**ZARZĄDZENIE**
**WOJEWODY LUBUSKIEGO**

z dnia 17 maja 2019 r.

**w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim**

Na podstawie art. 24 ust 2 rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.Urz. UE L 119) w związku art. 17 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2017 r. poz 2234 i z 2018 r. poz. 2340) zarządza się, co następuje:

**§ 1.** Wprowadza się Politykę Bezpieczeństwa Danych Osobowych w Lubuskim Urzędzie Wojewódzkim, stanowiącą załącznik do niniejszego zarządzenia.

**§ 2.** Uchyla się zarządzenie Wojewody Lubuskiego z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp.

**§ 2.** Zarządzenie wchodzi w życie z dniem podpisania.

Wojewoda Lubuski

**Władysław Dajczak**

LUBUSKI
URZĄD WOJEWÓDZKI

**Załącznik**
**do zarządzenia**
**Wojewody Lubuskiego**

# POLITYKA
# BEZPIECZEŃSTWA DANYCH OSOBOWYCH
# W LUBUSKIM URZĘDZIE WOJEWÓDZKIM
# W GORZOWIE WIELKOPOLSKIM

wersja 1.1

## HISTORIA ZMIAN

| Nr wersji | Data | Opis | Działanie (*) | Rozdziały(**) | Autorzy |
|---|---|---|---|---|---|
| 1.0 | | Utworzenie nowego dokumentu | N | W | P. Pikuła.<br>M. Piaskowski. |
| | | | W | W | G. Krzeski,<br>K. Jankowiak<br>A. Szymczak,<br>A. Ladowski. |
| 1.1 | | Dodanie załącznika nr 5 | N | W | P. Pikuła |
| | | | | | |
| | | | | | |
| | | | | | |

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja

(**) Rozdziały: numery rozdziałów lub W-Wszystkie

## Spis treści

**SPIS ZAŁĄCZNIKÓW:**

Słownik pojęć i skrótów

| **Termin / skrót** | **Wyjaśnienie/opis** |
|---|---|
| ADO | administrator danych osobowych – Wojewoda Lubuski |
| AS | administrator systemu – kierownik oddziału ds. informatyki |
| Polityka | oznacza niniejszą Politykę ochrony danych osobowych Lubuskiego Urzędu Wojewódzkiego |
| RODO | rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. Urz. UE L 119, s. 1). |
| IOD | inspektor ochrony danych – osoba powołana przez ADO |
| Kierownik komórki | kierownik komórki – dyrektor wydziału lub biura, Lubuski Wojewódzki Inspektor Nadzoru Geodezyjnego i Kartograficznego, Audytor Wewnętrzny, Pełnomocnik ds. Ochrony Informacji Niejawnych, kierownik Delegatury Lubuskiego Urzędu Wojewódzkiego |
| LUW | Lubuski Urząd Wojewódzki w Gorzowie Wielkopolskim |
| Osoba upoważniona | osoba, która upoważniona została na piśmie do przetwarzania danych osobowych przez administratora danych lub osobę wyznaczoną do wydawania odpowiedniego upoważnienia |
| SZBI | system zarządzania bezpieczeństwem informacji obowiązujący w LUW w rozumieniu Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113). |

| | |
|---|---|
| EU/EOG | państwa należące do Unii Europejskiej/Europejskiego Obszaru Gospodarczego |
| Prezes Urzędu | Prezes Urzędu Ochrony Danych Osobowych |
| Organ nadzorczy | Urząd Ochrony Danych Osobowych |
| Ustawa | ustawa o ochronie Danych Osobowych z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. 2018 poz. 1000 |
| System informatyczny administratora | rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych. |
| integralność | właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany |
| poufność | właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom |
| dostępność | właściwość zapewniająca, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie |
| zbiór danych | uporządkowany zestaw danych osobowych, o którym mowa w art. 4 RODO pkt. 2, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie |

# I. Wstęp

Polityka Bezpieczeństwa Danych Osobowych w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp. ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Niniejszy dokument jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE L 119, s. 1).

# II. Postanowienia ogólne

## 1. Cele Polityki Bezpieczeństwa Danych Osobowych

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, niniejsza Polityka ma na celu zapewnić odpowiednie środki, aby przetwarzanie odbywało się zgodnie z RODO.

## 2. Zakres stosowania

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. stażystów, praktykantów. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń IOD.

Z systemów informatycznych służących do przetwarzania danych osobowych

znajdujących się w posiadaniu ADO mogą korzystać również inne podmioty, na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźnie zdefiniowanie celu i zakresu oraz wskazanie odpowiedzialności.

### 3. Ogólne zasady dotyczące przetwarzania danych osobowych

Administrator Danych przetwarza dane osobowe z poszanowaniem zasad wyrażonych w art. 5 RODO. Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

## III. System obsługi praw jednostki

Administrator danych zapewnia obsługę praw osób, których dane dotyczą poprzez:

1) wdrożenie zasad przekazywania prawem wymaganych informacji przy pozyskiwaniu danych;
2) wdrożenie zasad, w zakresie realizacji żądań osób, których dane dotyczą w terminach i w sposób wymagany w RODO oraz zapewnienie dokumentacji realizacji tego obowiązku;

3) wdrożenie procedur pozwalających na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych;
4) poszanowanie oraz ochronę praw i wolności osób trzecich.

## IV. Przypisanie ról i organizacja procesów przetwarzania danych osobowych

ADO wyznacza role oraz odpowiedzialność poszczególnych osób realizujących zadania w procesie przetwarzania danych osobowych.

### 1. Administrator danych osobowych

Administrator danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) wdraża adekwatne, proporcjonalne oraz skuteczne środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO; przez odpowiednie środki rozumie się w szczególności:
    a. zatwierdzone kodeksy postępowania (o ile zostały wdrożone);
    b. certyfikację (o ile została dokonana na podstawie kryteriów certyfikacji, o których mowa w RODO przez Prezesa Urzędu lub podmiot certyfikujący zgodnie z wymogami Ustawy);
    c. wytyczne oraz opinie Europejskiej Rady Ochrony Danych;
    d. wytyczne Prezesa Urzędu;
    e. sugestie inspektora ochrony danych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi powierzonych im obowiązków (wzór upoważnienia - załącznik Nr 2);
3) wyznacza inspektora ochrony danych oraz określa zakres jego zadań i czynności i zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
4) zleca Dyrektorowi Generalnemu LUW, by we współpracy z administratorem systemu oraz inspektorem ochrony danych zapewnił użytkownikom odpowiednie warunki

pracy umożliwiające bezpieczne przetwarzanie danych;

5) podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

## 2. Inspektor Ochrony Danych

Inspektor ochrony danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) informuje administratora podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) monitoruje przestrzeganie RODO, innych przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków;

3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

4) współpracuje z organem nadzorczym;

5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

6) pełni rolę punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;

7) opiniuje wzory dokumentów dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne administratora danych;

8) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji – załącznik Nr 3) oraz ewidencję oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (wzór oświadczenia – załącznik Nr 4);

9) na podstawie otrzymanych informacji z komórek organizacyjnych Urzędu, aktualizuje rejestr czynności oraz rejestr kategorii czynności;

10) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, występuje z wnioskiem do ADO o nadanie upoważnienia do przetwarzania danych osobowych;

11) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, występuje z wnioskiem do AS o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;

12) prowadzi rejestr zasad, instrukcji oraz procedur zatwierdzonych lub wycofanych przez ADO będących uzupełnieniem niniejszej Polityki;

13) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych.

### 3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników;

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego ADO;

6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

7) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

8) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

9) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

10) prowadzi ewidencję identyfikatorów do stanowisk roboczych poszczególnych użytkowników;

11) na podstawie otrzymanych informacji z komórek organizacyjnych Urzędu, prowadzi wykaz systemów informatycznych niepodlegających zasadom, bezpieczeństwa ochrony danych, określonym w LUW.

**4. Kierownicy komórek**

1) zobowiązani są do zapewnienia działań zgodnych z prawem w ramach powierzonej komórki organizacyjnej;

2) zobowiązani są do stałego nadzoru i stosowania środków mających na celu zapewnienie bezpieczeństwa powierzonego im zasobu;

3) zobowiązani są zapewnić, aby przetwarzane w ramach powierzonej im komórki organizacyjnej dane były aktualne, adekwatne, stosowne oraz ograniczone do tego co niezbędne w stosunku do celów, w jakich są przetwarzane, a także przetwarzane nie dłużej niż jest to konieczne do realizacji celu;

4) zobowiązani są do realizacji obowiązku informacyjnego oraz o ile to możliwe dokumentowania tej czynności;

5) zobowiązani są do niezwłocznej konsultacji z IOD wszelkich żądań osób, których dane dotyczą i sposobu ich realizacji;

6) zobowiązani są do prowadzenia ewidencji zgłoszonych żądań wraz ze wskazaniem sposobu ich realizacji w zakresie powierzonej komórki organizacyjnej;

7) zobowiązani są do dokumentowania i przechowywania zgód na przetwarzanie danych

osobowych;

8) zobowiązani są do zgłoszenia IOD wszystkich przypadków nienależytego zabezpieczenia danych osobowych;

9) za pośrednictwem IOD występują z wnioskiem do ADO o wydanie, modyfikację lub uchylenie upoważnień do przetwarzania danych osobowych dla podległych im pracowników;

10) zobowiązani są zapewnić, aby podległe im osoby upoważnione do przetwarzania danych osobowych posiadały dostęp wyłącznie do zasobów niezbędnych do realizacji powierzonych obowiązków;

11) zobowiązani są do niezwłocznego informowania IOD o wszystkich zmianach przepisów, mających wpływ na sposób, cele lub zakres przetwarzania danych osobowych w podległej komórce organizacyjnej;

12) w procesie zarządzania zmianami organizacyjnymi lub technologicznymi mającymi wpływ na sposób, cele lub zakres przetwarzanych danych osobowych zobowiązani są do konsultacji nowych rozwiązań z IOD oraz AS w fazie projektowania;

13) zapewniają funkcjonowanie systemów informatycznych niepodlegających zasadom bezpieczeństwa LUW w ramach powierzonych komórek organizacyjnych zgodnie z dokumentacją opisującą zasady działania w/w systemów;

14) odpowiadają za dopełnienie obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych w przypadku, gdy występują w roli osoby wnioskującej o udzielanie zamówienia publicznego. Zasady realizacji zamówień publicznych regulują odrębne regulacje administratora danych.

## 5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do przestrzegania następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje

wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) ma obowiązek zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych *obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji*;

3) bierze udział w szkoleniach i zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych, postanowieniami niniejszej Polityki oraz SZBI;

4) stosuje określone przez ADO procedury i zasady mające na celu zgodne z prawem przetwarzanie danych;

5) korzysta z systemu informatycznego ADO w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

## V. Podstawowe standardy

### 1. Szkolenia w zakresie ochrony danych osobowych

IOD zakłada następujący plan szkoleń:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych;

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku znaczących zmian zasad lub procedur ochrony danych osobowych;

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

### 2. Projektowanie zmian

ADO uwzględnia konieczność oceny wpływu projektowanych zmian na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany.

## 3. Środki bezpieczeństwa

1) Środki ochrony danych dostosowuje się do skali ryzyka w oparciu o metodykę przyjętą w dokumentacji SZBI na podstawie:
   a. procesu szacowania ryzyka uwzględniającego czynności przetwarzania danych oraz kategorie czynności,
   b. oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   c. metod postępowania z ryzykiem.
2) ADO stosuje adekwatne standardy w celu zapewnienia bezpieczeństwa fizycznego i środowiskowego pomieszczeń LUW, w których przetwarzane są informacje oraz przechowywane są urządzenia je przetwarzające zgodnie z dokumentacją SZBI, m.in.: wydziela strefy bezpieczeństwa, reguluje zasady kontroli dostępu, zapewnia fizyczną ochronę obiektu, wdraża zasady minimalizacji ryzyka wynikającego z przyczyn środowiskowych, ustala wymagania bezpieczeństwa dla obszarów przetwarzania danych osobowych, wdraża zasady reglamentacji i zarządzania dostępem do danych.
3) ADO zapewnia poufność, integralność, dostępność systemów i usług przetwarzania oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego zgodnie z zasadami i procedurami przyjętymi w dokumentacji SZBI,
4) ADO zapewnia regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania zgodnie z zasadami i procedurami przyjętymi w dokumentacji SZBI,
5) ADO weryfikuje podmioty przetwarzające dane na jego rzecz, w zakresie możliwości zapewnienia adekwatnego poziomu bezpieczeństwa oraz zapewnia odpowiednie mechanizmy kontroli w/w podmiotów.
6) ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu (Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych – załącznik Nr 1).

## 4. Inwentaryzacja danych i prowadzone rejestry

1) Przetwarzane przez ADO dane osobowe powinny być poddawane przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zwrócić się do ADO o zarządzenie dodatkowej inwentaryzacji:

   a. inwentaryzację przetwarzanych danych osobowych przeprowadza się uwzględniając wszystkie zidentyfikowane czynności przetwarzania przynajmniej pod kątem czynności, celów przetwarzania, kategorii osób, kategorii danych, podstaw prawnych przetwarzania, sposobów zbierania danych, kategorii odbiorców danych, przekazywania poza EU/EOG lub do organizacji międzynarodowych, środków technicznych i organizacyjnych ochrony danych, weryfikacji podstaw prawnych przetwarzania;

   b. IOD może zarządzić przeprowadzenie dodatkowej inwentaryzacji w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

2) Rejestr czynności przetwarzania oraz rejestr kategorii przetwarzania zawierają informacje, o których mowa w art. 30 RODO i służą monitorowaniu przez ADO czynności, celów przetwarzania, kategorii osób, kategorii danych, podstaw prawnych przetwarzania, sposobów zbierania danych, kategorii odbiorców danych, przekazywania poza EU/EOG, środków technicznych i organizacyjnych ochrony danych.

3) Administrator danych wdraża:
   a. zasady zarządzania adekwatnością (zakresem) danych,
   b. zasady zarządzania okresem przechowywania danych.

## 5. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia.

## VI. Przeglądy Polityki

1) Polityka bezpieczeństwa danych osobowych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD informacji może zwrócić się do ADO o zarządzenie przeglądu polityki bezpieczeństwa stosownie do potrzeb.
2) IOD analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
    a. zmian w systemach informatycznych administratora danych,
    b. zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
    c. zmian w obowiązującym prawie.
3) IOD po uzgodnieniu z ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z AS. Zakres, przebieg i rezultaty audytu są dokumentowane.

## VII. Postanowienia końcowe

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem w zakresie koniecznym do wykonywanych obowiązków oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2) W zakresie nieuregulowanym niniejszą Polityką stosuje się zasady określone w Systemie Zarządzania Bezpieczeństwem Informacji Lubuskiego Urzędu Wojewódzkiego (SZBI).

LUBUSKI
URZĄD WOJEWÓDZKI

**Załącznik nr 1**
**do Polityki bezpieczeństwa**
**danych osobowych**

# INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

## I. Istota naruszenia danych osobowych

§ 1.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   a. nieautoryzowany dostęp do danych;
   b. nieautoryzowane modyfikacje lub zniszczenie danych;
   c. udostępnienie danych nieautoryzowanym podmiotom;
   d. nielegalne ujawnienie danych;
   e. pozyskiwanie danych z nielegalnych źródeł.

## II. Postępowanie w przypadku naruszenia danych osobowych

§ 2.

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to (najpóźniej w terminie 8 godzin od stwierdzenia zaistnienia zdarzenia) Inspektorowi Ochrony Danych, zwanemu dalej „IOD", który informuje o tym fakcie administratora danych.
2. Procesor (podmiot zajmującym się przetwarzaniem danych osobowych, które powierzył mu administrator), który w imieniu administratora danych stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie najpóźniej w terminie 24 godzin zgłosić ten fakt administratorowi danych lub IOD. W tym zakresie zobowiązany jest:
   a. poinformować o tym Powierzającego - Administratora Danych, podając wszelkie informacje dotyczące takiego naruszenia;
   b. ustalić przyczynę naruszenia;
   c. podjąć wszelkie czynności mające na celu usunięcie naruszenia i zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami;
   d. zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości.

§ 3.

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 4.

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub innej osoby upoważnionej przez administratora danych.

§ 5.

IOD podejmuje następujące kroki:

a. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
b. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
c. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 6.

IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając notatkę dla ADO. Dokumentacja gromadzona przez IOD stanowi rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO.

§ 7.

IOD zasięga potrzebnych mu opinii i proponuje działania naprawcze takie jak:

a. wyłączenie systemu, co w poszczególnych przypadkach powinno być poprzedzone uzgodnieniem tego z właścicielem procesu przetwarzanych danych oraz z osobą odpowiedzialną za systemy teleinformatyczne;
b. pozostawienie działającego systemu;
c. uruchomienie procedur odtwarzania z kopii zapasowych, procedur planu zapewniania ciągłości działania oraz podjęcie działań wynikających z instrukcji zarządzania poszczególnych systemów;
d. zapewnianie bezpiecznego przechowywania śladów i dowodów (także w wersji elektronicznej), szczególnie w przypadku gdy niezbędne jest przeprowadzenie postępowania wyjaśniającego;

## III. Naruszenie danych osobowych – odpowiedzialność

§ 8.

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, stosuje się kary dyscyplinarne.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami.

2. Odpowiedzialność Procesora określona jest w umowie powierzenia przetwarzania danych.

## IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 9.

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu zweryfikować naruszenie.

3. Administrator informuje organ w sytuacji:

a. kradzieży tożsamości;
b. straty finansowej;
c. naruszenia poufności danych chronionych tajemnicą zawodową;
d. utraty przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
e. ujawnienia danych z art. 9 lub 10 RODO.

## V. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 10.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych powinno:

a. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Zawiadomienie nie jest wymagane, w następujących przypadkach:
   a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

## VI. Postanowienia końcowe

§ 11.

1. Instrukcja powyższa używana jest w przypadku naruszenia ochrony danych osobowych
2. Instrukcja zarządzania incydentami jest przeznaczona dla wszystkich pracowników Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp., osób świadczących usługi na rzecz Urzędu, procesorów, stażystów i praktykantów.

Załącznik nr 2

Minimalne wymagania w zakresie pól informacyjnych zwartych w upoważnieniu

Gorzów Wielkopolski., dnia.....

**UPOWAŻNIENIE NR ……**
**DO PRZETWARZANIA DANYCH OSOBOWYCH**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 – dalej RODO) (Dz.Urz. UE L 119, s. 1)

**Upoważniam**

**Pana/(ą)** .....

Zatrudnionego/(ą) na stanowisku/
(lub proszę wpisać inną podstawę stosunku cywilnoprawnego) .....

w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim do przetwarzania danych osobowych w celu/celach:

……

Wyżej wymieniona osoba dopuszczona jest do przetwarzania danych osobowych jedynie w zakresie określonym w upoważnieniu.

Niniejsze upoważnienie wydaje się na czas trwania stosunku pracy, stosunku cywilnoprawnego bądź odwołania.

……
podpis Administratora Danych

Załącznik Nr 3

Wzór

**EWIDENCJA OSÓB UPRAWNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ EWIDENCJA OŚWIADCZEŃ O ZACHOWANIU W TAJEMNICY DANYCH OSOBOWYCH OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH**

| Lp. | Imię | Nazwisko | Stanowisko | Data nadania upoważnienia | Data ustania upoważnienia | Data podpisania oświadczenia | Zakres upoważnienia do przetwarzania danych osobowych | Identyfikator użytkownika (jeżeli dane są przetwarzane w systemie informatycznym) | Uwagi (nr dokumentu) |
|---|---|---|---|---|---|---|---|---|---|
| 1. | | | | | | | | | |
| 2. | | | | | | | | | |
| 3. | | | | | | | | | |
| … | | | | | | | | | |

Załącznik Nr 4

Wzór

**OŚWIADCZENIE**

1. Ja niżej podpisany (a) ……. zobowiązuję się do zachowania w tajemnicy wszelkich informacji w tym również danych osobowych, do których mam dostęp w związku z wykonywaniem przeze mnie zadań, usług lub obowiązków w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim zarówno w trakcie obecnie wiążącego mnie stosunku pracy lub innego rodzaju umowy jak i po zakończeniu powyższych relacji.
2. Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał(a) powierzonych danych osobowych.
3. Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu w art. 4 pkt 1 RODO.
4. Stwierdzam, że jest mi znana Polityka Bezpieczeństwa Danych Osobowych obowiązująca w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim.
5. Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych.

……
Data i podpis osoby upoważnionej

LUBUSKI
URZĄD WOJEWÓDZKI

**Załącznik nr 5**
**do Polityki bezpieczeństwa**
**danych osobowych**

# ZASADY REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

---

wersja 1.0

# HISTORIA ZMIAN

| Nr wersji | Data | Opis | Działanie (*) | Rozdziały(**) | Autorzy |
|---|---|---|---|---|---|
| 1.0 | | Utworzenie nowego dokumentu | N | W | P. Pikuła. |
| | | | W | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja

(**) Rozdziały: numery rozdziałów lub W-Wszystkie

## Spis treści

# 1. WPROWADZENIE

Niniejszy dokument zawiera opis zasad i procedur stosowanych przez pracowników Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wielkopolskim (LUW), w celu zapewnienia realizacji praw osób, których dane dotyczą oraz realizacji obowiązków Wojewody Lubuskiego względem tych osób zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. 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) oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000)

# 2. POSTANOWIENIA OGÓLNE

## 2.1.Podstawowe zasady przetwarzania danych osobowych

Wszyscy pracownicy Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wielkopolskim są zobowiązani do przestrzegania następujących zasad postępowania z danymi osobowymi:

a) przetwarzanie danych musi być zgodne z prawem, oznacza to w szczególności, że przetwarzanie odbywa się:
   - ✓ w związku z wypełnianiem obowiązku prawnego nałożonego na ,
   - ✓ w celu zawarcia i wykonania umowy, której stroną jest osoba, której dane dotyczą,
   - ✓ w związku z wykonywaniem zadania realizowanego w interesie publicznym, np. w przypadku realizacji prawa dostępu do informacji publicznej,
   - ✓ na podstawie zgody wyrażonej przez osobę, której dane dotyczą. Zgoda jednak jest tą przesłanką legalizującą przetwarzanie, która może zostać wykorzystana tylko w szczególnych przypadkach przewidzianych prawem lub w sytuacjach gdy przetwarzanie jest wymagane dla prawidłowej realizacji zadania LUW, a żadna z ww. podstaw nie ma zastosowania. W przypadku zgody musi być ona wyrażona w sposób wyraźny Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę. Wzór klauzuli zgody zawiera ***załącznik nr 1*** do niniejszych zasad;

b) przetwarzanie winno być rzetelne i odbywać się w sposób przejrzysty dla osoby, której dane dotyczą. Zasada ta oznacza, że osoba, której dane dotyczą jest informowana o operacji przetwarzania i jej celach, a realizowana jest w szczególności poprzez obowiązki i uprawnienia informacyjne opisane w punktach 3.1.1., 3.1.2. i 3.2.1. niniejszych zasad;

c) dane osobowe są zbierane tylko i wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie zostają przetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie tych danych do celów archiwalnych w interesie publicznym, do

celów badań naukowych lub historycznych oraz do celów statystycznych jest uznawane za zgodne z pierwotnymi celami;

d) dane, które są pozyskiwane i dalej przetwarzane muszą być adekwatne, tj. stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celów, w których są przetwarzane. Zasada ta oznacza między innymi minimalizację ilości zbieranych informacji;

e) należy zapewnić aby dane były prawidłowe i w razie potrzeby uaktualniane. Ponadto należy podjąć wszelkie działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Zasada ta realizuje się w szczególności poprzez prawo do sprostowania danych, prawo do usunięcia danych oraz prawo dostępu do danych, które to prawa zostały szerzej omówione w punktach: 3.2.1., 3.2.2.oraz 3.2.3.niniejszych zasad;

f) dane winny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, w których są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Każdy pracownik LUW jest zobowiązany do niezwłocznego przekazania dokumentów do archiwum zakładowego zgodnie z Rozporządzeniem Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. Dane archiwizowane powinny podlegać okresowemu przeglądowi, przynajmniej raz na rok pod kątem niezbędności ich przechowywania, a po zakończeniu okresu archiwizacji powinny być niezwłocznie usunięte z zachowaniem stosownych procedur;

g) dane winny być przetwarzane w sposób zapewniający ich integralność i poufność. Każdy pracownik odpowiada za właściwe zabezpieczenie danych osobowych, które przetwarza, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem zgodnie z zasadami obowiązującymi w LUW.

### 2.2. Zasady realizacji praw osób

Przy realizacji praw osób, których dane dotyczą należy zapewnić aby:

a) wszelkie przekazywane informacje były sformułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, dostosowanym do możliwości percepcyjnych odbiorcy;

b) informacji udzielano na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. W szczególnych przypadkach, jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą (np. poprzez uzyskanie wglądu do dowodu osobistego);

c) informacji, poza obowiązkami informacyjnymi, udzielono niezwłocznie, jednak nie później niż w terminie miesiąca od otrzymania żądania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim przypadku jednak w terminie miesiąca od otrzymania żądania informuje się osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeżeli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba ta zażąda innej formy. Wzór odpowiedzi dotyczącej wydłużenia terminu stanowi ***załącznik nr 2*** do niniejszej procedury;

d) jeżeli nie podejmie się działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania, należy poinformować ją o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem;

e) wszelkie informacje oraz komunikacja i działania podejmowane w związku z realizacją praw osób są wolne od opłat. Jeżeli jednak można wykazać i udokumentować iż żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, można pobrać ustalaną indywidualnie opłatę za udzielenie informacji albo odmówić podjęcia działań w związku z żądaniem.

f) w przypadku praw realizowanych na wniosek osoby, której dane dotyczą, jeżeli istnieją uzasadnione wątpliwości co do tożsamości tej osoby fizycznej składającej żądanie można wymagać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby;

g) gdy można wykazać, że nie jest się w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje się ją o tym. W takich przypadkach prawo, o którego realizację ta osoba występuje nie ma zastosowania, chyba że w celu wykonania prawa dostarczy dodatkowych informacji pozwalających ją zidentyfikować.

## 3. PROCEDURY REALIZACJI PRAW OSÓB

## 3.1. Obowiązki informacyjne

### 3.1.1. Prawo do bycia poinformowanym o przetwarzaniu danych przy zbieraniu danych od osoby, której dane dotyczą

1. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą podczas pozyskiwania tych danych podaje się następujące informacje:
   a) tożsamość i dane kontaktowe administratora;
   b) dane kontaktowe inspektora ochrony danych;
   c) cele w jakich dokonuje się przetwarzania oraz podstawę prawną tego przetwarzania;
   d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   e) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony. W przypadku przekazania danych z zastrzeżeniem odpowiednich zabezpieczeń, w tym wiążących reguł korporacyjnych lub na podstawie zgody wyrażonej przez osobę, której dane dotyczą albo gdy przekazanie jest niezbędne informuje się osobę o odpowiednich lub właściwych zabezpieczeniach. Dodatkowo przekazuje się jej informację o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
   f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   g) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   h) jeżeli przetwarzanie, zarówno w przypadku danych zwykłych jak i szczególnych kategorii danych, odbywa się na podstawie zgody podaje się informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   i) informację o prawie wniesienia skargi do organu nadzorczego;
   j) informację, 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;
   k) gdy ma to zastosowanie – informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, podaje się istotne informacje o zasadach ich podejmowania, a

także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje się osobę, której dane dotyczą, o tym innym celu oraz udziela się jej wszelkich innych stosownych informacji, o których mowa w ust. 1 lit. f) – k).
3. Ust. 1 i 2 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.
4. Obowiązek informacyjny realizują pracownicy komórek organizacyjnych LUW w momencie zbierania danych, zgodnie ze wzorem stanowiącym ***załącznik nr 3*** do niniejszych zasad.
5. Informacje, o których mowa powyżej mogą zostać przekazane na piśmie, w tym elektronicznie, a w szczególnych przypadkach mogą zostać odczytane.

### 3.1.2. Prawo do bycia poinformowanym o przetwarzaniu danych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1. W przypadku zbierania danych nie bezpośrednio od osoby, której dane dotyczą, podaje się następujące informacje:
   a) tożsamość i dane kontaktowe administratora;
   b) dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną ich przetwarzania;
   d) kategorie przetwarzanych danych osobowych;
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony. W przypadku przekazania danych z zastrzeżeniem odpowiednich zabezpieczeń, w tym wiążących reguł korporacyjnych lub na podstawie zgody wyrażonej przez osobę, której dane dotyczą albo gdy przekazanie jest niezbędne informuje się o odpowiednich lub właściwych zabezpieczeniach. Dodatkowo przekazuje się informację o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;

g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

h) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) jeżeli przetwarzanie, dotyczące zarówno danych zwykłych jak i szczególnych kategorii danych, odbywa się na podstawie zgody podaje się informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.;

j) informacje o prawie wniesienia skargi do organu nadzorczego;

k) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotne informacje o zasadach ich podejmowania, a także informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Informacje, o których mowa w ust. 1, podaje się najpóźniej w ciągu miesiąca, szczególnie:
   a) w rozsądnym terminie po pozyskaniu danych osobowych, mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
   b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z tą osobą; lub
   c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
3. Jeżeli planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje się osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 1 lit. f)–l).
4. Ust. 1– 3 nie mają zastosowania, gdy – i w zakresie, w jakim:
   a) osoba, której dane dotyczą, dysponuje już tymi informacjami;
   b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń odpowiednich dla tych danych, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego punktu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W

takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

c) gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem krajowym przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą

d) gdy dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

5. Obowiązek informacyjny realizują pracownicy komórek organizacyjnych LUW zgodnie ze wzorem stanowiącym ***załącznik nr 4*** do niniejszych zasad.
6. Informacje, o których mowa powyżej mogą zostać przekazane na piśmie, w tym elektronicznie, a w szczególnych przypadkach mogą zostać odczytane.

## 3.2. Prawa realizowane na wniosek

### 3.2.1. Prawo dostępu przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:
   a) w jakim celu są przetwarzane jej dane osobowe;
   b) jakich kategorii danych osobowych dotyczy przetwarzanie;
   c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
   e) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) o prawie wniesienia skargi do organu nadzorczego;
   g) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.
3. Jeżeli osoba, której dane dotyczą zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ta osoba, można pobrać opłatę zgodnie z obowiązującymi w LUW zasadami. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.
4. Kopię danych, o której mowa w ust. 3 wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do pliku. Nie wydaje się skanów dokumentów, ani ich kserokopii gdyż mogą zawierać dodatkowe dane nie dotyczące osoby występującej z wnioskiem.
5. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

### 3.2.2. Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
3. Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres LUW. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej zobowiązany jest dokonać weryfikacji przetwarzanych danych. W przypadku stwierdzenia konieczności wprowadzenia zmian informuje o tym bezpośredniego przełożonego. Następnie niezwłocznie dokonuje zmian, rejestrując ten fakt w aktach sprawy.
4. Prawo do sprostowania danych w trybie art. 16 RODO nie znajdzie zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy.

### 3.2.3. Prawo do usunięcia danych („prawo do bycia zapomnianym”)

1. 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) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zarówno danych zwykłych jak i szczególnych kategorii danych, a jednocześnie nie ma innej podstawy prawnej ich przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw, o którym mowa w punkcie 3.2.7.niniejszych zasad, wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy 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.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych 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.
3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
   a) do korzystania z prawa do wolności wypowiedzi i informacji;
   b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   c) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
   d) do ustalenia, dochodzenia lub obrony roszczeń.
4. W sytuacji gdy żądanie osoby, której dane dotyczą jest uzasadnione, a po stronie LUW nie ma podstaw prawnych odmowy realizacji żądania zgłasza się sprawę pracownikowi prowadzącemu archiwum zakładowe w celu dokonania usunięcia danych zgodnie z przepisami w zakresie brakowania dokumentacji niearchiwalnej zgodnie z kategorią archiwalną. Postępowanie dotyczy zarówno danych przetwarzanych w formie tradycyjnej jak i elektronicznej.

5. Dokumentacja z procedury brakowania dokumentacji niearchiwalnej jest przechowywana przez archiwum zakładowe.

### 3.2.4. Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.
2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce 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.
3. Do ograniczenia może dojść w następujących przypadkach:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych. W tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość 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, wobec przetwarzania wniosła sprzeciw, o którym mowa w punkcie 3.9. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.
4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każda osoba, która jest upoważniona do przetwarzania tych danych była świadoma iż dane te można jedynie przechowywać.
5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

### 3.2.5. Prawo do powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

1. Po dokonaniu sprostowania, usunięcia danych osobowych lub ograniczenia przetwarzania informuje się o tym każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

2. Jeżeli osoba, której dane dotyczą, tego zażąda informuje się ją o odbiorcach określonych w ust.1.

### 3.2.6. Prawo do przenoszenia danych

1. Jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany osoba ta ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące. Dotyczy to danych, które osoba składająca żądanie wcześniej dostarczyła. Osoba ta ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wielkopolskim.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Lubuski Wojewódzki w Gorzowie Wielkopolskim bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe i osoba wykaże, iż administrator, któremu mają zostać dane przekazane akceptuje taki sposób pozyskania danych.
3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.
4. Wykonanie prawa, o którym mowa w ust. 1 niniejszego działu, pozostaje bez uszczerbku dla prawa do usunięcia danych.
5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

### 3.2.7. Prawo do sprzeciwu

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym, jakim jest między innymi dostęp do informacji publicznej, w tym umieszczanie danych w Biuletynie Informacji Publicznej, z przyczyn związanych z jej szczególną sytuacją, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw, wobec przetwarzania dotyczących jej danych osobowych.
2. Administratorowi nie wolno już przetwarzać danych osobowych względem, których wniesiono sprzeciw, 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.

3. Najpóźniej przy okazji pierwszego kontaktu z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa powyżej, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
4. W momencie złożenia sprzeciwu wobec przetwarzania LUW niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli LUW posiada podstawę prawną, o której mowa powyżej informuję osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku gdy uzasadniona jest przesłanka do zrealizowania żądania postępuje się zgodnie z zapisami punktu 3.2.3. podpunkt 4.
5. Jeżeli dane osobowe są przetwarzane do celów badań naukowych, celów historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

#### 3.2.8. Prawo do poinformowania o naruszeniach

1. W przypadku wystąpienia incydentów bezpieczeństwa, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, z pewnymi wyjątkami, bez zbędnej zwłoki zawiadamia się osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa powyżej, wykonywane jest jasnym i prostym językiem, zawiera informacje opisujące charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, opis możliwych konsekwencji naruszenia ochrony danych osobowych oraz opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

### 3.3. Inspektor Ochrony Danych

1. W Lubuskim Urzędzie Wojewódzkim w Gorzowie Wielkopolskim został wyznaczony Inspektor Ochrony Danych.
2. W celu ułatwienia kontaktu z inspektorem utworzony został adres iod@lubuskie.uw.gov.pl podany do publicznej wiadomości na stronie internetowej LUW, w Biuletynie Informacji Publicznej oraz w klauzulach informacyjnych, na który każda osoba fizyczna, której dane są w związku z działaniami LUW ma prawo się skontaktować i uzyskać informacje wynikające z realizacji swoich praw.

## 4. OBSŁUGA WNIOSKÓW

1. Każdy wniosek o realizację praw osób wpływający na adres: iod@lubuskie.uw.gov.pl, bezpośrednio do kancelarii lub na skrzynki mailowe pracowników LUW musi zostać rejestrowany w EZD i zgodnie z instrukcją kancelaryjną przekazywany do Kierownika Komórki Organizacyjnej celem zadekretowania.
2. Kierownik Komórki Organizacyjnej przekazuje wniosek do Inspektora Ochrony Danych, który koordynuje jego realizację poprzez przekazanie do właściwych komórek organizacyjnych, w celu ustalenia, gdzie znajdują się dane osobowe wnioskodawcy oraz uzgadnia sposób załatwienia sprawy.
3. Odpowiedź przygotowują pracownicy poszczególnych komórek organizacyjnych, merytorycznie odpowiedzialnych za przetwarzanie danych w przedmiotowej sprawie. Pracownik komórki organizacyjnej LUW odpowiada za poprawność danych i identyfikację wnioskodawcy oraz wskazanie podstawy prawnej na podstawie której przetwarzane są dane osobowe. Inspektor doradza w zakresie terminu realizacji wniosku i innych elementów, o których mowa w punkcie 2.2. procedury. Wzór odpowiedzi stanowi ***załącznik nr 5.***
4. W celu zapewnienia udostępnienia danych jedynie osobom, których dane dotyczą dopuszcza się trzy kanały komunikacji:
   - ✓ elektroniczny – z podpisem kwalifikowanym lub potwierdzony profilem zaufanym e-PUAP, jeśli wniosek wpłynie „zwykłym mailem" można zażądać ponownego złożenia wniosku w dopuszczonym trybie;
   - ✓ tradycyjny – w formie papierowej opatrzony własnoręcznym podpisem;
   - ✓ ustnie (nie dotyczy kontaktu telefonicznego) – należy taką osobę wylegitymować w celu potwierdzenia tożsamości i sporządzić notatkę z podpisem wnioskodawcy. Notatka winna być włączona w akta sprawy.
5. Po załatwieniu sprawy komórka organizacyjna przekazuje wniosek i odpowiedź w sprawie, do Inspektora Ochrony Danych.
6. Rejestr wszystkich wniosków prowadzi Inspektor Ochrony Danych.

## 5. UPRAWNIENIA PRACOWNIKÓW LUW

Pracownik jest uprawniony do:

1. zgłaszania sytuacji związanych z niewłaściwą realizacją zasad opisanych w niniejszym dokumencie;

2. zgłaszania rozwiązań pozwalających na usprawnienie realizacji praw osób, których dane dotyczą.

## 6. POSTANOWIENIA KOŃCOWE

1. Wszyscy pracownicy są zobowiązani do zapoznania się i przestrzegania zasad określonych w niniejszym dokumencie.
2. Procedury podlegają przeglądowi przynajmniej raz w roku.

Załączniki:

1. Wzory klauzul zgody
2. Wzór odpowiedzi dotyczącej wydłużenia terminu
3. Wzór informacji z art. 13 RODO
4. Wzór informacji z art. 14 RODO
5. Wzór odpowiedzi

Załącznik nr 1

## Klauzula zgody

☐ Wyrażam zgodę na przetwarzanie przez Wojewodę Lubuskiego w Gorzowie Wielkopolskim z siedzibą ul. Jagiellończyka 8, 66 – 400 Gorzów Wielkopolski moich danych osobowych zawartych w …….. w zakresie ..…….. w celu……

Jestem świadoma/y przysługującego mi prawa do wycofania zgody, jak również faktu, że wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Zgodę mogę odwołać poprzez wysłanie maila opatrzonego podpisem kwalifikowanym lub potwierdzony profilem zaufanym e-PUAP na adres iod@lubuskie.uw.gov.pl z informacją o jej odwołaniu, w treści maila wskażę swoje imię i nazwisko, a w tytule wiadomości wpiszę „LUW Gorzów Wielkopolski - odwołanie zgody" lub listownie na adres LUW.

Załącznik nr 2

## Wzór odpowiedzi dotyczącej wydłużenia terminu

Gorzów Wielkopolski, dnia ……

**Numer sprawy**: ……

**Data wpływu**: …….

**Dotyczy**: wydłużenia terminu realizacji prawa do ……..

**Pani/Pan**
**Imię i nazwisko**
**ul. Nazwa i numer**
**Kod i miejscowość**

W związku z upływającym w dniu …… terminem realizacji Pana prawa do …….. informuję, że powyższy termin zostaje przedłużony o miesiąc/ dwa miesiące, tj. do dnia ……..

Powyższe opóźnienie spowodowane jest …….

| | |
|---|---|
| **Podstawa prawna** | Art. 12 ust.3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. 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) |

Załącznik nr 3

**Wzór informacji z art. 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą (przed wykorzystaniem należy każdorazowo zweryfikować zapisy)**

1. Administratorem Twoich danych osobowych jest Wojewoda Lubuski. Siedzibą Wojewody Lubuskiego jest Lubuski Wojewódzki w Gorzowie Wielkopolskim ul. Jagiellończyka 8, 66-400 Gorzów Wielkopolski. Kontakt jest możliwy za pomocą telefonu: +48 95 7 115 600 ; adresu e-mail: urzad.wojewodzki@lubuskie.uw.gov.pl; skrytki ePUAP: /43emu4tg7l/skrytka.
2. W sprawach związanych z danymi osobowymi kontaktuj się z Inspektorem ochrony danych poprzez adres e-mail: iod@lubuskie.uw.gov.pl, za pomocą telefonu: +48 95 7 115 600 lub pod adresem wskazanym w pkt. 1
3. Twoje dane osobowe przetwarzane będą w celu realizacji:
   - wypełniania obowiązku prawnego ciążącego na Administratorze w związku z realizowaniem zadań przez Wojewodę Lubuskiego na podstawie art. 6 ust. 1 lit. c Rozporządzenia;
   - wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z realizowaniem zadań przez Wojewodę Lubuskiego na podstawie art. 6 ust. 1 lit. e Rozporządzenia;
   - inny (proszę wskazać jaki).
4. W związku z przetwarzaniem danych w celu wskazanym powyżej, Twoje dane osobowe mogą być udostępniane innym odbiorcom lub kategoriom odbiorców. Odbiorcami danych mogą być:
   - podmioty upoważnione do odbioru Twoich danych osobowych na podstawie odpowiednich przepisów prawa;
   - podmioty, które przetwarzają Twoje dane osobowe w imieniu Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. podmioty przetwarzające).
5. Twoje dane osobowe będą przetwarzana przez okres niezbędny do realizacji wskazanego w pkt 3 celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z przepisów prawa.
6. W związku z przetwarzaniem przez Administratora danych osobowych przysługuje Ci:
   prawo dostępu do treści danych, na podstawie art. 15 Rozporządzenia;
   prawo do sprostowania danych, na podstawie art. 16 Rozporządzenia;
   prawo do usunięcia danych, na podstawie art. 17 Rozporządzenia;
   prawo do ograniczenia przetwarzania danych, na podstawie art. 18 Rozporządzenia;
   prawo wniesienia sprzeciwu wobec przetwarzania danych, na podstawie art. 21 Rozporządzenia.

7. W przypadku, w którym przetwarzanie Twoich danych odbywa się na podstawie zgody (tj. art. 6 ust. 1 lit. a Rozporządzenia), przysługuje Ci prawo do cofnięcia jej w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. Masz prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, gdy uznasz, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia.
9. Podanie przez Ciebie danych osobowych jest warunkiem prowadzenia sprawy przez Wojewodę Lubuskiego. Przy czym podanie danych jest:
   - obowiązkowe, jeżeli tak zostało to określone w przepisach prawa;
   - dobrowolne, jeżeli odbywa się na podstawie Twojej zgody lub ma na celu zawarcie umowy. Konsekwencją niepodania danych będzie brak możliwość realizacji czynności urzędowych lub nie zawarcie umowy.
10. Twoje dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

(Uwaga: realizacja powyższych praw musi być zgodna z przepisami prawa, na podstawie których odbywa się przetwarzanie danych oraz z zasadami archiwizacji).

Załącznik nr 4

## Wzór informacji z art. 14- Informacje podawane w przypadku pozyskania danych osobowych w sposób inny niż od osoby, której dane dotyczą (przed wykorzystaniem należy każdorazowo zweryfikować zapisy)

1. Administratorem Twoich danych osobowych jest Wojewoda Lubuski. Siedzibą Wojewody Lubuskiego jest Lubuski Wojewódzki w Gorzowie Wielkopolskim ul. Jagiellończyka 8, 66 –400 Gorzów Wielkopolski. Kontakt jest możliwy za pomocą telefonu: +48 95 7 115 600 ; adresu e-mail: urzad.wojewodzki@lubuskie.uw.gov.pl; skrytki ePUAP: /43emu4tg7l/skrytka.
2. W sprawach związanych z danymi osobowymi kontaktuj się z Inspektorem ochrony danych poprzez adres e-mail: iod@lubuskie.uw.gov.pl, za pomocą telefonu: +48 95 7 115 600 lub pod adresem wskazanym w pkt. 1
3. Twoje dane osobowe przetwarzane będą w celu realizacji:
   - wypełniania obowiązku prawnego ciążącego na Administratorze w związku z realizowaniem zadań przez Wojewodę Lubuskiego na podstawie art. 6 ust. 1 lit. c Rozporządzenia;
   - wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z realizowaniem zadań przez Wojewodę Lubuskiego na podstawie art. 6 ust. 1 lit. e Rozporządzenia.
4. Przetwarzanie danych osobowych obejmuje następujące kategorie Twoich danych: (należy wypisać kategorie np. imię i nazwisko, dane pracownicze, dane kontaktowe.)
5. W związku z przetwarzaniem danych w celu wskazanym powyżej, Twoje dane osobowe mogą być udostępniane innym odbiorcom lub kategoriom odbiorców. Odbiorcami danych mogą być:
   - podmioty upoważnione do odbioru Twoich danych osobowych na podstawie odpowiednich przepisów prawa;
   - podmioty, które przetwarzają Twoje dane osobowe w imieniu Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. podmioty przetwarzające).
6. Twoje dane osobowe będą przetwarzana przez okres niezbędny do realizacji wskazanego w pkt 3 celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z przepisów prawa.
7. W związku z przetwarzaniem przez Administratora danych osobowych przysługuje Ci:
   prawo dostępu do treści danych, na podstawie art. 15 Rozporządzenia;
   prawo do sprostowania danych, na podstawie art. 16 Rozporządzenia;
   prawo do usunięcia danych, na podstawie art. 17 Rozporządzenia;
   prawo do ograniczenia przetwarzania danych, na podstawie art. 18 Rozporządzenia;
   prawo wniesienia sprzeciwu wobec przetwarzania danych, na podstawie art. 21 Rozporządzenia
8. W przypadku, w którym przetwarzanie Twoich danych odbywa się na podstawie zgody (tj. art. 6 ust. 1 lit. a Rozporządzenia), przysługuje Ci prawo do cofnięcia jej w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

9. Masz prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, gdy uznasz, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia.
10. Twoje dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.
11. Twoje dane zostały uzyskane od ……. (należy podać dane administratora).

(Uwaga: realizacja powyższych praw musi być zgodna z przepisami prawa, na podstawie których odbywa się przetwarzanie danych oraz z zasadami archiwizacji).

Załącznik nr 5

# Wzór odpowiedzi na wniosek

Gorzów Wielkopolski, dnia ……

**Numer sprawy**: ……

**Data wpływu**: …….

**Dotyczy**: realizacji prawa do ……..

**Pani/Pan**
**Imię i nazwisko**
**ul. Nazwa i numer**
**Kod i miejscowość**

Informuję, iż Wojewoda Lubuski przetwarza (nie przetwarza) Pani/Pana dane osobowe w zakresie …… zgromadzone w ramach …… / dokonał/ nie dokonał[1] sprostowania/ usunięcia/ ograniczenia przetwarzania danych, o które Pani/Pan wnioskowała/wnioskował zrealizował/ nie zrealizował prawo do sprzeciwu w zakresie ……..

[2]Powyższa decyzja wynika z ……

**Podstawa prawna** Art. 15-22[3] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. 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)

[1] Niewłaściwe skreślić
[2] W przypadku odmowy realizacji prawa
[3] Wskazać odpowiednio

**Załącznik nr 6**
**do Polityki bezpieczeństwa**
**danych osobowych**

# METODYKA OCENY RYZYKA PRZY NARUSZENIACH OCHRONY DANYCH OSOBOWYCH

---

*Opracowano w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) dotyczące metod oceny wagi naruszenia (https://www.enisa.europa.eu/publications/dbn-severity)*

## I. OBOWIĄZEK NOTYFIKACJI NARUSZEŃ:

Art. 4 RODO definiuje **naruszenie ochrony danych osobowych** jako: „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"

Obowiązek notyfikacji naruszeń wynika z art. 33 i 34 RODO

- Art. 33 RODO:

„1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia."

- Motyw 85 RODO:

„Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub 4.5.2016 L 119/16 Dziennik Urzędowy Unii Europejskiej PL społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych **administrator powinien zgłosić je organowi nadzorczemu** bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, **chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych**. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki."

- Art. 34 RODO:

„1. Jeżeli naruszenie ochrony danych osobowych **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu."

- Motyw 86 RODO:

„Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, **jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie**

**niezbędnych działań zapobiegawczych**. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie."

## I. RYZYKO JAKO POWÓD NOTYFIKACJI

Znajomość prawdopodobieństwa i potencjalnej dotkliwości wpływu na osoby fizyczne:

1/ pomoże administratorowi w podjęciu skutecznych działań pozwalających zapanować nad skutkami naruszenia i je zminimalizować;

2/ pomoże administratorowi stwierdzić, czy zgłoszenie naruszenia organowi nadzorczemu oraz – w stosownych przypadkach – osobom, których dotyczy naruszenie, jest konieczne.

Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

## II. CZYNNIKI RYZYKA

1. Rodzaj naruszenia (poufność, dostępność i integralność).
2. Charakter: wrażliwość i ilość danych osobowych.
3. Łatwość identyfikacji osób fizycznych.
4. Waga konsekwencji dla osób fizycznych.
5. Cechy szczególne administratora danych.
6. Liczba osób fizycznych, na które naruszenie wywiera wpływ.

## III. KRYTERIA OCENY WAGI NARUSZENIA

Głównymi kryteriami oceny wagi naruszenia (**SE** – Severity Assessment) są:

1. Kontekst przetwarzania danych (**DPC** – Data Processing Context) – rodzaj i poziom wrażliwości danych w określonym kontekście przetwarzania.
2. Łatwość identyfikacji (**EI** – EASE of Identification) – łatwość identyfikacji osoby na podstawie danych, których dotyczy naruszenie (dla osoby, która uzyska dostęp do danych).
3. Okoliczności naruszenia (**CB** – Circumstances of breach) – specyficzne okoliczności naruszenia.

**SE = DPC x EI + CB**

/każdy z czynników podlega wycenie;
DPC – kontekst przetwarzania danych to czynnik bazowy, który określa poziom krytyczności zestawu danych, którego dotyczy naruszenie, w określonym kontekście przetwarzania;
EI – łatwość identyfikacji to czynnik korygujący, który może obniżyć wynik; im mniejsza łatwość identyfikacji osoby tym niższa wartość; iloczyn DPC i EI daje wstępny wynik oceny istotności naruszenia (SE);
CB – okoliczności naruszenia to czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku/

**DPC – kontekst przetwarzania danych (A + B)**

A) rodzaj i poziom wrażliwości danych osobowych
- dane z art. 6 (+5)
- dane z art. 9 i/lub 10 (+10)

B) specyficzne czynniki przetwarzania, które mogą podnieść lub obniżyć wycenę
- szeroki zakres danych odnoszący się do osoby (+2)
- charakter danych (+2)
- specyfika administratora/komórki organizacyjnej, w której miało miejsce naruszenie (+1)

**EI – łatwość identyfikacji osoby**
- znikoma możliwość identyfikacji (x1)
- ograniczona możliwość identyfikacji (x2)
- wysokie prawdopodobieństwo identyfikacji (x3)
- pewna identyfikacja (x4)

**CB – okoliczności naruszenia (A + B + C)**

A) naruszenie poufności danych
- dane ujawnione znanym odbiorcom danych (+1)
- dane ujawnione nieznanej liczbie odbiorców danych (+5)

(B) naruszenie integralności danych oraz naruszenie dostępności danych
- dane zmienione i użyte, ale jest możliwe ich odzyskanie lub czasowa niedostępność danych (+1)
- dane zmienione, użyte oraz brak możliwości ich odzyskania lub pełna niedostępność danych i brak możliwości ich odzyskania (+5)

(C) intencjonalność i skala
- intencjonalnie działanie sprawcy (+5)
- duża skala osób dotkniętych naruszeniem (+5)

## IV. OCENA WAGI NARUSZENIA

| Wynik | Waga naruszenia | Opis |
|---|---|---|
| SE < 20 | Niska | Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności |
| 21 ≤ SE <60 | Średnia | Osoby mogą napotkać niedogodności, możliwe do pokonania |
| 61 ≤ SE < 80 | Wysoka | Mogą wystąpić konsekwencje, możliwe do pokonania, ale z poważnymi trudnościami |
| 81 ≤ SE | Bardzo wysoka | Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje |

## V. POSTĘPOWANIE PO OCENIE

Ocena wagi naruszenia powinna stanowić integralną część notatki dotyczącej naruszenia, przekazywanej do administratora danych.

Naruszenie ocenione na poziomie niskim oraz średnim nie podlega notyfikacji do organu nadzorczego. Pozostałe naruszenia podlegają notyfikacji do organu nadzorczego, a naruszenia na poziomie bardzo wysokim podlegają powiadomieniu osób, których naruszenie ochrony danych dotyczy, zgodnie z obowiązującymi przepisami o ochronie danych osobowych.