taka istnieje) można zapoznać się z polityką prywatności, jaką firma stosuje?
    ☐ Tak ☐ Nie ☐ Nie wiem/ Nie dotyczy
16. Podmioty, których dane są przechowywane mają prawo wglądu do swoich danych osobowych, np. w celu wprowadzenia zmian, usunięcia danych, albo po prostu uzyskania kopi. Czy mieli już Państwo do czynienia z takimi przypadkami?
    ☐ Tak ☐ Nie ☐ Nie wiem/ Nie dotyczy

ZAŁĄCZNIK NR 3
do analizy ryzyka

Zidentyfikowany zasób (aktywa): DANE OSOBOWE
Wartość aktywa: 4
Właściciel ryzyka: Zespół Placówek Oświatowych nr 3 w Skarżysku-Kam.
Ryzyko dotyczące naruszeniem bezpieczeństwa i przetwarzaniem danych osobowych

LP	NAZWA ZAGROŻENIA	PRZYCZYNA	SKUTEK	OSZACOWANA WARTOŚĆ	
				Prawdopodobieństwa Skala (1-5)	Skutek Skala (0-3)
1	NARUSZENIE OCHRONY DANYCH OSOBOWYCH	**przypadkowe zniszczenie danych**	naruszenie zasad bezpieczeństwa informacji	2	1
		niezgodne z prawem zniszczenie danych	naruszenie zasad bezpieczeństwa informacji	2	1
		utrata danych	nieprzestrzeganie obowiązujących zasad kradzież atak wirusa	4	2
		modyfikacja	nieuzasadniony dostęp do danych osobowych włamanie do danych	2	1
		nieuprawnione ujawnienie	nieprzestrzeganie procedur nie zachowanie w tajemnicy danych	2	1
		nieuprawniony dostęp	nielegalny dostęp do stanowisk i pomieszczeń awaria sprzętu	2	1

Pieczęć i podpis właściciela ryzyka:

Dyrektor
mgr Bogumiła Sadza

Do istotności wartości aktywów (zasobów) należy przyjąć następujące wartości:

Ocena wpływu	Wartość	Opis
Krytyczne	**5**	Zasób jest krytyczny dla funkcjonowania organizacji, bez niego nie można realizować statutowych zadań (w tym czynności przetwarzania danych), może doprowadzić do przerwania ciągłości działania. Utrata danych osobowych szczególnej kategorii danych – utrata danych powoduje wysokie kary oraz odszkodowania.
Bardzo ważne	**4**	Zasób jest bardzo ważny dla funkcjonowania organizacji; utrata lub naruszenie bezpieczeństwa aktywa może powodować przerwanie procesów statutowych.
Duże	**3**	Zasób jest ważny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa może mieć wpływ na realizację zdań statutowych (w tym, czynności przetwarzania) - powoduje utrudnienia w normalnym funkcjonowaniu jednostki.
Umiarkowane	**2**	Zasób jest średnio ważny dla funkcjonowania organizacji, nieznacznie wpływa na realizację zadań statutowych (w tym czynności przetwarzania). utrata lub naruszenie bezpieczeństwa aktywa powoduje utrudnienia w normalnym funkcjonowaniu procesu biznesowego
Mało istotne	**1**	Zasób jest mało istotny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa nie ma wpływu na realizację statutowych zadań (w tym czynności przetwarzania).

Ocena prawdopodobieństwa wystąpienia zagrożenia dla poszczególnych aktywów		
Wartość	**Nazwa**	**Opis**
5	**bardzo prawdopodobne**	Istnieją racjonalne przesłanki by ocenić, ze zagrożenie wystąpi **(istnieje więcej niż 50% szans na wstąpienie)**. Zagrożenie miało miejsce w **przeciągu ostatniego roku.**
4	**prawdopodobne**	Wystąpienie zagrożenia jest realne, lecz **nie przekracza 50%** prawdopodobieństwa. Zagrożenie występuje sporadycznie i miało miejsce w **przeciągu ostatnich 2 lat.**
3	**możliwe**	Wystąpienie zagrożenia **jest możliwe**. Zagrożenie miało miejsce w **przeciągu ostatniego tygodnia.**
2	**mało prawdopodobne**	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest **znikoma (bliska zeru)**.
1	**rzadkie**	Zagrożenie występuje **raz w roku.**

Ocena skutków naruszenia praw lub wolności osób fizycznych			**Skutki wystąpienia naruszenia** praw lub wolności osób fizycznych		
Wartość	**Nazwa**	**Opis**	**Skutek prawny**	**Skutek finansowy**	**Skutek wizerunkowy**
3	**wysokie**	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych	*bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych*	*wystąpienie zagrożenia spowoduje straty finansowe w wysokości powyżej 100 tys. zł*	*wystąpienie zagrożenia powoduje istotny lub duży negatywny wpływ na wizerunek jednostki, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w wysokości powyżej 100 tys. zł*
2	**średnie**	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie	*wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa, z wyłączeniem przepisów karnych, lub w przypadku niepodjęcia odpowiednich działań naprawczych naruszenie prawa zostanie nieuniknione*	*wystąpienie zagrożenia spowoduje straty finansowe w maksymalnej wysokości do 100 tys. zł*	*wystąpienie zagrożenia ma mało znaczący negatywny wpływ na wizerunek jednostki lub krótkoterminową utratę wizerunku, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w maksymalnej wysokości do 100 tys. zł;*
1	**niskie**	Identyfikuje się nieznaczne skutki mogące prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych	*wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa*	*wystąpienie zagrożenia nie spowoduje strat finansowych*	*wystąpienie zagrożenia nie ma wpływu na wizerunek ADO lub ten wpływ jest znikomy, nie wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku*
0	**nie dotyczy**	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*

ZAŁĄCZNIK NR 3.1
do analizy ryzyka

Zidentyfikowany zasób (aktywa): PROGRAMY I SYSTEMY OPERACYJNE, SIEĆ
Wartość aktywa: 5
Właściciel ryzyka: Zespół Placówek Oświatowych nr 3 w Skarżysku-Kam.

Ryzyko związane z bezpieczeństwem danych w związku z zagrożeniami utraty poufności, integralności oraz dostępnością przetwarzanych danych

LP	NAZWA ZAGROŻENIA	PRZYCZYNA	SKUTEK	OSZACOWANA WARTOŚĆ	
				Prawdopodobieństwa Skala (1-5)	Skutek Skala (0-4)
1	NARUSZENIE POUFNOŚCI	zaniedbania ze strony pracowników np. nie przestrzeganie zasady czystego ekranu	nieuprawniony dostęp	4	2
		nieuprawniony dostęp do pomieszczenia lub pozostawienie pomieszczenia bez nadzoru	kradzież danych	4	2
		błędy popełniane przez użytkownika systemu np. samodzielne instalowanie oprogramowania	atak wirusa	4	2
		awaria sieci elektrycznej np. wichura	odcięcie zasilania	1	1
		utratę cennych danych lub uszkodzenie sprzętu komputerowego	awaria sprzętu	2	1
2	NARUSZENIE INTEGRALNOŚCI	nieprawidłowości przy przetwarzaniu danych przez osoby nieuprawnione brak kontroli nad stanowiskiem komputerowym	nieuprawniony dostęp	1	1
		zagubienie lub kradzież nośników danych np. komputerów przenośnych	kradzież danych	2	4
		infekcje wirusowe komputera np. brak działania systemu operacyjnego ataki hakerów	atak wirusa	4	2
		spadek napięcia elektrycznego brak zasilania np. UPS	odcięcie zasilania	3	1
		zbieranie się ładunków elektrostatycznych	awaria sprzętu	2	1
3	NARUSZENIE DOSTĘPNOŚCI	brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania	nieuprawniony dostęp	2	1
		podszywanie się pod innego użytkownika	kradzież	2	3
		awaria systemu operacyjnego lub ujawnienie wady oprogramowania aplikacyjnego	atak wirusa	4	3
		awaria zasilana	odcięcie zasilania	1	1

Pieczęć i podpis właściciela ryzyka:

Do istotności wartości aktywów (zasobów) należy przyjąć następujące wartości:

Ocena wpływu	Wartość	Opis
Krytyczne	**5**	Zasób jest krytyczny dla funkcjonowania organizacji, bez niego nie można realizować statutowych zadań (w tym czynności przetwarzania danych), może doprowadzić do przerwania ciągłości działania. Utrata danych osobowych szczególnej kategorii danych – utrata danych powoduje wysokie kary oraz odszkodowania.
Bardzo ważne	**4**	Zasób jest bardzo ważny dla funkcjonowania organizacji; utrata lub naruszenie bezpieczeństwa aktywa może powodować przerwanie procesów statutowych.
Duże	**3**	Zasób jest ważny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa może mieć wpływ na realizację zdań statutowych (w tym, czynności przetwarzania) - powoduje utrudnienia w normalnym funkcjonowaniu jednostki.
Umiarkowane	**2**	Zasób jest średnio ważny dla funkcjonowania organizacji, nieznacznie wpływa na realizację zadań statutowych (w tym czynności przetwarzania). utrata lub naruszenie bezpieczeństwa aktywa powoduje utrudnienia w normalnym funkcjonowaniu procesu biznesowego
Mało istotne	**1**	Zasób jest mało istotny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa nie ma wpływu na realizację statutowych zadań (w tym czynności przetwarzania).

Ocena prawdopodobieństwa wystąpienia zagrożenia dla poszczególnych aktywów		
Wartość	**Nazwa**	**Opis**
5	**bardzo prawdopodobne**	Istnieją racjonalne przesłanki by ocenić, ze zagrożenie wystąpi **(istnieje więcej niż 50% szans na wstąpienie)**. Zagrożenie miało miejsce w **przeciągu ostatniego roku.**
4	**prawdopodobne**	Wystąpienie zagrożenia jest realne, lecz **nie przekracza 50%** prawdopodobieństwa. Zagrożenie występuje sporadycznie i miało miejsce w **przeciągu ostatnich 2 lat.**
3	**możliwe**	Wystąpienie zagrożenia **jest możliwe**. Zagrożenie miało miejsce w **przeciągu ostatniego tygodnia.**
2	**mało prawdopodobne**	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest **znikoma (bliska zeru)**.
1	**rzadkie**	Zagrożenie występuje **raz w roku.**

Podczas doboru wartości przypisywanej skutkowi utraty poufności (Sp) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli utrata poufności dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji
2	Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji
3	Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, wpływa w sposób znaczący na wizerunek urzędu i organu, który ten urząd obsługuje, jednak nie wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, jednak może wiązać się z odpowiedzialnością administracyjną
4	Jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i może prowadzić do roszczeń odszkodowawczych ze strony tych osób, a także do odpowiedzialności karnej osób odpowiedzialnych za zapewnienie ochrony takiej informacji

Podczas doboru wartości przypisywanej skutkowi utraty integralności (Si) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest łatwo wykrywalna i przywrócenie integralności nie powoduje nadmiernych kosztów
2	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych, jednak istnieje możliwość skorygowania decyzji
3	Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych i nie istnieje możliwość skorygowania decyzji należy przyjąć
4	Jeżeli spowodowana zagrożeniem utrata integralności informacji może okazać się niewykrywalna należy przyjąć

Podczas doboru wartości przypisywanej skutkowi utraty dostępności (Sd) należy przyjąć następujące zasady:

Wartość	Opis
1	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany materializacją zagrożenia, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), a przywrócenie pełnego dostępu do informacji lub usług systemu nie wiąże się z dodatkowymi kosztami
2	Jeżeli okres czasu utraty dostępności informacji lub usług, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO), ale przywrócenie dostępu do informacji wiąże się z dodatkowymi kosztami
3	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, znacząco nie mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO) należy przyjąć
4	Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, wielokrotnie przekracza czas założony w planie zapewnienia ciągłości działania (RTO) lub jeżeli spowodowana zagrożeniem utrata dostępności informacji jest nieodwracalna należy przyjąć

ZAŁĄCZNIK NR 3.2
do analizy ryzyka

Zidentyfikowany zasób (aktywa): PERSONEL
Wartość aktywa: 4
Właściciel ryzyka: Zespół Placówek Oświatowych nr 3 w Skarżysku-Kam.

Ryzyko naruszenia praw lub wolności osób fizycznych – wynikających z RODO

LP	NAZWA ZAGROŻENIA	PRZYCZYNA	SKUTEK	OSZACOWANA WARTOŚĆ	
				Prawdopodobieństwa Skala (1-5)	Skutek Skala (0-3)
1	BRAK ZGODNOŚCI PRZETWARZANIA	brak zgody osoby, której dane dotyczą na przetwarzanie danych brak obowiązku wynikającego z przepisu prawa	brak podstawy prawnej do zbierania, wykorzystywania lub ujawniania danych (nieuprawniony sposób przetwarzania danych)	2	3
2	PRZETWARZANIE PO WYGAŚNIĘCIU CELU PRZETWARZANIA	przetwarzanie danych przez okres dłuższy niż to niezbędne do celu, w którym dane te są przetwarzane	nieuzasadnione użycie lub ujawnienie danych	2	2
3	PRZEKAZYWANIE DANYCH INNYM PODMIOTOM KTÓRE W IMIENIU ADMINISTRATORA WYKONUJĄ OPERACJE PRZETWARZANIA	brak umowy powierzenia danych lub innego dokumentu, który określa sposób przetwarzania danych	brak podstawy prawnej	2	2
4	NIESPEŁNIENIE OBOWIĄZKU INFORMACYJNEGO WOBEC OSÓB FIZYCZNYCH	brak klauzuli informacyjnej określającej cel, w którym zostały zebrane treść klauzul może być niezrozumiała	naruszenie procedur oraz przepisów prawa	2	2
5	NARUSZENIE ZASADY ”PRAWIDŁOWOŚCI”	przetwarzanie danych niekompletnych lub nieaktualnych	naruszenie procedur oraz przepisów prawa.	2	1
6	NARUSZENIE ZASADY INTEGRALNOŚCI I POUFNOŚCI	nieuprawniony dostęp do danych nieuprawnione modyfikowanie danych utrata danych, zniszczenie (przypadkowe lub celowe)	powiadomienie osób fizycznych o naruszeniu bezpieczeństwa danych naruszenie procedur oraz przepisów prawa	4	3
7	ZBIERANIE NADMIARU DANYCH NIEZGODNIE Z CELEM	nieprzestrzeganie zasady minimalizacji nieprzestrzeganie zasady ograniczenia celu	naruszenie przepisów prawa	2	1

Pieczęć i podpis właściciela ryzyka:

Do istotności wartości aktywów (zasobów) należy przyjąć następujące wartości:

Ocena wpływu	Wartość	Opis
Krytyczne	**5**	Zasób jest krytyczny dla funkcjonowania organizacji, bez niego nie można realizować statutowych zadań (w tym czynności przetwarzania danych), może doprowadzić do przerwania ciągłości działania. Utrata danych osobowych szczególnej kategorii danych – utrata danych powoduje wysokie kary oraz odszkodowania.
Bardzo ważne	**4**	Zasób jest bardzo ważny dla funkcjonowania organizacji; utrata lub naruszenie bezpieczeństwa aktywa może powodować przerwanie procesów statutowych.
Duże	**3**	Zasób jest ważny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa może mieć wpływ na realizację zdań statutowych (w tym, czynności przetwarzania) - powoduje utrudnienia w normalnym funkcjonowaniu jednostki.
Umiarkowane	**2**	Zasób jest średnio ważny dla funkcjonowania organizacji, nieznacznie wpływa na realizację zadań statutowych (w tym czynności przetwarzania). utrata lub naruszenie bezpieczeństwa aktywa powoduje utrudnienia w normalnym funkcjonowaniu procesu biznesowego
Mało istotne	**1**	Zasób jest mało istotny dla funkcjonowania organizacji, utrata lub naruszenie bezpieczeństwa aktywa nie ma wpływu na realizację statutowych zadań (w tym czynności przetwarzania).

Ocena prawdopodobieństwa wystąpienia zagrożenia dla poszczególnych aktywów		
Wartość	**Nazwa**	**Opis**
5	**bardzo prawdopodobne**	Istnieją racjonalne przesłanki by ocenić, ze zagrożenie wystąpi **(istnieje więcej niż 50% szans na wstąpienie)**. Zagrożenie miało miejsce w **przeciągu ostatniego roku.**
4	**prawdopodobne**	Wystąpienie zagrożenia jest realne, lecz **nie przekracza 50%** prawdopodobieństwa. Zagrożenie występuje sporadycznie i miało miejsce w **przeciągu ostatnich 2 lat.**
3	**możliwe**	Wystąpienie zagrożenia **jest możliwe**. Zagrożenie miało miejsce w **przeciągu ostatniego tygodnia.**
2	**mało prawdopodobne**	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest **znikoma (bliska zeru)**.
1	**rzadkie**	Zagrożenie występuje **raz w roku.**

Ocena skutków naruszenia praw lub wolności osób fizycznych			**Skutki wystąpienia naruszenia** praw lub wolności osób fizycznych		
Wartość	**Nazwa**	**Opis**	**Skutek prawny**	**Skutek finansowy**	**Skutek wizerunkowy**
3	**wysokie**	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych	*bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych*	*wystąpienie zagrożenia spowoduje straty finansowe w wysokości powyżej 100 tys. zł*	*wystąpienie zagrożenia powoduje istotny lub duży negatywny wpływ na wizerunek jednostki, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w wysokości powyżej 100 tys. zł*
2	**średnie**	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie	*wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa, z wyłączeniem przepisów karnych, lub w przypadku niepodjęcia odpowiednich działań naprawczych naruszenie prawa zostanie nieuniknione*	*wystąpienie zagrożenia spowoduje straty finansowe w maksymalnej wysokości do 100 tys. zł*	*wystąpienie zagrożenia ma mało znaczący negatywny wpływ na wizerunek jednostki lub krótkoterminową utratę wizerunku, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w maksymalnej wysokości do 100 tys. zł;*
1	**niskie**	Identyfikuje się nieznaczne skutki mogące prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych	*wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa*	*wystąpienie zagrożenia nie spowoduje strat finansowych*	*wystąpienie zagrożenia nie ma wpływu na wizerunek ADO lub ten wpływ jest znikomy, nie wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku*
0	**nie dotyczy**	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*

ZAŁĄCZNIK NR 4
do analizy ryzyka

Arkusz identyfikacji ryzyka ze względu na stopień ważności

Lp.	Obszar ryzyka	Poziom ryzyka
1.	DANE OSOBOWE	4
2.	PROGRAMY I SYSTEMY OPERACYJNE, SIEĆ	5
3.	PERSONEL	4

ZAŁĄCZNIK NR 5
do analizy ryzyka

Sprawozdanie dla Administratora Danych Osobowych

z przeprowadzonej analizy ryzyka (nazwa ryzyka)

Nazwa zasobu (aktywa)	
Wartość zasobu	
Właściciel ryzyka	
Opis zagrożeń	
Łączne prawdopodobieństwo wystąpienia zagrożenia	
Opis zabezpieczeń	
Wynik analizy ryzyka (poziom)	
Następstwa wystąpienia ryzyka	

Skarżysko-Kam. dnia ……. …….

(podpis Inspektora Ochrony Danych)