Zarządzenie Nr 197/2023
Wójta Gminy Brody
z dnia 13 listopada 2023 r.

w sprawie wprowadzenia Procedury analizy ryzyka i oceny skutków dla przetwarzania danych osobowych

Na podstawie art. 33 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t. j. Dz. U. z 2023 r., poz. 40 z późn. m.) oraz 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) (Dz. U. UE. L. z 2016 r. Nr 119.1), zarządzam co następuje:

§ 1

Wprowadza się Procedurę analizy ryzyka i oceny skutków dla przetwarzania danych w Urzędzie Gminy Brody stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2

Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 3

Traci moc zarządzenie nr 162/2019 Wójta Gminy Brody z dnia 31.10.2019 r.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia nr 197/2023
Wójta Gminy Brody
z dnia 13 listopada 2023 r.

Analiza ryzyka i ocena skutków dla przetwarzania danych

w Urzędzie Gminy Brody

§ 1

Wstęp

1. Administrator przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa danych osobowych w celu zidentyfikowania obszarów, które mogą istotnie wpływać na osobę, której przetwarzanie dotyczy.
2. Na szacowanie ryzyka składa się:
   1) analiza ryzyka ogólnego,
   2) ocena skutków dla przetwarzania danych (DPIA).

§ 2

Definicje

1. **Administrator danych** – Wójt Gminy Brody;
2. **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych;
3. **Analiza ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;
4. **ASI** – Administrator Systemów Informatycznych w Urzędzie;
5. **Bezpieczeństwo informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych takich atrybutów jak poufność, integralność oraz dostępność;
6. **Dostępność** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania wtedy, kiedy jest to potrzebne;
7. **Integralność** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci danych osobowych pozostają kompletne, dane nie zostały w sposób nieuprawniony zmienione, zniszczone w sposób nieautoryzowany;
8. **IOD** – Inspektor Ochrony Danych w Urzędzie;
9. **Kierownik komórki organizacyjnej** – osoby na samodzielnych stanowiskach oraz osoby kierujące komórkami organizacyjnymi w Urzędzie Gminy w Brodach zgodnie z Regulaminem organizacyjnym dla Urzędu Gminy w Brodach;
10. **Incydent** – zdarzenie prowadzące lub mogące doprowadzić do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w

inny sposób przetwarzanych. Naruszenie może powodować w stosunku do osoby fizycznej szkodę o charakterze majątkowym lub niemajątkowym;

11. **Ocena ryzyka** – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
12. **Podatność** – słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie;
13. **Postępowanie z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;
14. **Poufność** – właściwość polegająca na tym, że dane osobowe nie są udostępniane lub wyjawiane nieupoważnionym osobom, podmiotom lub procesom;
15. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
16. **RODO –** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
17. **Rozliczalność** - oznacza, że działania podmiotu np. użytkownika mogą być mu przypisane**,** właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
18. **Ryzyko** – rozumie się przez to kombinację prawdopodobieństwa zagrożenia i jego konsekwencji; prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów;
19. **Ryzyko szczątkowe** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
20. **Skutki** – rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia);
21. **Szacowanie ryzyka** – rozumie się przez to proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyka związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy;
22. **Szczególne kategorie danych osobowych** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia; dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej) oraz dane dotyczące seksualności lub orientacji seksualnej osoby fizycznej;
23. **Urząd** – Urząd Gminy Brody;
24. **Ustawa o ochronie danych osobowych –** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781);
25. **Zagrożenie** – potencjalna przyczyna niepożądanego naruszenie (potencjalny incydent);
26. **Zbiór danych osobowych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

§ 3

Klasyfikacja czynności przetwarzania

1. W pierwszej kolejności należy podzielić czynności przetwarzania (określone w rejestrze czynności przetwarzania) na te, które wymagają oceny skutków dla przetwarzania danych (DPIA) oraz te, względem których należy wykonać analizę ryzyka ogólnego. Ocenę skutków dla ochrony danych (DPIA) należy przeprowadzić w sytuacji jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Kryteria pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko określone są w Komunikacie Prezesa Urzędu Ochrony danych osobowych ogłoszonym na podstawie art. 54 ust. 1 ustawy o ochronie danych osobowych w związku z art. 35 ust. 4 RODO. Klasyfikacja czynności przetwarzania stanowi załącznik nr 1 do niniejszej Procedury.

2. Przetwarzanie spełniające przynajmniej dwa z wymienionych w Komunikacie kryteriów będzie wymagać oceny skutków dla ochrony danych. Administrator może równocześnie stwierdzić, iż przetwarzanie wyczerpuje więcej niż dwa kryteria, ale mimo to nie przeprowadza oceny skutków dla ochrony danych.

§ 4

Szacowanie ryzyka

1. Proces szacowania ryzyka dokonuje się w odniesieniu do zbiorów danych osobowych określonych w rejestrze czynności przetwarzania lub rejestrze kategorii czynności przetwarzania danych osobowych. Ryzyko rozpatrywane jest w kontekście utraty atrybutów poufności, integralności i dostępności danych osobowych.

2. Określa się Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorach lub w procesie przetwarzania. Prawdopodobieństwo wystąpienia zagrożenia zidentyfikowano zgodnie z poniższą skalą:

PRAWDOPODOBIEŃSTWO	SKALA	CZĘSTOTLIWOŚĆ WYSTĄPIENIA ZDARZENIA
Zdarzenie niemal pewne	4	Może wystąpić częściej niż raz w miesiącu
Zdarzenie wysoce prawdopodobne	3	Może wystąpić wielokrotnie w ciągu roku (raz w miesiącu lub rzadziej)
Zdarzenie mało prawdopodobne	2	Może wystąpić kilka razy w roku
Zdarzenie nieprawdopodobne	1	Może wystąpić raz lub nie zdarzy się w ciągu roku

3. Określa się Skutki (S) wystąpienia zdarzenia uwzględniając m.in. straty finansowe, wizerunkowe, osobiste osoby fizycznej, sankcje/skutki karne. Skutek wystąpienia zagrożenia ustalono zgodnie z poniższą skalą:

SKUTEK	SKALA	OPIS NASTĘPSTW
Bardzo wysoki	4	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych dla osób fizycznych. Zagrożenie ustawową karą pozbawienia wolności. Bardzo wysokie koszty wielu procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole organów ścigania. Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowych zadań albo osiąganie założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa albo wizerunkowa (brak zaufania ze strony osób, które Urząd obsługuje w ramach wykonywanych zadań publicznych). Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.
Wysoki	3	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych. Zdarzenie powoduje np. wysokie ustawowe kary pieniężne dla jednostki. Koszt kilku procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole i kary UODO. Zdarzenie objęte ryzykiem powoduje znaczącą stratę posiadanych zasobów, ma negatywny wpływ na wykonywanie zadań. Wpływa negatywnie na reputację jednostki (brak zaufania ze strony osób, które Urząd obsługuje w ramach wykonywanych zadań publicznych). Skutki zdarzenia wiążą się z trudnym procesem przywracania stanu poprzedniego.
Średni	2	Zdarzenie wywołuje średni skutek. Może spowodować nałożenie kar ustawowych w dolnej granicy kary. Koszt nielicznych procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, niewielkie zakłócenie lub opóźnienie w wykonywaniu zadań. Niski wpływ na reputacje jednostki. Skutki zdarzenia można łatwo usunąć.
Niski	1	Zdarzenie wywołuje niski skutek. Nie skutkuje poważnym wpływem na prawa i wolności osób fizycznych np. nie grozi dyskryminacją, kradzieżą tożsamości, oszustwem spowodowanym kradzieżą tożsamości. Zdarzenie objęte ryzykiem powoduje minimalną stratę finansową lub krótkotrwałe zakłócenia lub opóźnienie w wykonywaniu zadań. Niski wpływ na reputację. Skutki zdarzenia można łatwo usunąć
zdarzenie nie powoduje skutku (nie występuje)	0	Nie ma straty finansowej. Po stronie osoby fizycznej, której przetwarzanie dotyczy nie występuje ani szkoda o charakterze majątkowym, ani osobistym. Zaufanie osób, które Urząd obsługuje w ramach wykonywanych zadań publicznych nie doznaje żadnego uszczerbku.

§ 5

Analiza ryzyka

1. Wzór analizy ryzyka w zakresie wykonywania:
   1) analizy ryzyka ogólnego,
   2) oceny skutków dla przetwarzania danych (DPIA).

WZÓR ANALIZY RYZYKA:

$$R = P^{x} S$$

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczanego ryzyka	
P	wartość przypisana prawdopodobieństwu materializacji zagrożenia	1 - zdarzenie nieprawdopodobne, 2 - zdarzenie mało prawdopodobne, 3 - zdarzenie wysoce prawdopodobne, 4 - zdarzenie niemal pewne.
S	Skutki zdarzenia	0 – zdarzenie nie powoduje skutku (nie występuje), 1 – zdarzenie wywołuje niski skutek, 2 – zdarzenie wywołuje średni skutek, 3 – zdarzenie wywołuje wysoki skutek, 4 - zdarzenie wywołuje bardzo wysoki skutek.

2. Wyliczone ryzyka należy porównać ze skalą. Zakres macierzy przedstawia poniższa tabela:

			SKUTEK				
			0	**1**	**2**	**3**	**4**
PRAWDOPODOBIEŃSTWO	Zdarzenie nieprawdopodobne	**1**	**0**	**1**	**2**	**3**	**4**
	Zdarzenie mało prawdopodobne	**2**	**0**	**2**	**4**	**6**	**8**
	Zdarzenie wysoce prawdopodobne	**3**	**0**	**3**	**6**	**9**	**12**
	Zdarzenie niemal pewne	**4**	**0**	**4**	**8**	**12**	**16**

3. W związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do analizy ryzyka ogólnego, przyjęto klasyfikację działań:

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: - obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; - pozostawienie ryzyka i niepodejmowanie dalszych działań; - unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; - przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Poziom ryzyka nieakceptowany – wymaga bezwzględnej reakcji – cel: zredukowanie podatności

4. W związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do oceny skutków dla przetwarzania danych (DPIA), przyjęto klasyfikację działań:

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: -obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; -pozostawienie ryzyka i niepodejmowanie dalszych działań; -unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; -przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Wymaga bezwzględnej reakcji – cel: zredukowanie podatności Konsultacja z organem nadzorczym konieczna w momencie, kiedy Administrator nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego mimo, że przewidział wprowadzenie środków bezpieczeństwa.

5. Wyniki analizy szacowania ryzyka zawarte są w arkuszach ryzyka (analizy ryzyka ogólnego i oceny skutków dla przetwarzania danych DPIA), w których pracownicy Urzędu dokonują oceny prawdopodobieństwa wystąpienia zagrożenia oraz skutków, jakie zagrożenie może wywołać (wzór stanowi załącznik nr 2 do Procedury).

§ 6
Ocena ryzyka dla przetwarzania danych osobowych

1. Decyzje Administratora jakie może podjąć wobec zidentyfikowanego ryzyka:
   1) akceptacja ryzyka (zachowanie ryzyka) – nie wprowadza się żadnych zmian w zakresie zidentyfikowanego ryzyka (najczęściej do przyjęcia na poziomie niskim),
   2) redukcja ryzyka (modyfikowanie ryzyka) – polega na obniżeniu poziomu ryzyka poprzez na przykład zastosowanie dodatkowych zabezpieczeń,
   3) unikanie ryzyka – polega na unikaniu działań determinujących powstanie określonych typów ryzyka,
   4) przeniesienie (transfer) ryzyka – polega na przeniesieniu ryzyka najczęściej poprzez scedowanie skutków ryzyka na podmiot zewnętrzny.
2. Ryzyko przekraczające akceptowalny poziom ryzyka wymaga określenia rodzaju reakcji na ryzyko – przeciwdziałania ryzyku. Ryzykiem akceptowalnym jest ryzyko niskie.
3. Wzór arkusza oceny ryzyka dla analizy ryzyka ogólnego oraz oceny skutków dla przetwarzania danych (DPIA) stanowi załącznik nr 3 do niniejszej Procedury.

4. W przypadku gdy Administrator decyduje się obniżyć (zredukować) ryzyko, przy współpracy IOD, Kierownika komórki organizacyjnej i ASI ustala działania naprawcze, termin realizacji i osoby odpowiedzialne za ich realizację. Monitorowanie wdrożenia działań naprawczych polega na dokonaniu ponownego obliczenia wyniku szacowania dla tego zagrożenia.

§ 7

Jeżeli mimo zastosowania odpowiednich środków technicznych lub organizacyjnych, analiza następstw utraty poufności, integralności lub dostępności w kontekście czynności przetwarzania sklasyfikowanych do oceny skutków dla przetwarzania danych (DPIA) w dalszym ciągu powoduje wysokie ryzyko szczątkowe, Administrator konsultuje się z organem nadzorczym, o którym mowa w art. 36 RODO.

Załącznik nr 1
do Procedury analizy ryzyka i oceny skutków
dla przetwarzania danych w Urzędzie Gminy Brody

Klasyfikacja czynności przetwarzania

			KRYTERIA WYSTĄPIENIA OCENY SKUTKÓW									
Lp.	**Nr czynności**	**NAZWA CZYNNOŚCI PRZETWARZANIA (zgodna z rejestrem czynności przetwarzania)**	**Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych**	**Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki**	**Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajda si 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**	**Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29)**	**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**	**Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł**	**Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób. które dysponuj a uprawnieniami władczymi i/lub oceniającymi**	**Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych**	**Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy**	**CZY OCENA SKUTKÓW JEST WYMAGANA**
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*

Załącznik nr 2

do Procedury analizy ryzyka i oceny skutków dla przetwarzania danych w Urzędzie Gminy Brody

ARKUSZ RYZYKA

Opis zagrożenia	**Prawdopodobieństwo wystąpienia zagrożenia (P) Skala od 1 do 4**	**Skutki (S) Skala od 0 do 4**	**Skala ryzyka (R) (*kol.2xkol. 3*)**	**Poziom ryzyka: Niskie (0-4) Średnie (6-9) Wysokie (12-16)**	**Proponowane działania naprawcze** (wypełnić w przypadku, gdy w kolumnie 4 skala ryzyka jest większa niż 4)	**Uwagi**
1	*2*	*3*	*4*	*5*	*6*	*7*
1. Zagrożenia dla poufności danych osobowych[1]:						
1.1. Udostępnianie danych osobowych osobom nieupoważnionym						
1.2. Zabranie danych osobowych przez osobę nieuprawnioną						
1.3. Pokonanie zabezpieczeń fizycznych lub programowych						
1.4. Niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych						
1.5. Nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.)						
1.6. Niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych						
1.7. Naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych						
1.8. Podsłuch lub podgląd danych osobowych						
1.9. Elektromagnetyczna emisja ujawniająca						
1.10. Utrata lub zagubienie nośnika zawierającego dane osobowe						
1.11. Ujawnienie haseł dostępu do zasobów z danymi osobowymi						
1.12. Klęska żywiołowa, w wyniku której utracono poufność danych						
1.13. Udostępnienie adresów e-mail odbiorcom wiadomości grupowej						
1.14. Nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe						

[1] Poufność - właściwość polegająca na tym, że dane osobowe nie są udostępniane lub wyjawiane nieupoważnionym osobom, podmiotom lub procesom

Opis zagrożenia	**Prawdopodobieństwo wystąpienia zagrożenia (P) Skala od 1 do 4**	**Skutki (S) Skala od 0 do 4**	**Skala ryzyka (R) (*kol.2xkol. 3*)**	**Poziom ryzyka: Niskie (0-4) Średnie (6-9) Wysokie (12-16)**	**Proponowane działania naprawcze** (wypełnić w przypadku, gdy w kolumnie 4 skala ryzyka jest większa niż 4)	**Uwagi**
1	*2*	*3*	*4*	*5*	*6*	*7*
1.15. Niedyskrecja osób uprawnionych do przetwarzania danych osobowych						
1.16. Stosowanie korupcji lub szantażu w celu wydobycia określonych informacji od wybranych pracowników jednostki						
1.17. Ujawnienie danych w wyniku wysłania danych na błędny adres odbiorcy						
1.18.						
1.19.						
2. Zagrożenia dla integralności danych osobowych[2]:						
2.1. Uszkodzenie (celowe bądź przypadkowe) systemu operacyjnego lub urządzeń sieciowych						
2.2. Celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych						
2.3. Działalnie złośliwego oprogramowania (wirusy)						
2.4. Awarie sprzętowe (serwer i inne komputery)						
2.5. Pożar, zalanie, ekstremalna temperatura, inne						
2.6. Zagrożenia zewnętrzne, np. klęski żywiołowe, atak terrorystyczny, włamanie						
2.7. Nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego						
2.8. Błędy, pomyłki						
2.9. Brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika						
2.10. Awarie oprogramowania						
2.11. Brak kopii bezpieczeństwa						
2.12. Brak narzędzi, urządzeń i innych składników wspomagających integralność (np. brak archiwum)						
2.13. Zaniechania organizacyjne personelu						
2.14. Dokonanie zmiany hasła dostępu do konta użytkownika bez jego wiedzy i zgody						

[2] Integralność - właściwość polegająca na tym, że aktywa w postaci danych osobowych pozostają kompletne, dane nie zostały w sposób nieuprawniony zmienione, zniszczone w sposób nieautoryzowany

Opis zagrożenia	**Prawdopodobieństwo wystąpienia zagrożenia (P) Skala od 1 do 4**	**Skutki (S) Skala od 0 do 4**	**Skala ryzyka (R) (*kol.2xkol. 3*)**	**Poziom ryzyka: Niskie (0-4) Średnie (6-9) Wysokie (12-16)**	**Proponowane działania naprawcze** (wypełnić w przypadku, gdy w kolumnie 4 skala ryzyka jest większa niż 4)	**Uwagi**
1	*2*	*3*	*4*	*5*	*6*	*7*
2.15.						
3. Zagrożenia dla dostępności danych[3]:						
3.1. Włamanie do pomieszczenia, w którym znajdują się dokumentny, system, kradzież urządzeń, nośników						
3.2. Nieprzydzielenie użytkownikowi systemu informatycznego identyfikatorów						
3.3. Awaria zasilania						
3.4. Usunięcie plików lub wykonanie czynności mogącej przerwać lub utrudnić funkcjonowanie systemu						
3.5. Katastrofy budowlane, zalanie, zawalenie, pożar						
3.6. Utrata kluczowych pracowników						
3.7. Awaria sprzętu						
3.8. Błąd /awaria oprogramowania						
3.9.						
3.10						

Data, podpis ……..

Tabela nie określa zamkniętego katalogu ryzyka.

[3] Dostępność - to właściwość polegająca na tym, że aktywa w postaci danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania wtedy, kiedy jest to potrzebne;

Załącznik nr 3

do Procedury analizy ryzyka i oceny skutków dla przetwarzania danych w Urzędzie Gminy Brody

Arkusz oceny ryzyka (dla analizy ryzyka ogólnego/oceny skutków dla przetwarzania danych)

Nr ryzyka (R)	Czynności przetwarzania (zbiory danych przetwarzane na danym stanowisku)	Rodzaj zagrożenia	Rodzaj atrybutu (poufność dostępność, integralność)	Poziom ryzyka (R)				Decyzja wobec ryzyka (redukcja, akceptacja, unikanie, przeniesienie)
				Prawdopodobieństwo	Skutek	Wartość ryzyka	Ryzyko po wstępnym procesie szacowania ryzyka	
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*

Sporządził: ……,

Zatwierdził: ……..