WÓJT GMINY
KIWITY
woj. warmińsko-mazurskie

ZARZĄDZENIE Nr 52/26
WÓJTA GMINY KIWITY
z dnia 15 czerwca 2026 r.

w sprawie wprowadzenia analizy ryzyka

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2026r. poz. 662) oraz 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 (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1. zarządzam co następuje:

§ 1. Wprowadza się analizę ryzyka stanowiącą załącznik niniejszego zarządzenia.

§ 2. Analiza ryzyka jest prowadzona w formie pisemnej.

§ 3. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Jacek [illegible]

RADCA PRAWNY
Bogusława Dworzańska

ANALIZA RYZYKA

URZĄD GMINY KIWITY

Metryka dokumentu:

Tytuł:	Analiza ryzyka dla podstawowych praw i wolności
Komentarz:	Edycja 1
Data utworzenia:	17.06.2026

Spis treści:

1.1 Podstawa prawna

Zgodnie z art. 24 RODO obowiązkiem ADO jest ocena ryzyka naruszenia praw i wolności osób fizycznych celem zastosowania adekwatnych środków technicznych i organizacyjnych. Ocenę dokonuje się biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania danych oraz wagę zagrożenia.

Analizie ryzyka mogą podlegać zarówno zbiory danych osobowych jak i procesy przetwarzania danych osobowych np. zbiór pracowników, zbiór kontrahentów lub proces tworzenia kopii zapasowe bazy danych oraz systemu operacyjnego.

Cele w zakresie bezpieczeństwa przetwarzania zgodnie z art. 32 RODO:

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.

1.2 Definicje

Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych

Identyfikowanie ryzyka – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

Kontekst – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.

Naruszenie (incydent/zdarzenie) ochrony danych osobowych - to 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

Ryzyko – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów (spowoduje szkody lub zniszczenie).

Ryzyko naruszenia praw i wolności – prawdopodobieństwo zaistnienia określonego zdarzenia będącego naruszeniem oraz powagi tego zdarzenia tj. wielkości szkody jaki to zdarzenie może spowodować w odniesieniu do osoby, której dane dotyczą.

RODO - Rozporządzeniem 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.

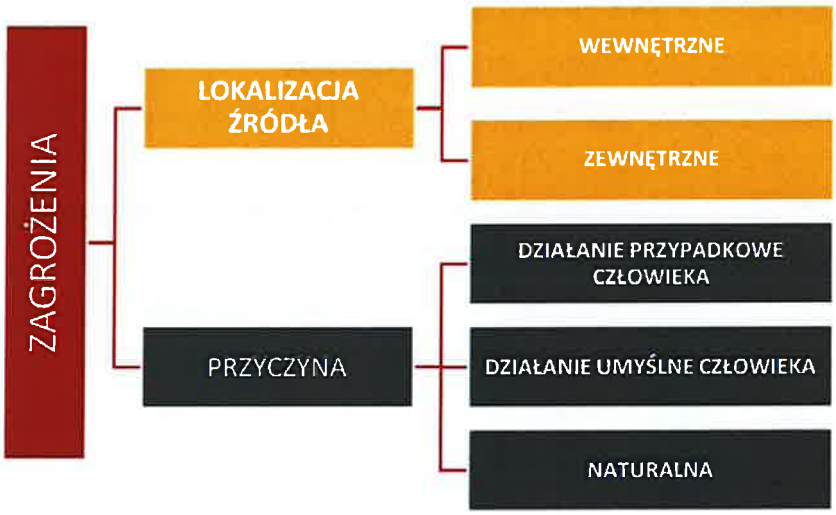
Podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

Zagrożenie - potencjalne naruszenie (potencjalny incydent)

Skutki - rezultaty niepożądanego incydentu/zdarzenia (straty w wypadku wystąpienia zagrożenia)

1.3 Zagrożenia

Zidentyfikowane zagrożenia, które mogą wystąpić podczas przetwarzania danych w zbiorze/procesie zostały uwzględnione w Tabeli Oceny ryzyka.



Rysunek: Podział zagrożeń _źródło GIODO

1.4 Podatności

Rysunek: Przykładowe podatności wg normy PN-ISO/IEC 27005_źródło GIODO

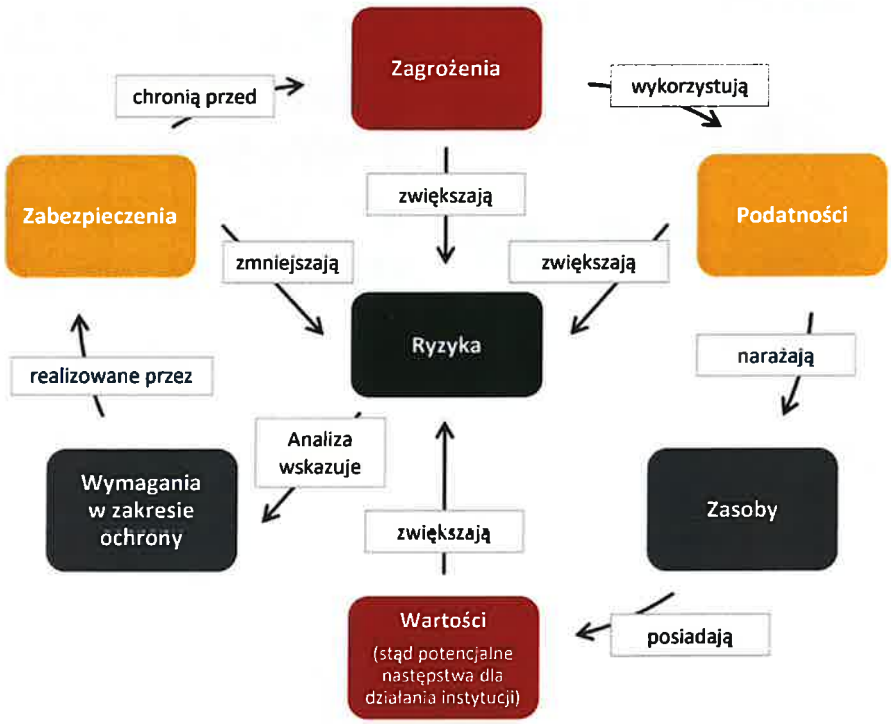
1.5 Zarządzanie ryzykiem

Rysunek: Etapy stosowania podejścia opartego na ryzyku _źródło GIODO

Etapy zarządzania ryzykiem:

- I etap - ustalenie kontekstu (informacji i uwarunkowań związanych z działaniem przedsiębiorstwa)
- II etap - zdefiniowanie i określenie każdego ryzyka zagrażającego podmiotowi przetwarzającemu dane osobowe wraz z ich źródłami, przyczynami i wstępnym zidentyfikowaniem szkód im towarzyszących,
- III etap – szacowanie prawdopodobieństwa wystąpienia zdefiniowanych rodzajów ryzyka, a także określenie wartości prawdopodobnych strat,
- IV etap – postępowanie z ryzykiem.

1.6 Czynniki wpływające na ryzyko



Rysunek: Czynniki wpływające na ryzyko i związki między nimi wg PN-I-13335:1999 _źródło GIODO

1.7 Pomiar ryzyka

Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia.
Ryzyka dla wszystkich zagrożeń i ich skutków zostały wyliczane wg formuły:

Ryzyko = Prawdopodobieństwo x Skutek

Tabela 1: Przyjęta skala prawdopodobieństwa wystąpienia zagrożenia

Skala (Waga)	PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA
0	Zagrożenie nieprawdopodobne
1	Zagrożenie prawie nieprawdopodobne; zagrożenie nigdy nie wystąpiło
2	Zagrożenie jest mało realne; zagrożenie nie wystąpiło w okresie ostatnich 24 miesięcy
3	Zagrożenie jest realne lub bardzo realne; zagrożenie wystąpiło w okresie ostatnich 24 miesięcy

Tabela 2: Przyjęta skala skutków wystąpienia zagrożenia

Skala (Waga)	SKUTKI WYSTĄPIENIA ZAGROŻENIA
0	Brak skutków - zagrożenie nie powoduje skutku
1	Małe - nie prowadzi do naruszenia przepisu prawa, - wystąpienie zagrożenia powoduje znikome skutki finansowe o wartości do 5 000 zł, - wystąpienie zagrożenia nie wpływu lub ma znikomy wpływ na wizerunek jednostki.
2	Średnie - wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa z wyłączeniem przepisów karnych, w przypadku podjęcia odpowiednich działań naprawczych naruszenie prawa zostanie uniknione, - wystąpienie zagrożenia spowoduje straty finansowe o wartości od 5 000 zł

	do 50 000 zł, - wystąpienie zagrożenia ma mało znaczący wpływ na wizerunek jednostki lub wpływa na krótkoterminową utratę wizerunku
3	Duże - bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych, - wystąpienie zagrożenia spowoduje straty finansowe o wartości powyżej 50 000 zł, - wystąpienie zagrożenia powoduje istotny lub duży wpływ na wizerunek jednostki

Tabela 3: Przyjęta skala ryzyka

Skala (Waga)	POZIOM RYZYKA
1-3	Ryzyko pomijalne i akceptowalne (możliwa akceptacja)
4-6	Ryzyko jest opcjonalne (możliwa akceptacja lub obniżenie)
9	Ryzyko jest nieakceptowalne (wymagane obniżenie)

1.8 Postepowanie z ryzykiem

Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń

Przeniesienie ryzyka –przerzucenie ryzyka (outsourcing, ubezpieczenie)

Unikanie ryzyka – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)

Redukcja ryzyka – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę)

Wszędzie, gdzie ADO decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.

1.9 Informowanie o ryzyku

W proces informowania o ryzyku oraz konsultacji powinny być zaangażowane wszystkie strony zainteresowane: na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych, tj.:

a. ADO
b. Inspektor Ochrony Danych
c. właściciele zasobów wykorzystywanych do realizacji operacji przetwarzania danych osobowych;
d. właściciele procesów odpowiedzialnych za weryfikację:

- zgodności w wymaganiami prawnymi oraz regulacjami wewnętrznymi,
- skuteczności wdrożenia i efektywności utrzymania ochrony danych osobowych w organizacji.

1.10 Konsultacje z organem nadzorczym

Jeżeli po zastosowaniu środków minimalizujących ryzyko związanych z:

a. koniecznością i proporcjonalnością przetwarzania danych lub/i
b. wysokim ryzkiem naruszenia praw i wolności osób fizycznych,

nie ma możliwości obniżenia ryzyka do poziomu akceptowalnego i zapewnienia zgodności z wymaganiami RODO, to przed rozpoczęciem przetwarzania ADO musi skonsultować się z organem nadzorczym.

1.11 Ponowna analiza ryzyka

Ponowna analiza ryzyka powinna zostać przeprowadzona po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne) oraz w ramach cyklicznych przeglądów.

Analiza ryzyka powinna być wykonywana co najmniej raz na 3 lata.

Tabela 1_Ocena ryzyka_17.06.2026

Lp.	Zagrożenie	Prawdopodobieństwo x skutek = wartość ryzyka	Potencjalny skutek	Działania minimalizujące ryzyko	Reakcja na zaistniałe zagrożenie
1.	Kradzież dokumentów, danych przez pracowników	1*3 =3 **ryzyko akceptowalne**	Nieuprawnione użycie danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Monitoring terenu i obiektu. **Wdrożono:** Dokumenty zawierające dane osobowe przechowywane są pod kluczem, nadawanie upoważnień do przetwarzania DO w zakresie adekwatnym do pełnionych obowiązków służbowych, logowanie do systemu informatycznego z wykorzystaniem indywidualnego loginu i hasła, szkolenia wewnętrzne pracowników, zasadę „czystego biurka".	Poinformowanie ADO, IOD Poinformowanie organu nadzorczego (UODO) w ciągu 72h
2.	Kradzież dokumentów przez osoby z zewnątrz	1*3 =3 **ryzyko akceptowalne**	Nieuprawnione użycie danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Monitoring terenu i obiektu. **Wdrożono:** Szkolenia wewnętrzne pracowników, zasadę „czystego biurka", zabezpieczenie dokumentów zawierających DO w szafach zamykanych na klucz.	Poinformowanie ADO, IOD Poinformowanie organu nadzorczego (UODO) w ciągu 72h
3.	Atak hakerski	1*3 =3 **ryzyko akceptowalne**	Wyciek danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Zabezpieczenie komputerów programem antywirusowym stosowanie firewalla (fortigate).	Poinformowanie ADO, IOD Serwis komputera, przegląd/analiza zabezpieczeń.

				Wdrożono: a. Procedury korzystania z internetu b. Procedury korzystania z poczty służbowej, c. Szkolenia wewnętrzne z zakresu RODO i bezpieczeństwa informacji dla pracowników.	Poinformowanie organu nadzorczego (UODO) w ciągu 72h
4.	Błąd dostawcy usług zewnętrznych	1*2 =**2** **ryzyko akceptowalne**	Wyciek lub utrata danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Współpraca na podstawie umowy powierzenia danych	Poinformowanie ADO, IOD Egzekwowanie konsekwencji wynikającyc z umowy o powierzenia danych Poinformowanie organu nadzorczego (UODO) w ciągu 72h
5.	Awaria u dostawcy usług zewnętrznych (poczta, hosting itd.)	1*2 =**2** **ryzyko akceptowalne**	Brak dostępu do danych	**Postępowanie: REDUKCJA RYZYKA** Współpraca z wypróbowanymi i rekomendowanymi dostawcami deklarującymi przestrzeganie RODO	Poinformowanie ADO, IOD Analiza konieczności zmiana dostawcy usług
6.	Systemy operacyjne nie mające wsparcia producenta.	1*2 =**2** **ryzyko akceptowalne**	Utrata lub wyciek danych osobowych korzystanie z systemów operacyjnych (...) bez dołożenia należytej staranności w celu zapewnienia im aktualizacji do najnowszej wersji w sposób istotny obniża poziom bezpieczeństwa realizowanych w ten sposób procesów przetwarzania	**Postępowanie: REDUKCJA RYZYKA** Na wszystkich stanowiskach komputerowych są zainstalowane systemy operacyjne mające wsparcie producenta.	Poinformowanie ADO, IOD Zapewnienie aktualizacji systemu operacyjnego do najnowszej wersji.
7.	Kradzież telefonu komórkowego	1*1 =**1** **ryzyko akceptowalne**	Utrata lub/i wyciek danych osobowych	**Postępowanie: brak**	Poinformowanie ADO, IOD Poinformowanie policji i organu

					nadzorczego (UODO) w ciągu 72h
8.	Awaria oprogramowania	1*2 =**2** **ryzyko akceptowalne**	Brak dostępu do danych	**Postępowanie: REDUKCJA RYZYKA** **Wdrożono:** Bieżąca kontrola i serwis systemów informatycznych Regularna aktualizacja oprogramowania.	Poinformowanie ADO, IOD Przegląd/analiza zabezpieczeń, analiza przyczyn, wdrożenie ew. zmian.
9.	Kradzież laptopa	1*1 =**1** **ryzyko akceptowalne**	Utrata danych osobowych	**Postępowanie: REDUKCJA RYZYKA** **Wdrożono:** a. dostęp do laptopa po zalogowaniu, b. szyfrowanie danych na dyskach zawierających DO (przy wynoszeniu urządzenia poza obszar podmiotu), c. regularny backup danych, d. procedura korzystania z komputerów przenośnych, e. szkolenia wewnętrzne pracowników.	Poinformowanie ADO, IOD Poinformowanie policji. Poinformowanie organu nadzorczego (UODO) w ciągu 72h jeśli zachodzi ryzyko naruszenia praw i wolności.
10.	Zagubienie laptopa	1*1 =**1** **ryzyko akceptowalne**	Utrata danych osobowych	**Postępowanie: REDUKCJA RYZYKA** **Wdrożono:** a. dostęp do laptopa po zalogowaniu, b. szyfrowanie danych na dyskach zawierających DO (przy wynoszeniu urządzenia poza obszar jednostki), c. regularny backup danych, d. procedurę korzystania z komputerów przenośnych, e. szkolenia wewnętrzne pracowników.	Poinformowanie ADO, IOD Poinformowanie policji. Poinformowanie organu nadzorczego (UODO) w ciągu 72h jeśli zachodzi ryzyko naruszenia praw i wolności.
11.	Infekcja złośliwym oprogramowaniem	1*2 =**2** **ryzyko akceptowalne**	Utrata lub/i wyciek danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Stosowanie programu antywirusowego oraz firewalla (fortigate) **Wdrożono:** a. regularny backup danych, b. cykliczne wykonywanie backupu danych na nośniku	Poinformowanie ADO, IOD Poinformowanie organu nadzorczego (UODO) w ciągu 72h

				zewnętrznym, c. procedura korzystania z komputerów przenośnych, d. procedury korzystania z internetu, e. procedury korzystania z poczty służbowej, f. szkolenia wewnętrzne pracowników.	
12.	Atak socjotechniczny (phishing, telefon)	1*2 =**2** **ryzyko akceptowalne**	Nieuprawnione użycie danych osobowych	**Postępowanie: REDUKCJA RYZYKA** **Planowane (sugerowane działania):** a. szkolenia wewnętrzne pracowników, b. nieudostępnianie żadnych danych osobowych przez telefon bez weryfikacji tożsamości rozmówcy.	Poinformowanie ADO, IOD Poinformowanie organu nadzorczego (UODO) w ciągu 72h
13.	Awaria serwera	1*2 =**2** **ryzyko akceptowalne**	Brak dostępu do danych	**Postępowanie: REDUKCJA RYZYKA** Regularny backup danych.	Poinformowanie ADO, IOD Wymiana/naprawa/wypożyczenie serwera Odtworzenie danych z backupu danych.
14.	Zalanie	1*1=**1** **ryzyko akceptowalne**	Utrata danych osobowych	**Postępowanie: REDUKCJA RYZYKA** Regularny przegląd techniczny budynku	Poinformowanie ADO, IOD Odtworzenie zbioru danych i przechowywanie ich w bezpiecznym miejscu
16.	Pożar	1*3 =**3** **ryzyko akceptowalne**	Utrata danych osobowych	**Postępowanie: REDUKCJA RYZYKA** System PPOŻ w obiektach. Regularny przegląd techniczny budynku Instrukcja przeciwpożarowa.	Poinformowanie ADO, IOD Odtworzenie zbioru danych i przechowywanie ich w bezpiecznym miejscu
17.	Brak prądu	1*2 =**2** **ryzyko akceptowalne**	Brak dostępu do danych	**Postępowanie: REDUKCJA RYZYKA** W serwerowni oraz na wszystkich stanowiskach komputerowych są zainstalowane UPS	Poinformowanie ADO, IOD