ZAŁĄCZNIK NR 1 - WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... pomiędzy:

....., z siedzibą w ..... (kod: .....)

przy ulicy ....., NIP ....., REGON

....., zwanym dalej Administratorem danych osobowych lub Administratorem, reprezentowanym przez :

1) .....

a

....., z siedzibą w ..... (kod: .....)

przy ulicy ....., NIP ....., REGON

....., zwanym dalej Przetwarzającym, reprezentowanym przez:

1) .....

§ 1

Postanowienia ogólne

1. Na mocy niniejszej umowy Administrator danych osobowych zawartych w zbiorze ..... *(nazwa zbioru)* powierza, w zakresie określonym w § 2 niniejszej umowy, przetwarzanie danych osobowych zawartych w tym zbiorze Przetwarzającemu.
2. Zbiór prowadzony jest w formie .....
3. Właścicielem zbioru jest osoba pełniąca funkcję ..... *(np. kierownika Sekcji IT).*
4. Administratorem systemu informatycznego, w którym utworzony został zbiór jest ..... , tel. ..... *(jeżeli dotyczy).*
5. Przetwarzający zapewnia, że:
   a) posiada fachową wiedzę i zasoby koniecznego do należytej realizacji niniejszej umowy, w szczególności wdrożył środki techniczne i organizacyjne, w tym te dotyczące wymogów bezpieczeństwa przetwarzania, odpowiadające wymogom określonym w rozporządzeniu 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 (zwane dalej również ogólnym rozporządzeniem o ochronie danych lub RODO);
   b) będzie zabezpieczał interes prawny osób, których dane przetwarza;

c) będzie w pełni przestrzegał wymogów określonych w zatwierdzonym Kodeksie postępowania, o którym mowa w art. 40 RODO lub zatwierdzonych mechanizmach certyfikacji, o których mowa w art. 42 RODO,

d) będzie realizował wytyczne Administratora w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych,

e) dane osobowe będą przetwarzane na terenie Unii Europejskiej i nie będą przekazane do państwa trzeciego lub organizacji międzynarodowej spoza Unii Europejskiej.

6. Przetwarzający nie jest uprawiony do dalszego przekazywania danych osobowych innemu podmiotowi, bez szczegółowej pisemnej zgody Administratora. W zgodzie tej zostaną określone wymogi dotyczące podmiotu, któremu Przetwarzający może powierzyć dane i sposobu postępowania z danymi, w tym ich zabezpieczeń.

§ 2

Określenie zakresu i okresu powierzenia przetwarzania

1. Administrator powierza dane osobowe wchodzące do zbioru wymienionego w § 1 ust. 1 niniejszej umowy. Zakres powierzonych danych obejmuje:
   1) .....
   2) .....

   Administrator oświadcza, że są to dane osobowe ..... *(np. pracowników, studentów).*
2. Przetwarzający uprawiony jest do przetwarzania danych od dnia zawarcia niniejszej umowy do dnia ..... r. / Przetwarzający uprawiony jest do przetwarzania danych przez czas nieokreślony od dnia zawarcia.
3. Przetwarzający zobowiązany jest do natychmiastowego zaprzestania przetwarzania danych w przypadku:
   1) upływu okresu na jaki umowa została zawarta / wypowiedzenia niniejszej umowy;
   2) ustania celu, dla którego niniejsza umowa została zawarta.
4. Po zakończeniu przetwarzania w imieniu Administratora danych, Przetwarzający powinien – zgodnie z decyzją Administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega Przetwarzający, nakładają obowiązek przechowywania danych osobowych. Informacja w tym zakresie zostanie przekazywana Przetwarzającemu, w formie pisemnej, przez Administratora, na co najmniej 3 dni robocze przed zakończeniem obowiązywania niniejszej umowy.
5. W przypadku usunięcia danych - Przetwarzający zobowiązany jest poinformować pisemnie Administratora o wykonaniu tej operacji oraz o sposobie jej wykonania - w terminie 3 dni roboczych od dnia wykonania operacji.

§ 3

Określenie celu

Powierzenie przetwarzania danych osobowych następuje w celu

.....

.....

§ 4

Obowiązki Przetwarzającego

1. Przetwarzający zobowiązuje się, że:
   1) podejmie wszelkie środki wymagane na mocy art. 32 RODO;
   2) w miarę możliwości będzie pomagał Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO;
   3) będzie pomagał Administratorowi wywiązać się z obowiązków określonych w art. 32 – 36 RODO;
   4) udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach prawa powszechnie obowiązującego oraz umożliwienia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji;
   5) niezwłocznego informowania Administratora o stwierdzonych Incydentach dotyczących danych zgromadzonych w zbiorze i współpracy z przedstawicielami Administratora przy usuwaniu jego skutków oraz badaniu przyczyn jego wystąpienia.
2. Przetwarzający oświadcza, że jeżeli naruszy przy przetwarzaniu powierzonych mu danych postanowienia RODO, będzie on traktowany jako Administratora w odniesieniu do tego przetwarzania.
3. Przetwarzający oświadcza, że osoby uprawnione do składania oświadczeń woli w jego imieniu oraz jego pracownicy i współpracownicy dopuszczeni do przetwarzania danych złożyli oświadczenia zgodnie ze wzorem zawartym w załączniku nr 1 do umowy. Oświadczenia te zostały przekazane Administratorowi w dniu zawarcia niniejszej umowy. W przypadku konieczności zmiany osób, które będą miały dostęp do przetwarzanych danych, Administrator zostanie poinformowany przez Przetwarzającego pisemnie o niniejszym przed dopuszczeniem nowych osób do przetwarzania danych. Wraz z ww. informacją Administratorowi zostanie przekazane oświadczenie wskazane załączniku nr 1.

§ 5

Kary umowne

1. W przypadku nałożenia na Administratora kary administracyjnej za niezgodne z przepisami prawa powszechnie obowiązującego przetwarzanie danych osobowych zgromadzonych w przekazanym zbiorze lub niezgodne z prawem zabezpieczenie tego zbioru, Przetwarzający:
   a) zwróci Administratorowi, w terminie 7 dni od otrzymania informacji w tym zakresie od Administratora, kwotę wynikającą z nałożonej na niego kary,
   b) zapłaci Administratorowi karę umowną w wysokości .....
2. W przypadku ujawnienia danych osobowych przetwarzanych w przekazanym zbiorze - Przetwarzający zapłaci Administratorowi karę umowną w wysokości .....
3. W przypadku naruszenia postanowień niniejszej umowy, w szczególności w zakresie § 1 ust. 5 lit. c, § 1 ust. 6, § 2 ust. 5, § 4 ust. 3 - Przetwarzający zapłaci Administratorowi karę umowną w wysokości .....
4. W przypadku stwierdzenia podczas działań wskazanych w § 4 ust. 1 pkt 4 niniejszej umowy, że Przetwarzający narusza postanowienia RODO wytycznych wskazanych w § 1 ust. 5 lit c - Przetwarzający zapłaci Administratorowi karę umowną w wysokości .....

§ 6

Postanowienia końcowe

1. Strony umowy postanawiają, że będą się kontaktowały za pośrednictwem następujących osób:
   a) ze strony Administratora: .....
   b) ze strony Przetwarzającego: .....
2. Zmiana postanowień niniejszej umowy wymaga zachowania formy pisemnej – pod rygorem nieważności, z zastrzeżeniem zmiany postanowień § 1 ust. 1 i § 6 ust. 1. Strony zobowiązują się informować pisemni o zmianie ww. osób – w terminie 3 dni roboczych od wprowadzenia zmian.
3. Umowa została zawarta w czterech egzemplarzach, po dwa dla każdej ze Stron.

.....
(data i podpis Administratora)

.....
(data i podpis Przetwarzającego)

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji

Wzór wykazu budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe

LP	BUDYNEK	NAZWA	NR/SYMBOL
1.	SZKOŁA	V Liceum Ogólnokształcące im. Marii Skłodowskiej-Curie w Lublinie, ul. Lipowa 7, 20-020 Lublin	-
2.	POMIESZCZENIA	Sale lekcyjne	002, 104, 105, 106,108, 109,111, 112, 201, 202, 204, 205, 210, 211, 213, 214, 215, 216, 301, 304, 305, 306, 309, 310, 313, 314, 315
3.		Biblioteka	009
4.		Archiwum	-
5.		Pokój Nauczycielski	206
6.		Gabinet Dyrektora	102
7.		Gabinet wicedyrektorów	209, 115
8.		Gabinet planu	114
9.		Sekretariat	101
10.		Gabinet kadr i kierownika gospodarczego	113
11.		Pokój socjalny pracowników obsługi	007
12.		Gabinet pedagoga	207
13.		Serwerownia	006
14.		Pokój socjalny wychowania fizycznego	008
15.		Zaplecze biologii	-
16.		Zaplecze chemii	316
17.		Zaplecze fizyki	302

Załącznik nr 3

do Polityki Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin

Procedura sprawdzeń

Spis treści

1 Cel

Procedura określa podstawowe zasady wykonywania audytów wewnętrznych, których celem jest ocena funkcjonowania systemu ochrony danych osobowych pod kątem jego zgodności z wymaganiami prawa powszechnie obowiązującego, aktami prawa wewnętrznego, , odpowiednimi politykami bezpieczeństwa, kodeksami zgodnie z art. 40 RODO oraz normami.

2 Zakres

Przedmiotem procedury jest metodyka planowania, organizacji i przeprowadzania sprawdzeń systemu ochrony danych osobowych.

Zakres procedury obejmuje sprawdzanie zgodności przetwarzania danych osobowych z przepisami prawa powszechnie obowiązującego i aktami prawa wewnętrznego w zakresie ochrony danych osobowych, kodeksami, o których mowa w art. 40 RODO oraz opracowanie sprawozdania w tym zakresie.

Planowanie sprawdzenia

3.1 Za przeprowadzanie sprawdzenia jest odpowiedzialny Inspektor Ochrony Danych. Zadania dotyczące systemu informatycznego w trakcie sprawdzeń realizuje ASI pod nadzorem Inspektor Ochrony Danych.

3.2 ASI odpowiada za część techniczną weryfikacji dotyczącą systemu informatycznego.

3.3 Inspektor Ochrony Danych odpowiada za potwierdzenie zgodności i ocenę skuteczności działania systemu.

3.4 W Jednostce Organizacyjnej przyjęto następujące zasady dotyczące przeprowadzania sprawdzeń:

a. przynajmniej raz w roku przeprowadzić sprawdzenie zgodności systemu ochrony danych osobowych z uwzględnieniem zabezpieczeń technicznych, fizycznych i organizacyjnych,

b. w zależności od potrzeb realizować sprawdzenia incydentalne, obligatoryjnie przeprowadzane po incydencie w obszarze objętym naruszeniem ochrony danych osobowych.

3.5 Sprawdzenia incydentalne mogą wynikać z powodów:

a. pogorszenia skuteczności zabezpieczeń,

b. pogorszenia dyscypliny przestrzegania zasad ochrony danych osobowych,

c. wprowadzenia nowych wymagań z uwagi na zmianę wymogów prawnych nakładanych na system bezpieczeństwa jednostki,

d. wprowadzenie nowego programu lub systemu przetwarzającego dane osobowe lub nowego systemu zabezpieczeń,

e. wszelkich zmian mających wpływ na bezpieczeństwo danych osobowych.

3.6 Sprawdzenia planowe realizowane są zgodnie z planem sprawdzeń systemu ochrony danych osobowych

opracowywanym przez Inspektora Ochrony Danych na okres nie krótszy niż kwartał i nie dłuższy niż rok i zatwierdzonym przez Administratora.

3.7 Inspektor Ochrony Danych przygotowuje do 15 grudnia każdego roku Plan sprawdzeń na następny rok i przedstawia go do akceptacji Administratorowi. Inspektor Ochrony Danych, co najmniej raz na pięć lat, przeprowadza sprawdzenie wszystkich zbiorów danych oraz systemów informatycznych służących do przetwarzania lub zabezpieczania danych osobowych. Sprawdzenie to powinno objąć następujące zagadnienia:

a. zabezpieczenia: organizacyjne i techniczne zbiorów danych osobowych,

b. system informatyczny służący do przetwarzania danych osobowych,

c. kompletność zidentyfikowanych zbiorów danych osobowych,

d. przesłanki legalności przetwarzania danych osobowych,

e. przesłanki legalności przetwarzania danych szczególnie chronionych,

f. zakres i cel przetwarzania danych,

g. merytoryczna poprawność danych i ich adekwatność do celu przetwarzania,

h. obowiązek informacyjny,

i. profilowanie,

j. przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,

k. powierzenie przetwarzania danych osobowych (w tym zakres i poprawność konstruowania umów powierzenia przetwarzania danych),

l. zabezpieczenia danych: organizacyjne i techniczne,

m. zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi zabezpieczeniami, technologiami, systemami i itp.

4 Przygotowanie sprawdzenia

4.1 Inspektor Ochrony Danych powiadamia Administratora o sprawdzeniu na min. 7 dni przed datą rozpoczęcia sprawdzenia.

4.2 Najpóźniej na tydzień przed terminem rozpoczęcia sprawdzenia Inspektor Ochrony Danych w porozumieniu z ASI oraz ewentualnie z pomocą Inspektora Ochrony Danych Urzędu Miasta Lublin, sporządzają program sprawdzenia, który jest dystrybuowany wg potrzeb.

4.3 Kryteria programu sprawdzenia uzależnione są od zakresu sprawdzenia, określonych przez Inspektora Ochrony

Danych oraz ASI.

5 Sprawdzenia zlecane przez Urząd Miasta Lublin

5.1 W jednostce mogą być przeprowadzane sprawdzenia w zakresie określonym przez Urząd Miasta Lublin.

5.2 Sprawdzenia mogą być realizowane przez Inspektora Ochrony Danych jednostki, Inspektora Ochrony Danych Urzędu Miasta Lublin lub przez osoby/podmioty zewnętrze działające w imieniu Urzędu Miasta Lublin.

6 Przebieg sprawdzenia

6.1 Sprawdzenie rozpoczyna się krótkim spotkaniem otwierającym, w którym bierze udział Kierownik sprawdzanej komórki organizacyjnej Jednostki oraz Inspektor Ochrony Danych. W trakcie spotkania Inspektor Ochrony Danych przedstawia cel i zakres sprawdzenia, omawia program sprawdzenia, wyjaśnia wątpliwości.

6.2 Inspektor Ochrony Danych realizuje przyjęty zakres sprawdzenia.

6.3 Inspektor Ochrony Danych dokumentuje obiektywne dowody potwierdzające istnienie stwierdzonych niezgodności mogących stanowić podstawę podjęcia działań przywracających stan zgodny z prawem. Inspektor Ochrony Danych potwierdza stwierdzone niezgodności swoim podpisem i proponuje działania naprawcze, o ile istnieje konieczność ich uruchomienia.

6.4 Na zakończenie sprawdzenia odbywa się spotkanie zamykające z udziałem Inspektora Ochrony Danych i Kierownika sprawdzanej komórki organizacyjnej Jednostki, podczas którego dokonywane jest podsumowanie sprawdzenia.

7 Sprawozdanie ze sprawdzenia

7.1 Z każdego zrealizowanego sprawdzenia Inspektor Ochrony Danych sporządza sprawozdanie, którego wzór jest zawarty w ***Załączniku nr 1 do niniejszej Procedury sprawdzeń***. Sprawozdanie powinno zawierać stwierdzone naruszenia ochrony danych osobowych oraz propozycje działań przywracający stan zgodny z prawem. W przypadku uruchomienia działań naprawczych sprawozdanie powinno zawierać określenie ich przyczyn. W sprawozdaniu zamieszcza się ocenę realizacji i skuteczności działań będących następstwem poprzedniego sprawdzenia.

7.2 Raport ze sprawdzenia jest dostarczany do Kierownika Jednostki w ciągu 30 dni od daty zakończenia sprawdzenia.

8 Następstwa sprawdzenia

8.1 W oparciu o wyniki sprawdzenia Inspektor Ochrony Danych w porozumieniu z osobami odpowiedzialnymi za obszar występowania niezgodności, np. Kierownikami komórek organizacyjnych czy Administratora Systemu Informatycznego, tworzy plany działań w celu usunięcia wykrytych niezgodności.

8.2 Plany działań korygujących akceptuje Kierownik Jednostki Organizacyjnej.

8.3 Za realizację działań korygujących odpowiadają osoby wskazane w planach działań korygujących.

8.4 Weryfikacja realizacji i skuteczności działań korygujących przeprowadzana jest we wskazanym w planie terminie realizacji planu lub maksymalnie podczas kolejnego sprawdzenia. Może być ona dokonywana wcześniej na polecenie Kierownika Jednostki.

9 Dokumenty związane

1. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

10 Załączniki

1. Załącznik nr 1 – Wzór sprawozdania ze sprawdzenia

Załącznik nr 1 – Wzór sprawozdania ze sprawdzenia danych osobowych

Oznaczenie sprawdzenia	
Oznaczenie Administratora i jego siedziby	
Imię i nazwisko Inspektora Ochrony Danych	
Wykaz czynności podjętych przez Inspektora Ochrony Danych w toku sprawdzenia	
Imiona, nazwiska osób biorących udział w sprawdzeniu	
Data rozpoczęcia sprawdzenia	
Data zakończenia sprawdzenia	
Przedmiot sprawdzenia	
Zakres sprawdzenia	
Efekty przeprowadzonych działań w po ostatnim sprawdzeniu	
Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz ocena zgodności przetwarzania danych z przepisami prawa powszechnie obowiązującego, aktami prawa wewnętrznego, politykami i Kodeksami .	
Wnioski i zalecenia (wraz z wskazaniem osoby odpowiedzialnej za realizację oraz terminu realizacji)	
Stwierdzone przypadki naruszenia przepisów prawa powszechnie obowiązującego, aktów prawa wewnętrznego, polityk i Kodeksów	
Planowane/podjęte działania przywracające stan zgodny z prawem (wraz z wskazaniem osoby odpowiedzialnej za realizację oraz terminu realizacji)	
Wykaz załączników	
Podpis Inspektora Ochrony Danych	
Data i miejsce podpisania sprawozdania	

Załącznik nr 6

do Polityki Bezpieczeństwa Informacji

Wzór upoważnienia do przetwarzania danych osobowych

Niniejszym pan/pani ..... zostaje upoważniony(a) do przetwarzania danych osobowych.

Stanowisko upoważnianego pracownika:

.....

Upoważnienie jest nadawane do następujących zbiorów danych osobowych w zakresie:

.....

.....

.....

.....

Uprawnienia do aplikacji służących do przetwarzania danych osobowych:

.....

.....

.....

Czas, na który udziela się upoważnienia:

.....

Miejscowość:

Data: :.....

Upoważniam:.....

Administrator Danych Osobowych

Oświadczenie o poufności upoważnionego.

Zobowiązuję się:

- zachować w tajemnicy przetwarzane dane osobowe;
- nie przekazywać ani nie ujawniać bez każdorazowej uprzedniej pisemnej zgody Administratora, jakichkolwiek danych osobowych żadnej osobie;
- ponieść wobec Administratora odpowiedzialność za naruszenie obowiązków w zakresie zachowania w tajemnicy danych osobowych;
- nie wykorzystywać i nie rozpowszechniać danych osobowych za wyjątkiem wykorzystywania wyłącznie w zakresie koniecznym dla celów realizacji obowiązków służbowych;
- dołożyć odpowiednich starań w celu zapewnienia i utrzymania odpowiednich środków zabezpieczających ochronę danych osobowych przed nieuprawnionym dostępem i bezprawnym wykorzystaniem przez osoby nieuprawnione.

Miejscowość:

Data:.....

Podpis Upoważnionego:.....

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji

Procedura szacowania ryzyka

Spis treści

1 Cel procedury

Celem Procedury szacowania ryzyka jest:

1. określenie zasad inwentaryzowania informacji chronionych,
2. określenie zasad szacowania ryzyka.

2 Zakres obowiązywania

Niniejszy dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przetwarzanie (papierowej, elektronicznej i innej).

3 Terminologia

Ryzyko w bezpieczeństwie informacji – zwane dalej ryzykiem – potencjalna sytuacja mogąca wystąpić z określonym prawdopodobieństwem, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów w celu spowodowania strat dla organizacji.

Ryzyko szczątkowe – poziom ryzyka po wdrożeniu zabezpieczeń.

Poziom ryzyka akceptowalnego – poziom zapewniający, że ryzyka szczątkowe są świadomie zaakceptowane przez Kierownika Jednostki Organizacyjnej.

Aktywo informacyjne - wszelkie informacje chronione w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością Jednostki Organizacyjnej.

Właściciel aktywa informacyjnego – Kierownik Jednostki Organizacyjnej lub Urząd Miasta Lublin.

Poufność informacji – atrybut bezpieczeństwa aktywa informacyjnego oznaczający, że dostęp do informacji powinny mieć jedynie osoby uprawnione.

Integralność – atrybut bezpieczeństwa aktywa i zasobu informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych.

Dostępność – atrybut bezpieczeństwa aktywa i zasobu informacyjnego oznaczający dostęp do informacji dla osób uprawnionych wtedy, kiedy jej potrzebują do przetwarzania.

Podatności – rozumiemy jako wady, luki lub słabości w strukturze fizycznej, organizacji działania Jednostki Organizacyjnej, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), które mogą być wykorzystane przez zagrożenie do spowodowania strat.

Zagrożenie informacji – potencjalne działanie wobec aktywa i zasobu informacyjnego lub procesu, mogące wykorzystać określoną podatność, w celu spowodowania strat.

Prawdopodobieństwo wystąpienia zagrożenia – potencjalna możliwość lub częstość występowania zagrożenia.

4 Identyfikacja i klasyfikacja informacji

Inwentaryzacja i ocena wartości aktywów i zasobów jest niezbędna, aby określić, jakie aktywa i zasoby powinny podlegać ochronie. Identyfikacja umożliwia określenie rodzaju i miejsca ich przechowywania oraz przetwarzania. Ocena wartości aktywa i zasobu umożliwia zmierzenie zależności Jednostki Organizacyjnej od danego aktywa i zasobu, a następnie przeprowadzenie identyfikacji i analizy ryzyka. Identyfikuje się te zasoby, od których zależy prawidłowe funkcjonowanie Jednostki Organizacyjnej. Przy wykonywaniu inwentaryzacji aktywów i zasobów uwzględnia się wymagania prawne wynikające z ustaw i rozporządzeń.

Klasyfikacji zasobów dokonuje się zgodnie z zapisami Polityki Bezpieczeństwa Informacji.

1. Metodyka identyfikacji aktywów informacyjnych:
   a) inwentaryzacja oraz identyfikacja aktywów i zasobów informacyjnych,
   b) określenie miejsc przetwarzania informacji,
   c) zidentyfikowanie właścicieli zasobów,
   d) wyszczególnienie zasobów oraz określenie istotności tych zasobów dla Jednostki Organizacyjnej,
   e) klasyfikacja aktywów i zasobów informacyjnych przeprowadzona przez gestorów informacji.
2. Klasyfikacja zasobów informacyjnych jest przeprowadzona przez właścicieli informacji, czyli jej gestorów, w formularzu będącym załącznikiem nr 1 do niniejszej procedury. Klasyfikacja dokonywana jest w kontekście trz podstawowych cech bezpieczeństwa informacji:
   a) **POUFNOŚCI**, która oznacza, że dostęp do informacji powinny mieć jedynie osoby uprawnione
   b) **INTEGRALNOŚCI**, która określa jakość informacji w aspekcie kompletności, spójności i wiarygodności danych
   c) **DOSTĘPNOŚCI**, która oznacza dostępność informacji dla osób uprawnionych.

Ocenę istotności (wartości) aktywów informacyjnych i zasobów wykonuje się według skali numerycznej od 1 do 4, gdzie 4 oznacza najwyższą wagę. Dla każdego z atrybutów informacji przyjmuje się wartości ze skali. Ostatecznie dla każdego z aktywów informacyjnych kalkuluje się istotność zgodnie z poniższą formułą:

$$WA = P + I + D$$

gdzie

WA – wartość aktywa

P – atrybut poufności aktywa podany w skali od 1 do 4

I – atrybut integralności aktywa podany w skali od 1 do 4

D – atrybut dostępności aktywa podany w skali od 1 do 4

Do oceny wartości zasobów przyjęto Tabelę Istotności Zasobów o 4-o stopniowej skali wartości. Wartości przypisuje się do atrybutu poufności, integralności oraz dostępności każdego z aktywów. Wartość 4 oznacza największą istotność bezpieczeństwa aktywa, np. poufność oceniona na 4 oznacza najwyższą wartość wymagań dla zachowania poufności rozpatrywanego aktywa. Analogicznie w tym przykładzie wartość 0 dla poufności oznacza brak wymagań dla zachowania poufności rozpatrywanego aktywa.

Wartość liczbowa	Opis
4	Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu drastycznie zakłóca lub całkowicie uniemożliwia pracę z aktywem. Możliwa jest również poważna odpowiedzialność prawna i negatywny rozgłos medialny.
3	Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może znacząco zakłócić pracę z aktywem. Możliwa jest również odpowiedzialność prawna lub negatywny rozgłos medialny.
2	Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może utrudnić pracę z aktywem. Możliwy jest również negatywny rozgłos medialny.
1	Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może w niewielkim stopniu utrudnić pracę z aktywem, jednak główne zadania w zakresie danego aktywą mogą być nadal realizowane.

Wartość liczbowa	Opis
0	Brak wymagań bezpieczeństwa w zakresie danego atrybutu. Oznacza to brak konieczności stosowania zabezpieczeń w danym obszarze.

Przynależność aktywa informacyjnego do właściwej klasy zależy od wartości tego aktywa. Wartość WA aktywa informacyjnego oblicza się zgodnie z wzorem podanym powyżej.

Przyjmuje się 4 klasy ochrony informacji:

1. Klasa 1 – niski poziom ochrony. WA < 2
2. Klasa 2 – średni poziom ochrony. 8 > WA >= 2
3. Klasa 3 – wysoki poziom ochrony. 11 > WA >= 8
4. Klasa 4 – bardzo wysoki poziom ochrony. WA > =11

Efektem identyfikacji i klasyfikacji informacji powinien być Wykaz aktywów informacyjnych, będący wejściem do etapu analizy ryzyka dla bezpieczeństwa informacji.

Wykaz zidentyfikowanych aktywów i zasobów informacyjnych zawiera ***Załącznik nr 1 do niniejszej procedury***. Zbiorczy wykaz aktywów i zasobów informacyjnych prowadzi Kierownik Jednostki Organizacyjnej.

Szacowanie ryzyka

5.1 Analiza ryzyk

Analizę ryzyka przeprowadza się w zakresie obszarów o największej istotności, w szczególności analizuje się ryzyka utraty wymaganego poziomu poufności, integralności oraz dostępności dla danych osobowych. Ryzyka szacuje się szczególnie dla danych osobowych w kontekście utraty praw lub wolności osób fizycznych zgodnie z art. 32 RODO. Należy założyć, że utrata wymaganego poziomu poufności, integralności lub dostępności danych osobowych może skutkować naruszeniem praw lub wolności osób fizycznych. Przyjmuje się, że powaga tego naruszenia jest adekwatna do poziomu ryzyka określanego zgodnie z niniejszą procedurą.

Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla poziomu ryzyka większego niż akceptowalny. W przyjętym modelu jest to wartość **w większa lub równa 32**. Analiza ryzyka jest przeprowadzana **nie rzadziej niż raz do roku, w terminie określonym przez Kierownika Jednostki Organizacyjnej.** Ryzyka są monitorowane przez Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego.

Analiza ryzyka przeprowadzana jest **również po wprowadzeniu zmian** mających wpływ na wymagany poziom poufności, integralności oraz dostępności aktywów informacyjnych.

Wzór Rejestru ryzyka Jednostki Organizacyjnej w bezpieczeństwie informacji jest załącznikiem nr 2 do niniejszej procedury.

5.2 Identyfikacja zagrożeń i podatności

Zagrożenie jest potencjalnym działaniem wobec aktywa i zasobu informacyjnego, mogącym wykorzystać określoną podatność, mającym na celu spowodowanie strat.

Należy rozpoznać zagrożenia dla bezpieczeństwa informacji przetwarzanych i przechowywanych w Jednostce Organizacyjnej oraz określić ich wpływ na bezpieczeństwo tychże informacji.

Należy brać pod uwagę następujące klasy zagrożeń w szczególności:

1. zewnętrzne – kryzys finansowy, zmiana prawa, klęski żywiołowe, siła wyższa,

2. ludzkie – kradzież, podsłuch, zgubienie, szpiegowanie, celowe działanie użytkownika, niecelowe działanie użytkownika, działanie intruza,
3. użytkownika – brak odpowiedniego przeszkolenia,
4. proceduralne – błędy w ochronie fizycznej i technicznej,
5. Sprzętu i oprogramowania – wady oprogramowania, awarie sprzętu,

Każde zdarzenie będące zagrożeniem dla zasobu powinno być powiązane z podatnością, którą należy rozumieć w szczególności jako wadę, lukę lub słabość w strukturze fizycznej, zasobach materialnych, organizacji, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), która może być wykorzystana przez zagrożenie w celu spowodowania strat.

Wyniki identyfikacji zagrożeń i podatności po przeprowadzanej analizie wraz z ich wartościami odpowiednich parametrów, przypisanymi do odpowiednich aktywów i zasobów informacyjnych przedstawione są ***Rejestrze ryzyk w bezpieczeństwie informacji***.

5.3 Dobór zabezpieczeń

Cele stosowania zabezpieczeń i zabezpieczenia powinny być dobierane adekwatnie do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

Zabezpieczenia fizyczne, techniczne i organizacyjne dobierane są tak, aby uzupełniać się wzajemnie, zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 27002:2014:12 oraz dobrymi praktykami.

5.4 Proces szacowania ryzyka

Każda miara powiązana z elementem bezpieczeństwa powinna być rozpatrywana w **trzech niezależnych aspektach: poufności, integralności oraz dostępności**. Wartości dla poufności, integralności oraz dostępności obliczane są niezależnie, stąd każdy element bezpieczeństwa charakteryzuje się trzema odrębnymi grupami parametrów podlegających identycznym obliczeniom i zasadom zgodnie z przyjętą metodyką analizy ryzyka zatwierdzoną w Jednostce Organizacyjnej.

5.4.1 Krok 1. Scenariusze wykorzystania podatności przez zagrożenie

Opis potencjalnego zdarzenia wykorzystania podatności przez zagrożenie jest kluczowy dla przeprowadzenia prawidłowej analizy. Powinny być rozpatrywane zdarzenia, których działanie prowadzi do utraty całkowitej bądź częściowej poufności, integralności oraz dostępności aktywa. Zdarzenia powinny być opisywane w szczególności za pomocą:

1. źródła ryzyka,
2. opisu podatności,
3. opisu zagrożenia,
4. nazwy aktywa/zasobu podlegającego zdarzeniu.

5.4.2 Krok 2 – prawdopodobieństwo wystąpienia zdarzenia

Dla każdego zdarzenia, w wyniku którego może zrealizować się rozpatrywane ryzyko, należy dobrać odpowiednie wartości prawdopodobieństwa. Podczas oceny prawdopodobieństwa wystąpienia zagrożenia wykorzystującego wskazaną podatność w celu spowodowania strat w zasobie, należy uwzględniać nie tylko potencjalne zajście zdarzenia w przyszłości, lecz również sytuacje z przeszłości.

Dla każdego prawdopodobieństwa należy dobrać wartości zgodnie z poniższą tabelą.

Wartość	Opis

4	Realizacja raz w tygodniu
3	Realizacja raz na trzy miesiące
2	Realizacja raz na rok
1	Realizacja raz na dwa lata lub rzadziej

Uwaga. Dla niektórych sytuacji przyjmuje się niezerowe wartości prawdopodobieństwa, pomimo że sytuacja występuje niezmiernie rzadko. Przykładem są: klęski żywiołowe, katastrofy naturalne, pożar, powódź.

5.4.3 Krok 3 – wpływ zagrożenia

Wpływ zagrożenia rozumiemy jako skutki dla naszej organizacji w wyniku opisanego scenariusza zdarzenia. Tutaj wpływ rozumiemy jako utratę bezpieczeństwa dla poufności, integralności oraz dostępności zasobu. Wartości wpływu dobieramy dla poufności, integralności oraz dostępności zgodnie z poniższą tabelą.

Wartość	Opis
4	Bardzo poważne naruszenie bezpieczeństwa zasobu, które może rodzić konsekwencje prawne, wizerunkowe oraz dla ciągłości działania organizacji. Naruszenie dotyczy najważniejszych elementów zasobu. Naruszenie uniemożliwia korzystanie z zasobu. Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne lub nawet nieodwracalne konsekwencje.
3	W wyniku naruszenia poważnie zakłócone są procesy zależne od korzystania z zasobu. W wyniki zadziałania zagrożenia organizacja odczuwa poważne zakłócenie natury technicznej oraz organizacyjnej. Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne konsekwencje, które są w stanie rozwiązać z wieloma trudnościami.
2	Naruszone jest bezpieczeństwo zasobu, jednak nie rodzi ono konsekwencji prawnych, wizerunkowych i innych poważnych skutków dla organizacji. Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne niedogodności, które są w stanie rozwiązać pomimo kilku trudności
1	Naruszenie bezpieczeństwa ma ograniczone konsekwencje dla organizacji. Nie rodzi skutków prawnych, wizerunkowych czy dla ciągłości działania organizacji. Osoby fizyczne, których dane osobowe są objęte naruszeniem, praktycznie nie odczuwają skutków.
0	Brak wpływu

5.4.4 Krok 4 – inwentaryzacja zabezpieczeń

Właściwa ocena sytuacji, w której może zadziałać zagrożenie, wymaga określenia stosowanych zabezpieczeń dla zasobu. Szczególnie istotna jest skuteczność stosowanych zabezpieczeń dla zapewnienia poufności, integralności oraz dostępności zasobu.

W przyjętej metodzie należy uwzględnić obecnie stosowane zabezpieczenia podczas określania wartości wpływu zagrożenia na aktywo.

5.4.5 Krok 5 – ocena ryzyka

dobraniu odpowiednich wartości i uwzględnieniu obecnego stanu zabezpieczeń, Arkusz kalkulacyjny automatycznie oblicza wartości ryzyk. Wartości ryzyk przyjmują wartości z przedziału od 1 do 64.

W przyjętej metodzie ryzyko zależy od wartości wpływu, prawdopodobieństwa oraz klasy ochrony aktywa. Należy oszacować ryzyko utraty poufności Rp, integralności Ri oraz dostępności aktywa Rd.

$$Rp = Wartość\ skutków\ z\ powodu\ utraty\ poufności * Wartość\ prawdopodobieństwa * Klasa\ aktywa(zależna\ od\ WA)$$

$$Ri = Wartość\ skutków\ z\ powodu\ utraty\ integralności * Wartość\ prawdopodobieństwa * Klasa\ aktywa(zależna\ od\ WA)$$

$$Rd = Wartość\ skutków\ z\ powodu\ utraty\ * Wartość\ prawdopodobieństwa * Klasa\ aktywa(zależna\ od\ WA)$$

Bardzo istotnym krokiem jest dobranie ryzyka akceptowalnego, poniżej którego wartości ryzyka będzie określać jako szczątkowe (rezydualne). Poziom ryzyka akceptowalnego należy określić na podstawie oszacowań ryzyka dla wszystkich przyjętych do analizy zagrożeń. Należy przyjąć poziom ryzyka akceptowalnego dla każdego z obszarów lub procesów organizacji, lub przyjąć globalną wartość ryzyka akceptowalnego. Wynik porównania wartości ryzyk dla zagrożeń i wartości ryzyka akceptowalnego jest podstawą procesu zarządzania ryzykiem, w którym powinniśmy reagować na ryzyka ponad akceptowalne na kilka sposobów np. stosując dodatkowe zabezpieczenia.

W przyjętym modelu należy kierować się poniższą mapą ryzyka.

Skutki dla organizacji	Prawdopodobieństwo scenariusza zdarzenia			
	Niskie	Średnie	Wysokie	Bardzo wysokie
Bardzo wysokie	Od 24 do 32	Od 32 do 40	Od 40 do 48	Powyżej 48
Wysokie	Od 16 do 24	Od 24 do 32	Od 32 do 40	Od 40 do 48
Średnie	Od 8 do 16	Od 16 do 24	Od 24 do 32	Od 32 do 40
Niskie	Od 1 do 8	Od 8 do 16	Od 16 do 24	Od 24 do 32

Ryzyka w kolorze niebieskim należy monitorować, czy nie zbliżają się do kolejnego obszaru. Kolorem pomarańczowym zaznaczono te ryzyka, którymi należy zająć się w dłuższym okresie czasu. Natomiast kolorem czerwonym zaznaczono te ryzyka, którymi należy zająć się natychmiast.

5.5 Postępowanie z ryzykiem

Kierownik Jednostki Organizacyjnej zatwierdzając Rejestr ryzyk w bezpieczeństwie informacji określa zasady postępowania z ryzykiem. Zgodnie z PN-ISO/IEC 27005:2014 stosuje się cztery warianty postępowania z ryzykiem:

1. **Modyfikowanie ryzyka** - polega na zredukowaniu poziomu ryzyka przez taki wybór zabezpieczeń, aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne.
2. **Zachowanie ryzyka** - polega na podjęciu decyzji o zachowaniu ryzyka bez podejmowania dalszych działań, na podstawie oceny ryzyka.
3. **Unikanie ryzyka** - polega na unikaniu działań lub warunków, które powodują powstanie określonych ryzyk.
4. **Dzielenie ryzyka** - na podstawie oceny ryzyka zaleca się transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem.

Wszystkie ryzyka o wartości poniżej akceptowanego poziomu ryzyka o wartości mniejszej niż 32 zostaną **zachowane**. W przypadku poziomu ryzyka o wartości równej i większej 32 po wybraniu wariantu postępowania z ryzykiem należy przygotować plan postępowania z ryzykiem.

Plan postępowania z ryzykiem powinien zawierać:

1. opis postępowania z ryzykiem,
2. wybrane zabezpieczenia,
3. wskazanie odpowiedzialności za realizację planu,
4. ewentualne koszty związane z realizacją planu,
5. w razie potrzeby harmonogram działań.

Plan postępowania z ryzykiem zatwierdza Kierownik Jednostki Organizacyjnej, a realizację monitoruje Inspektor Ochrony Danych. Za wdrożenie planów odpowiedzialni są wyznaczeni przez Kierownika Jednostki Organizacyjnej pracownicy.

5.6 Monitorowanie i przegląd ryzyka

Proces identyfikacji i analizy ryzyka w Jednostce Organizacyjnej jest procesem ciągłym i monitorowanym w szczególności pod względem:

1. nowych lub zwiększonych zagrożeń pojawiających się zarówno na zewnątrz, jak i wewnątrz Jednostki Organizacyjnej,
2. szacowania prawdopodobieństwa występujących zdarzeń,
3. analizy nowych lub zwiększonych podatności mogących umożliwić zagrożeniom ich wykorzystanie,

4. analizy zwiększonych konsekwencji szacowanych zagrożeń, podatności, ryzyk, których agregacja może spowodować przekroczenie kryteriów akceptacji ryzyka.

Przebieg procesu monitorowania ryzyka sprawia, że należy zapewnić ciągłą dostępność zasobów organizacyjnych i technicznych, które mogą go realizować.

Proces monitorowania ryzyka polega na prowadzeniu przeglądu ryzyk w terminie wskazanym przez Kierownika Jednostki Organizacyjnej oraz na zgłoszeniu nowych i zmian w istniejących ryzykach w trakcie roku.

Monitorowanie i przegląd procesu zarządzania ryzykiem dotyczy w szczególności:

1. kontekstu prawnego i umownego Jednostki Organizacyjnej,
2. kryteriów szacowania ryzyka,
3. kategorii zasobów i ich wartościowania,
4. kryteriów akceptowania ryzyka,
5. kontrolowanie kosztów zarządzania ryzykiem.

6 Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

7 Załączniki

1. Załącznik nr 1 – Wzór Wykazu aktywów informacyjnych.
2. Załącznik nr 2 – Wzór Rejestru ryzyk Jednostki Organizacyjnej w bezpieczeństwie informacji.

Załącznik nr 9 do PBI – Wzór Rejestru naruszeń bezpieczeństwa, w tym incydentów

Lp.																		
Administratora danych lub informacja o współadministratorach danych (nazwa i adres)																		
Miejsce																		
Forma i nośniki danych																		
Lokalny Administrator Zbiorów (albo określoną osobę gdy wyciek miał miejsce na danych nieprzetwarzanych w zbiorze)																		
Charakterystykę naruszenia																		
Określenie kogo dotyczą skutki naruszenia																		
Kategorie lub rodzaje osób, których dane zostały naruszone																		
Rodzaje/kategorie naruszonych danych																		
Szacowana liczba osób dotkniętych naruszeniem																		
Szacowana liczba rekordów/wpisów w ramach naruszenia																		
Skutki naruszenia - dla osób fizycznych (wszystkie możliwe konsekwencje)																		
Informacja o zgłoszeniu naruszenia do właściwego organu nadzorczego (forma, data i godzina, zgłaszający, link do treści zgłoszenia)																		
Ewentualne wyjaśnienie przekroczenia 72h terminu na zgłoszenie																		
Ewentualna informacja o zgłoszeniu naruszenia dotkniętym naruszeniem osobom fizycznym (+ link do treści zgłoszenia)																		
Ewentualna informacja o publicznym poinformowaniu o naruszeniu osób fizycznych dotkniętych naruszeniem (+ link do treści zgłoszenia, + powód wybrania tej metody)																		
Zastosowane środki w celu minimalizacji skutków naruszenia																		
Zastosowane środki w celu wyeliminowania naruszeń tego typu na przyszłość																		

PRZYKŁADOWA INSTRUKCJA TWORZENIA KLAUZULI INFORMACYJEJ

Informacje o:

a. **Administratorze Danych Osobowych (zwanym też Administratorem):**

Nazwa Administratora Danych Osobowych[1]	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

b. **Inspektorze Ochrony Danych (jeżeli dotyczy)[2]:**

Inspektor Ochrony Danych *(imię i nazwisko – opcjonalnie)*	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

Osoba ta uprawniona jest do kontaktu z klientami w imieniu Administratora Danych Osobowych w sprawach związanych z ochroną, gromadzeniem, przetwarzaniem, modyfikowaniem i usunięciem danych osobowych.

Definicje:

Administrator informuje, że:

a. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i dane wrażliwe.

   Jako przykład danych zwykłych można wskazać:

   - numery identyfikacyjne: imię, nazwisko, adres zamieszkania, PESEL, NIP, paszport, dowód osobisty,
   - cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne,
   - cechy fizjologiczne: grupa krwi,
   - cechy ekonomiczne: status majątkowy, lista zaległości finansowych.

---

[1] Należy wskazać nazwę *(np. Urząd Gminy w .....)* i adres podmiotu *(ul. Niezapominajki 1, 01-926 Warszawa)*, który zbiera dane osobowe oraz dane kontaktowe do tego podmiotu

[2] Zgodnie z postanowieniami RODO Administrator nie ma obowiązku powoływania Inspektora Ochrony Danych (wówczas sam pełni jego funkcję); podmiot nie musi podawać imienia i nazwiska osoby pełniącej funkcję Inspektora Ochrony Danych; musi natomiast wskazywać dane kontaktowe do osoby pełniącej tę funkcję;

- środki komunikacji elektronicznej: numer telefonu, adres e-mai.

Do danych wrażliwych zaliczają się dane dotyczące:

- pochodzenie rasowe i etniczne,
- przekonania religijne czy światopoglądowe,
- przynależność do związków zawodowych czy partii,
- poglądy polityczne,
- stan zdrowia,
- kod genetyczny,
- dane biometryczne
- dane o seksualności lub orientacji seksualnej,
- wyroków skazujących i naruszeń prawa.

b. **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Przy czym przez sformułowanie „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

c. **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

d. **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.

e. **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).

f. **Usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Informacje o pobieranych/gromadzonych danych:

1) Cel przetwarzania: .....[3]

2) Podstawa prawna przetwarzania danych osobowych: .....[4]

---

[3] Należy wskazać cel gromadzenia i przetwarzania danych osobowych, np. proces rekrutacyjny – zatrudnienie pracownika

[4] Np. art. ..... ustawy z dnia ..... o ..... (Dz.U. .....)

3) Informacja, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych: .....[5]

4) Kategorie odnośnych danych osobowych: .....[6]

5) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją: .....[7]

6) Informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO:

a. nie dotyczy/dane osobowe zostaną przekazane do[8]*:

Nazwa Podmiotu	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

dane kontaktowe Inspektora Ochrony Danych tego podmiotu[9]:

Inspektor Ochrony Danych *(imię i nazwisko – opcjonalnie)*	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

b. zabezpieczenia stosowane przez podmiot/organizację międzynarodową zapewniają ochronę danych nie gorszą niż wymagane przez przepisy 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);

c. osoba przekazująca dane Administratorowi może zwrócić się, do Inspektora Danych Osobowych lub bezpośrednio do osoby wskazanej w lit. a, o przekazanie jej kopii danych osobowych, które temu podmiotowi zostały przekazane do przetwarzania;

d. cel przekazania danych osobowych: .....

e. podstawa prawna powierzenie przetwarzania: .....

---

[5] Dane osobowe są zbierane w celu wypełnienia obowiązków wynikających z ustawy z dnia .... (Dz.U.....) lub na podstawie umowy z dnia ....., której przedmiotem jest .....

[6] Dane dotyczące pracowników, małoletnich, czy też osób z zewnątrz (mieszkańcy Gminy .....)

[7] Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią,

[8] Jw.

[9] Jw.

7) Informacja o zawarciu umowy powierzenia przetwarzania: Administrator zawarł umowę powierzenia przetwarzania/Administrator nie zawarł umowę powierzenia przetwarzania.* Umowa została zawarta z:

Nazwa Podmiotu	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

dane kontaktowe Inspektora Ochrony Danych tego podmiotu:

Inspektor Ochrony Danych *(imię i nazwisko – opcjonalnie)*	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

a. zabezpieczenia stosowane przez ww. podmiot zapewniają ochronę danych nie gorszą niż wymagane przez przepisy 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);

b. osoba przekazująca dane może zwrócić się, do Inspektora Danych Osobowych lub bezpośrednio do osoby wskazanej w lit. a, o przekazanie jej kopii danych osobowych, które temu podmiotowi zostały przekazane do przetwarzania;

c. cel przekazania danych osobowych: .....[10]

d. podstawa powierzenie przetwarzania: .....[11]

8) Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu: .....[12]

9) Źródło pochodzenia danych osobowych: .....[13]

10) Informacja o profilowaniu (przez profilowanie rozumie się dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się)[14]: tak/nie*

---

[10] Jw.

[11] Jw.

[12] np. 2 lata, przez okres procesu rekrutacji,

[13] np. dane zostały przekazane przez osobę ubiegającą się o zatrudnienie,

[14] RODO wskazuje dwie kategorie profilowania: polegające na ocenie prawdziwych informacji pozyskanych na temat danej osoby albo na wytworzeniu nowej informacji o osobie, na podstawie wiedzy pozyskanej na jej temat. W drugim przypadku nowa informacja będzie jedynie statystycznie prawdziwa, a co za tym idzie pojawia się ryzyko przypisania podmiotowi danych cech, których w istocie on nie posiada, co z kolei doprowadzić może do nieusprawiedliwionego pozbawienia go dostępu do pewnych dóbr i usług. RODO przewiduje również dwie formy profilowania – profilowanie zwykłe (z udziałem czynnika ludzkiego) oraz zautomatyzowane, gdzie cały

a. informacje o zasadach podejmowania decyzji (czyli w jaki sposób ta ocena następuje oraz przy pomocy jakich narzędzi będzie dochodzić do takiej oceny)[15]:

.....

b. informacje o znaczeniu i przewidywanych konsekwencjach dla osoby, której dane te dotyczą (jakie skutki prawne może nieść za sobą taka decyzja lub w jaki sposób prawnie będzie ta decyzja na daną osobę wpływać):

.....[16]

11) Informacja o współadministrowaniu danymi: Przekazane dane osobowe są gromadzone w zbiorze, który jest współadministrowany przez następujące podmioty[17]:

Nazwa Współadministratora	Adres	Dane kontaktowe Wpóładministratora	Dane kontaktowe Inspektora Ochrony Danych
		Tel. ..... Fax. ..... e-mail	Tel. ..... Fax. ..... e-mail ..... Imię i nazwisko: ..... (opcjonalnie)
		Tel. ..... Fax. ..... e-mail	Tel. ..... Fax. ..... e-mail ..... Imię i nazwisko: ..... (opcjonalnie)

Informacja o prawach osoby, której dane są przetwarzane:

12) Osobie, której dane są przetwarzane przysługuje prawo do złożenia skargi związanej z przetwarzaniem jej danych osobowych przez Administratora lub podmiot/organizację, której dane osobowe zostały przekazane do[18]:

Nazwa organu nadzoru	Adres	Dane kontaktowe
		Tel. ..... Fax. ..... e-mail .....

13) Informacje o prawie do wniesienia żądania udzielenia jej informacji o przetwarzanych danych:

proces oceny oraz podjęcie decyzji dokonują programy komputerowe (procesy kończące się podjęciem zautomatyzowanej decyzji). Należy zauważyć, że wskazane kategorie profilowania mogą przybierać zarówno formę profilowania zwykłego, jak i zautomatyzowanego.

[15] Wypełnia się w przypadku wykonywania profilowania

[16] np. przyznanie premii,

[17] Należy wskazać wszystkich współadministratorów zbioru (np. gdy dwa różne podmioty wspólnie korzystają i zbierają dane, które umieszczane są w zbiorze)

[18] Należy wskazać organ nadzoru utworzony na podstawie ustawy o ochronie danych osobowych (Prezesa Urzędu Ochrony Danych Osobowych)

a. Osoba, której dane są przetwarzane ma prawdo do złożenia w każdym czasie żądania udzielenie jej informacji o przetwarzanych danych.

b. Administrator bez zbędnej zwłoki – nie później niż w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO (żądanie do sprostowania, zaprzestania lub usunięcia danych osobowych). W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

c. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

d. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

14) Informacja o prawie wniesienia żądania wniesienia sprostowania jej danych: Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Osoba, której dane są przetwarzane ma prawo do złożenia żądania w każdym czasie u Administratora.

15) Informacja o prawie wniesienia żądania ograniczenia przetwarzania danych: Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania jej danych w następujących przypadkach:

a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;

b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

c. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d. osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe będą dalej przetwarzane, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

16) Informacja o prawie wniesienia sprzeciwu wobec przetwarzania danych: Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, w tym profilowania. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

17) Informacja dotycząca „prawa do bycia zapomnianym": Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b. brak jest podstawy prawnej przetwarzania;
   c. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na wobec przetwarzania;
   d. dane osobowe były przetwarzane niezgodnie z prawem;
   e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;
   f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

   Jeżeli Administrator upublicznił dane osobowe, ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Potwierdzenie otrzymania klauzuli informacyjnej:

Oświadczam, że zostałem poinformowany o przysługujących mi prawach dotyczących ochrony, przetwarzania, powierzenia, sprostowania, usunięcia danych osobowych – w prostej i zrozumiałej formie. Wszystkie moje wątpliwości zostały mi wyjaśnione. Oświadczam, że przekazuję dane osobowe świadomie i dobrowolnie.

Imię i nazwisko: .....

Adres: .....

Podpis ..... data .....