


# POLITYKA OCHRONY DANYCH OSOBOWYCH

Starostwo Powiatowe w Żyrardowie

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Starostwo Powiatowe w Żyrardowie
Wersja:	Nr 1
z dnia:	
Zatwierdził(a):	<div>WICESTAROSTA</div> <div> Krzysztof Dziwisz</div>

## SPIS TREŚCI

1. INFORMACJE OGÓLNE .....	4
1.1. Definicje .....	4
1.2. Administrator Danych .....	6
1.3. Cel systemu ochrony danych osobowych .....	6
1.4. Zakres systemu ochrony danych osobowych.....	6
2. ROLE I ODPOWIEDZIALNOŚCI .....	7
2.1. Role w systemie ochrony danych osobowych .....	7
2.2. Odpowiedzialność.....	7
3. IDENTYFIKACJA PRZETWARZANYCH DANYCH OSOBOWYCH.....	9
3.1. Identyfikacja danych osobowych.....	9
3.2. Rejestr czynności przetwarzania danych osobowych.....	9
4. ZASADY PRZETWARZANIA DANYCH .....	10
4.1. Ogólne zasady dotyczące przetwarzania danych osobowych .....	10
4.2. Szczegółowe zasady przetwarzania danych osobowych .....	10
4.2.3. Dokładność i aktualność danych osobowych .....	11
4.2.4. Czasowe przetwarzanie danych osobowych .....	12
4.2.5. Zasady dotyczące profilowania.....	12
4.2.6. Przetwarzanie danych szczególnych.....	12
4.2.7. Zasady udostępnienia i powierzania danych osobowych.....	13
4.2.8. Zasady transgraniczności i przetwarzania w państwie trzecim .....	14
4.2.9. Zasady analizy podmiotów przetwarzających .....	14
5. ANALIZA RYZYKA I OCENA SKUTKÓW .....	15
5.1. Analiza ryzyka .....	15
5.2. Ocena skutków .....	15
6. ŚRODKI ZAPEWNIAJĄCE BEZPIECZEŃSTWO DANYCH.....	16
6.1. Środki fizyczne .....	16
6.2. Środki organizacyjne .....	16
6.2.1. Zasady upoważniania osób do przetwarzania danych osobowych .....	16
6.2.2. Rejestr osób upoważnionych do przetwarzania danych osobowych .....	17
6.2.3. Szkolenia .....	17
6.2.4. Audyt wewnętrzny.....	17
6.2.5. Przegląd systemu ochrony danych osobowych .....	18

6.3.	Środki techniczne.....	18
6.3.1.	Rejestr systemów teleinformatycznych w których przetwarzane są dane osobowe.....	18
6.3.2.	Zasady ochrony danych osobowych przetwarzanych w systemach informatycznych....	18
7.	OCHRONA DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA.....	19
7.1.	Zasady ochrony danych w fazie projektowania (Privercy by design) .....	19
7.2.	Zasada domyślnej ochrony danych (Privercy by default) .....	19
8.	PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ .....	20
8.1.	Zasady ogólne .....	20
8.2.	Identyfikacja zgłaszającego.....	20
8.3.	Rejestracja zgłoszenia .....	21
8.4.	Opracowanie odpowiedzi .....	21
8.5.	Bezpieczeństwo przekazywanych odpowiedzi .....	21
9.	POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH .....	21
9.1.	Zasady ogólne dot. naruszenia ochrony danych osobowych .....	22
9.2.	Zasady komunikacji.....	22
9.3.	Zasady raportowania .....	22
10.	ODPOWIEDZIALNOŚĆ KARNA ZA NARUSZENIE OCHRONY DANYCH OSOBOWYCH.....	23
11.	WYKAZ ZAŁĄCZNIKÓW .....	23
12.	DOKUMENTY ZWIĄZANE.....	24

## 1. INFORMACJE OGÓLNE

### 1.1. Definicje

**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).

**Ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. poz. 1000).

**Dane osobowe** (zgodnie z art. 4 ust. 1 pkt 1 RODO) - 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 szczególne** (szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 2 RODO) – ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych dane genetyczne oraz dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

**Naruszenie ochrony danych osobowych** (zgodnie z art. 4 ust. 1 pkt 12 RODO) - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

**Odbiorca** (zgodnie z art. 4 ust. 1 pkt 9 RODO) – 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 Unii lub prawem państwa członkowskiego, 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.

**Organ nadzorczy** (zgodnie z art. 4 ust. 1 pkt 21 RODO) – Prezes Urzędu Ochrony Danych Osobowych.

**Osoba nieuprawniona** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe z naruszeniem przepisów o ochronie danych osobowych, lub poza wyraźnym uprawnionym poleceniem ADO.

**Osoba upoważniona** – osoba wykonująca zadania polegające na przetwarzaniu, w formie tradycyjnej lub elektronicznej, danych osobowych na wyraźne polecenie ADO i jest upoważniona do wykonywania tych czynności.

**Państwo trzecie** – państwo nienależące do Unii Europejskiej, a po uwzględnieniu RODO w Porozumieniu o Europejskim Obszarze Gospodarczym, państwo trzecie będzie oznaczało państwo spoza Europejskiego Obszaru Gospodarczego.

**Podmiot przetwarzający** (zgodnie z art. 4 ust. 1 pkt 8 RODO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

**Przetwarzanie** (zgodnie z art. 4 ust. 1 pkt 2 RODO) – 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.

**Strona trzecia** (zgodnie z art. 1 pkt 10 RODO) – oznacza 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.

**Usługi społeczeństwa informacyjnego** (zgodnie z art. 1 ust. 1 pkt 25 RODO) – każda usługa świadczona za wynagrodzeniem, na odległość, drogą elektroniczną, pozbawioną charakteru materialnego, realizowana na indywidualne żądanie usługobiorcy.

**Wyraźne polecenie administratora** – oznacza powierzenie zadań wymagających przetwarzania danych osobowych osobie fizycznej, niezależnie od formy prawnej, w szczególności poprzez zawarcie umowy o pracę, określenie zadań w ramach zakresu czynności lub dokumencie równoważnym, powierzenie pełnienia funkcji wraz z określeniem zadań lub zlecenie zadań w formie umowy cywilnoprawnej.

**Zbiór danych** (zgodnie z art. 4 ust. 1 pkt 6 RODO) – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

**Zgoda** (zgodnie z art. 4 ust. 1 pkt 11 RODO) – osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

**Dostępność danych** – rozumie się przez to właściwość zapewniającą, że dane są udostępniane osobie upoważnionej wtedy, gdy ich potrzebuje do przetwarzania.

**Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

**Poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom.

## 1.2. Administrator Danych

Administratorem danych osobowych jest Starostwo Powiatowe w Żyrardowie reprezentowane przez Starostę, który ustala cele i sposoby przetwarzania danych osobowych.

Administrator danych osobowych mając na uwadze jak ważne jest bezpieczeństwo przetwarzanych danych osobowych ze względu na ochronę podstawowych praw i wolności osób fizycznych, a w szczególności ich prawo do ochrony danych osobowych oraz w celu zapewnienia zgodności z wymaganiami prawa, a w tym ochronę dobrego imienia jednostki, ustanawia system ochrony danych osobowych.

Ramy ustanowionego systemu ochrony danych osobowych tworzy niniejsza polityka ochrony danych osobowych oraz powiązane z nią dokumenty.

Administrator danych osobowych deklaruje pełne zaangażowanie w dążeniu do spełnienia wymagań wynikających z 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) (zwanego dalej RODO), Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000) i wymagań kontraktowych w tym obszarze oraz ciągłe doskonalenie systemu ochrony danych osobowych.

## 1.3. Cel systemu ochrony danych osobowych

Celem niniejszego dokumentu jest określenie: (1) zasad przetwarzania danych osobowych zgodnych z przepisami prawa (2) i ochrony danych osobowych, przed udostępnieniem osobom nie upoważnionym, pozyskaniem przez osobę nieuprawnioną, zmianą, uszkodzeniem lub zniszczeniem (3) oraz obowiązków osób odpowiedzialnych za przetwarzanie danych osobowych jak i osób odpowiedzialnych za ich bezpieczeństwo.

Celem systemu ochrony danych osobowych jest spełnienie wymagań wynikających z RODO, Ustawy o ochronie danych osobowych oraz wymagań kontraktowych.

## 1.4. Zakres systemu ochrony danych osobowych

Zasady opisane w niniejszym dokumencie mają zastosowanie do wszystkich danych osobowych, niezależnie od ich pochodzenia, przetwarzanych u Administratora Danych, we wszystkich procesach w organizacji. Każdy pracownik i współpracownik musi się zapoznać z niniejszym dokumentem w zakresie jego obowiązków. Dla firm zewnętrznych oraz ich podwykonawców został opracowany wyciąg, który stanowi załącznik nr 1 do niniejszego dokumentu.

## 2. ROLA I ODPOWIEDZIALNOŚCI

### 2.1. Role w systemie ochrony danych osobowych

W systemie ochrony danych osobowych określono następujące role:

**Administrator danych osobowych (ADO)**, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi, ustala cele i sposoby przetwarzania danych osobowych.

**Inspektor ochrony danych (IOD)**, osoba powołana przez Administratora Danych Osobowych w celu nadzorowania procesu ochrony danych osobowych w organizacji, a w szczególności:

- informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i Ustawy o ochronie danych osobowych;
- monitorowanie przestrzegania rozporządzenia RODO oraz niniejszego dokumentu i regulacji powiązanych w zakresie ochrony danych osobowych;
- wsparcie procesu analizy ryzyka oraz oceny skutków dla ochrony danych, poprzez udzielanie zaleceń oraz późniejsze monitorowanie ich realizacji;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego pomiędzy zainteresowanymi stronami tj. organem nadzorczym oraz osobami, których dane dotyczą, w kwestiach związanych z przetwarzaniem danych osobowych.

**Administrator Systemów Informatycznych (ASI)**, pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych.

**Osoba dopuszczona do przetwarzania danych osobowych**, osoba, której nadano upoważnienie do przetwarzania danych osobowych zgodnie z art. 29 RODO.

### 2.2. Odpowiedzialność

Administrator danych osobowych jest odpowiedzialny za:

- Ustanowienie, wdrożenie i utrzymanie procesu ochrony danych osobowych, tak aby zapewnić zgodność z przepisami prawa w szczególności opisanych w art. 5 ust.1 RODO;
- Zapewnienie możliwości spełnienia obowiązków wynikających z przysługujących praw osobie, której dane dotyczą;
- Zapewnienie odpowiednich środków w celu przejrzystego informowania i przejrzystej komunikacji podczas wykonywania praw przez osobę, której dane dotyczą;
- Zapewnienie spełnienia obowiązku informacyjnego w stosunku do osoby, której dane osobowe przetwarza;

- Wdrożenie odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania;
- Zapewnienie prowadzenia odpowiednich rejestrów, w tym rejestru czynności przetwarzania;
- Wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego bezpieczeństwa określonego na podstawie analizy ryzyka, w tym między innymi w stosownym przypadku:
  - pseudonimizację i szyfrowanie danych osobowych,
  - zdolność co ciągłego zapewnienia poufności, integralności, dostępności i odporność systemów i usług przetwarzania,
  - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu (fizycznego lub technicznego),
  - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- Oraz wypełnienie obowiązków prawnych wynikających z RODO i Ustawy o ochronie danych osobowych.

Inspektor ochrony danych (IOD) ma następujące zadania:

- Zbieranie informacji w celu identyfikacji procesów przetwarzania;
- Analizowanie i sprawdzanie zgodności tego przetwarzania;
- Informowanie, doradzanie i rekomendowanie określonych działań ADO i/lub podmiotowi przetwarzającemu;
- Przeprowadzanie audytów wewnętrznych i opracowywanie raportów po audytowych wraz z rekomendacjami;
- Wsparcie procesu edukacyjnego w zakresie ochrony danych osobowych osób dopuszczonych do ich przetwarzania u ADO;
- Wsparcie w procesie wykrywania i analizy incydentów naruszeń bezpieczeństwa danych osobowych oraz zgłaszanie incydentów zgodnie z RODO do Urzędu Ochrony Danych Osobowych (dalej: UODO);
- Reprezentowanie Administratora danych osobowych przed Prezesem UODO podczas postępowań administracyjnych;
- Wsparcie procesu zarządzania ryzykiem oraz procesu oceny skutków przetwarzania danych osobowych;
- Opiniowanie zmian w systemach informatycznych, procesach biznesowych w obszarze prawidłowości oraz bezpieczeństwa przetwarzania danych osobowych;
- Opiniowanie umów powierzenia przetwarzania danych osobowych;
- Opracowanie corocznego raportu z przeglądu systemu ochrony danych osobowych i reprezentowanie go Administratorowi.

Osoba dopuszczona do przetwarzania danych osobowych jest odpowiedzialna za:

- Zapoznanie się z niniejszym dokumentem oraz jego przestrzeganie;



- Zachowanie w poufności przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia, nawet po zakończeniu współpracy;
- Wskazywanie obszarów do doskonalenia w systemie ochrony danych osobowych;
- Zgłaszanie wszelkich zauważonych lub potencjalnych naruszeń dotyczących bezpieczeństwa danych osobowych lub słabości systemu ochrony danych osobowych.

### 3. IDENTYFIKACJA PRZETWARZANYCH DANYCH OSOBOWYCH

#### 3.1. Identyfikacja danych osobowych

Podstawą systemu ochrony danych osobowych jest identyfikacja przetwarzanych danych osobowych. Administrator Danych zobowiązany jest przeprowadzić proces identyfikacji zakresu danych osobowych przetwarzanych w realizowanych przez niego procesach oraz określić, jakie operacje w zakresie przetwarzania danych osobowych są wykonywane.

Operacje przetwarzania danych osobowych to:

- **Zbieranie:** zebranie danych osobowych drogą elektroniczną lub tradycyjną lub bezpośrednio lub mieszane.
- **Utrwalanie:** wprowadzanie danych osobowych do systemów informatycznych lub dokumentacji papierowej.
- **Przechowywanie:** przetrzymywanie danych osobowych w postaci elektronicznej (systemy ICT, urządzenia mobilne, komputer, laptop itd.) lub przetrzymywanie w postaci papierowej (np. przechowywanie w szafach biurowych, szafach specjalnych, w szufladzie biurka itd.).
- **Opracowywanie:** wytwarzanie dokumentacji w postaci elektronicznej lub papierowej, w której dane osobowe są wykorzystywane ale nie są one zmieniane np. przygotowanie listy płac, lista umów ubezpieczenia z informacjami o osobach, których umowy dotyczą itd.
- **Zmienianie:** wprowadzanie zmian w danych osobowych niezależnie od postaci (papierowo lub/i elektronicznie).
- **Udostępnianie:** przekazywanie danych osobowych innym podmiotom na podstawie prawa lub zawartych umów powierzenia.
- **Usuwanie:** usuwanie trwale danych osobowych z systemów elektronicznych lub nośników tradycyjnych.

Na podstawie zebranych w procesie identyfikacji przetwarzanych danych osobowych powstaje rejestr czynności przetwarzania.

#### 3.2. Rejestr czynności przetwarzania danych osobowych

Administrator zgodnie z art. 30 RODO zobowiązany jest do prowadzenia:

- rejestru czynności przetwarzania danych osobowych, za które odpowiada (wzór stanowi załącznik nr 2 do niniejszej polityki);

- rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (wzór stanowi załącznik nr 3 do niniejszej polityki).

IOD jest odpowiedzialny za nadzorowanie prowadzenia rejestrów. Rejestry mogą być prowadzone w postaci elektronicznej.

## 4. ZASADY PRZETWARZANIA DANYCH

### 4.1. Ogólne zasady dotyczące przetwarzania danych osobowych

Zgodnie z wymogami RODO dane osobowe muszą być:

- Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zasada zgodności z prawem, rzetelności i przejrzystości”);
- Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; w myśl art. 89 ust. 1 RODO dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie uznaje się za niezgodne z pierwotnymi celami („zasada ograniczenia celu”);
- Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane („zasada minimalizacji danych”);
- **Prawidłowe i w razie potrzeby uaktualniane**; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- **Przechowywane w formie umożliwiającej identyfikację osoby**, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, w których dane te 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 na mocy artykułu 89 ust.1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą;
- **Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych**, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych lub organizacyjnych.

### 4.2. Szczegółowe zasady przetwarzania danych osobowych

#### 4.2.1. Przesłanki przetwarzania

ADO przetwarza dane osobowe na podstawie:

- zgody osoby, których dane osobowe dotyczą (art. 6. ust 1. pkt a RODO);

- zawartej umowy przez osobę, której dane osobowe dotyczą, a przetwarzanie jest niezbędne do wykonania umowy (art. 6 ust.1 pkt b RODO);
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust.1 pkt c RODO)
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 pkt d RODO)
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust.1 pkt e RODO)
- przetwarzanie danych osobowych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędnym charakterem wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust.1 pkt f RODO);

*Powyższy punkt nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.*

- na mocy zawartej umowy powierzenia zgodnie z art. 28 RODO.

#### 4.2.2. Obowiązek informacyjny

ADO przy zbieraniu danych osobowych musi wypełnić obowiązki informacyjne, zgodnie z art. 13 i 14 RODO.

Minimalny zakres informacji, które muszą być umieszczone w obowiązku informacyjnym znajduje się w załączniku nr 4 do niniejszej polityki.

Obowiązek informowania nie wykonuje się, jeżeli przepisy innej ustawy zezwalają na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub gdy osoba, której dane dotyczą, posiada informacje, o których mowa wyżej.

Jeżeli przetwarzanie danych osobowych wymaga zgody osoby, której dane dotyczą to należy ją pobrać zgodnie ze wzorem stanowiącym załącznik nr 5 do niniejszej polityki.

Zgodnie z art. 14 RODO należy każdorazowo wykonywać obowiązek informacyjny w stosunku do osób, których dane są przetwarzane w zbiorze, a zostały pozyskane z innych źródeł, chyba że dane osobowe zostały powierzone do przetwarzania w myśl art. 28 RODO.

Obowiązek informacyjny należy spełnić również w przypadku zmiany celu przetwarzania danych, do którego dane zostały zebrane.

#### 4.2.3. Dokładność i aktualność danych osobowych

ADO ma obowiązek zapewnić, aby wszystkie gromadzone i przetwarzane dane osobowe były dokładne i aktualne. Dokładność danych sprawdza się bezpośrednio po ich zebraniu, a następnie w regularnych

odstępach czasu. W przypadku znalezienia jakichkolwiek niedokładnych lub nieaktualnych danych, należy niezwłocznie podjąć wszelkie uzasadnione kroki w celu zmiany lub usunięcia tych danych, zależnie od okoliczności.

#### 4.2.4. Czasowe przetwarzanie danych osobowych

ADO nie przechowuje danych osobowych dłużej niż to konieczne do realizacji celów, dla których dane te zostały pierwotnie zgromadzone i przetworzone. Po zakończeniu realizacji celu w którym dane zostały zebrane ADO musi podjąć niezwłocznie wszelkie rozsądne kroki w celu ich usunięcia (bez opóźnień).

Po wygaśnięciu celu przetwarzania danych osobowych mogą być one tylko i wyłącznie przetwarzane w celu spełnienia wymogów przepisów prawa.

#### 4.2.5. Zasady dotyczące profilowania

RODO wprowadza pojęcie „profilowanie”, które zgodnie z art. 4 ust. 1 pkt 4 RODO oznacza 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.

Osoba, której dane osobowe dotyczą, na podstawie art. 22 RODO, ma prawo by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, chyba że:

- osoba, której dane osobowe dotyczą wyraziła w sposób wyraźny zgodę na tą czynność;
- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO;
- jest dozwolona prawem, któremu podlega ADO i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Za każdym razem należy powiadomić o wykonywaniu profilowaniu lub jego braku osobę, której dane osobowe dotyczą. Obowiązek informacyjny dotyczy także sytuacji, kiedy mechanizmy profilowania nie wywołują wobec tej osoby skutków prawnych lub w podobny sposób istotnie na nią nie wpływają, np. marketing na stronie internetowej na podstawie aktywności osoby, która przegląda daną stronę.

#### 4.2.6. Przetwarzanie danych szczególnych

RODO w art. 9 definiuje dane osobowe szczególnej kategorii (zwane dalej danymi szczególnymi) jako dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Danych szczególnych organizacja nie może przetwarzać, chyba że zostanie spełniony jeden z poniższych warunków:

- Osoba, której dane dotyczą, wyraziła w sposób wyraźny zgodę na przetwarzanie danych osobowych (chyba że przepis prawa stanowi, iż osoba, której dane osobowe dotyczą nie może uchylić zakazu);
- Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora danych osobowych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa;
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- Przetwarzanie dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłączenie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osoby, których dane dotyczą;
- Przetwarzanie dotyczy danych osobowych w sposób oczywisty upubliczniony przez osobę, której dane dotyczą;
- Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa;
- Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa lub zgodnie z umową z pracownikiem służby zdrowia zgodnie z prawem;
- Przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, na podstawie przepisów prawa;
- Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie przepisów prawa.

#### 4.2.7. Zasady udostępnienia i powierzania danych osobowych

Dane osobowe udostępnia się na pisemny, umotywowany wniosek pochodzący od danego podmiotu lub osoby, chyba że szczególne przepisy prawa stanowią inaczej.

Wniosek o udostępnienie informacji, o którym mowa powyżej, powinien zawierać:

- nazwę podmiotu, jego adres oraz podpis osoby upoważnionej do jego reprezentowania;
- podstawę prawną upoważniającą go do otrzymania informacji na mocy przepisów prawa lub zawartej umowy;
- wskazanie przeznaczenia dla udostępnionych danych;
- zakres żądanych informacji;
- uzasadnienie potrzeby posiadania informacji, jeżeli ich otrzymywanie nie wynika z przepisów prawa lub zawartej umowy.

Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione. Każdorazowe udostępnienie danych osobowych musi być zatwierdzone przez ADO.

Powierzenie danych osobowych do przetwarzania odbywa się zgodnie z art. 28 RODO. Zgodnie z tym artykułem powierzenie może nastąpić na podstawie odpowiedniej umowy spełniającej wymogi wynikające z art. 28 ust. 3 RODO. Każda umowa o powierzeniu danych osobowych przed podpisaniem przez upoważnione osoby musi zostać parafowana przez IOD lub zatwierdzona drogą mailową. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 6 do niniejszej polityki.

#### 4.2.8. Zasady transgraniczności i przetwarzania w państwie trzecim

Transgraniczne przetwarzanie danych osobowych, zgodnie z art. 4 ust. 1 pkt 23 RODO oznacza:

- przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
- przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.

Administrator lub podmiot przetwarzający komunikuje się w sprawie dokonywanego przez nich transgranicznego przetwarzania jedynie z wiodącym organem nadzorczym.

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych reguluje rozdział V RODO.

Ze względu na to, że przekazywanie danych osobowych do państwa trzeciego (poza UE) może powodować zwiększenie ryzyka naruszenia praw i wolności osoby, które dane dotyczą, ADO jest zobowiązany do identyfikacji takich sytuacji oraz zastosowania odpowiednich środków bezpieczeństwa.

Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

W razie braku decyzji wyżej wymienionej w stosunku do danego państwa trzeciego administrator może przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. W sytuacji spełnienia wymienionych zabezpieczeń w oparciu o art. 46 ust. 2 RODO można przekazać bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego UODO.

#### 4.2.9. Zasady analizy podmiotów przetwarzających

Podmiot przetwarzający dane osobowe na rzecz ADO przed rozpoczęciem współpracy może zostać poddany analizie, czy daje rękojmię odpowiednich wdrożonych zabezpieczeń. ADO podejmuje decyzję w tym zakresie na podstawie zakresu powierzonych danych osobowych.

W związku z powyższym IOD dokonuje analizy na podstawie odpowiedzi przesłanych przez podmiot przetwarzający wysłanego wcześniej kwestionariusza, który stanowi załącznik nr 7. IOD na podstawie analizy przekazuje rekomendację:

- rozpoczęcia współpracy;
- wstrzymania współpracy do momentu usunięcia niezgodności;
- odstąpienie od współpracy.

IOD przekazuje rekomendację ADO, który podejmuje ostateczną decyzję w tym zakresie.

IOD taką analizę przeprowadza z częstotliwością nie mniejszą niż raz na 12 miesięcy w stosunku do wskazanych ADO podmiotów przetwarzających.

IOD prowadzi rejestr przeprowadzonych analiz podmiotów przetwarzających dane osobowe. Wzór rejestru stanowi załącznik nr 8.

## **5. ANALIZA RYZYKA I OCENA SKUTKÓW**

### **5.1. Analiza ryzyka**

ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

ADO przeprowadza i dokumentuje analizę stosowanych środków bezpieczeństwa danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i skutkach dla dostępności integralności i poufności danych.

Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

W ramach analizy ryzyka, ADO identyfikuje i ocenia stosowane mechanizmy kontroli ryzyka dla poszczególnych zagrożeń, a w przypadku stwierdzenia takiej potrzeby, planuje i wdraża uwzględniając koszty i aktualny stan wiedzy, nowe metody kontroli ryzyka zapewniające zadowalający poziom bezpieczeństwa.

Analiza ryzyka przeprowadzana jest nie rzadziej niż raz na rok.

### **5.2. Ocena skutków**

Przed rozpoczęciem przetwarzania danych osobowych, który ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub

wolności osób fizycznych, ADO dokonuje oceny skutków planowanych czynności przetwarzania dla ochrony danych.

Ocena skutków dla ochrony danych, zgodnie z art. 35 ust. 3 RODO, jest wymagana w szczególności w przypadku:

- a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
- b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa,
- c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Analiza ryzyka i ocena skutków przeprowadzana jest zgodnie z Metodologią analizy ryzyka i oceny skutków.

## **6. ŚRODKI ZAPEWNIAJĄCE BEZPIECZEŃSTWO DANYCH**

### **6.1. Środki fizyczne**

Obszarem przetwarzania danych osobowych jest obszar, w którym wykonywane są operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.

Szczegółowy wykaz obszarów przetwarzania został przedstawiony w załączniku nr 9 do niniejszej polityki ochrony danych osobowych.

Przebywanie wewnątrz obszaru, o którym jest mowa powyżej, osób nieupoważnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

Wykaz zastosowanych środków ochrony fizycznej dla określonego obszaru przetwarzania znajduje się w załączniku nr 10 do niniejszej polityki ochrony danych osobowych.

### **6.2. Środki organizacyjne**

#### **6.2.1. Zasady upoważniania osób do przetwarzania danych osobowych**

W celu spełnienia wymogu wynikające z art. 29 RODO ustanowiono następujące zasady:

- Dostęp do danych osobowych w organizacji mają tylko osoby upoważnione.



- Upoważnienie do przetwarzania danych osobowych nadaje ADO lub wskazana przez niego osoba. Wzór upoważnienia stanowi załącznik nr 11.
- Dostęp do przetwarzania danych osobowych są nadawane pracownikom i współpracownikom organizacji zgodnie z zakresem ich obowiązków służbowych lub zleconymi działaniami operacyjnym.
- Osoba, która otrzymała upoważnienie do przetwarzania danych osobowych jest zobowiązana do zapoznania się z niniejszą polityką i przestrzegania jej postanowień oraz jest zobowiązana do zachowania w tajemnicy danych osobowych i ich ochrony nawet po zakończeniu przetwarzania danych osobowych przez Administratora. Fakt ten potwierdza własnoręcznym podpisem na odpowiednim oświadczeniu. Wzór oświadczenia stanowi załącznik nr 12.
- Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do przejścia szkolenia w zakresie:
  - niniejszej polityki,
  - RODO i Ustawy w zakresie stosownym do wykonywanych obowiązków służbowych.

#### 6.2.2. Rejestr osób upoważnionych do przetwarzania danych osobowych

Rejestr osób upoważnionych do przetwarzania danych osobowych jest prowadzony przez ADO lub wyznaczoną przez niego osobę zgodnie ze wzorem stanowiącym załącznik nr 13 do niniejszej polityki.

#### 6.2.3. Szkolenia

Każda osoba dopuszczona do przetwarzania danych osobowych w ramach organizacji musi zostać przeszkolona za zakresu ochrony danych osobowych. Ważność takiego szkolenia została ustanowiona na 24 miesiące, jednakże, jeżeli następuje zmiana stanowiska, to osoba musi zostać ponownie przeszkolona. Lista osób przeszkolonych jest prowadzona przez Administratora lub wskazaną osobę. Szkolenie mogą odbywać się w formie e-learningowej.

#### 6.2.4. Audyt wewnętrzny

IOD jest zobowiązany do przygotowania programu audytów, w którym określa zakres i kryteria oraz harmonogram audytów zgodnie z zatwierdzonym planem. Celami audytu jest:

- potwierdzenie zgodności wdrożonego systemu ochrony danych osobowych z RODO i Ustawą;
- potwierdzenie skuteczności wdrożonych zabezpieczeń organizacyjnych i technicznych;
- potwierdzenie zgodności wdrożonego systemu ochrony danych osobowych u podmiotów, którym ADO powierzył przetwarzanie danych osobowych.

Program audytów jest zatwierdzany przez ADO na początku każdego roku kalendarzowego. Załącznik nr 14 do niniejszej polityki stanowi wzór programu audytów.

Z każdego przeprowadzanego audytu zgodnie z założonym programem powstaje raport po audytowy, w którym IOD przedstawia stan faktyczny i ocenia jego zgodność. W sytuacji wykrycia niezgodności (niespełnienie wymogu) IOD wskazuje rekomendację dla ADO.

Raport z przeprowadzonego audytu musi zostać przedstawiony w ciągu 30 dni od momentu zakończenia danego audytu. ADO zatwierdza raport oraz określa, które rekomendacje należy zrealizować oraz przez kogo powinny one być wykonane.

IOD jest zobowiązany do monitorowania stanu wdrożenia zatwierdzonych rekomendacji.

#### 6.2.5. Przegląd systemu ochrony danych osobowych

Raz do roku IOD jest zobowiązany opracować i przedstawić do ADO raport przeglądu zarządzania. ADO jest zobowiązany przyjąć przedstawiony raport oraz zatwierdzić proponowane działania związane z systemem ochrony danych osobowych.

Raport z przeglądu systemu ochrony danych osobowych powinien zawierać następujące elementy:

- stan działań podjętych w wyniku poprzedniego przeglądu;
- zmiany w zakresie istotnych czynników, które mogą wpłynąć na system ochrony danych osobowych;
- informacje wynikające z postępów dotyczących planu postępowania z ryzykiem;
- wyniki audytów wewnętrznych wraz z informacją o stanie wdrażanych działań;
- zidentyfikowane incydenty naruszenia danych osobowych;
- wyniki szacowania ryzyka i przeprowadzonej oceny skutków dla ochrony danych osobowych;
- informacje zwrotne od zainteresowanych stron.

### 6.3. Środki techniczne

#### 6.3.1. Rejestr systemów teleinformatycznych w których przetwarzane są dane osobowe

ADO przy współpracy ASI prowadzi rejestr systemów przetwarzających dane osobowe. Rejestr ten obejmuje systemy zarządzane przez dział IT, jak i systemy zewnętrzne dostarczane przez zewnętrzne podmioty. Wzór rejestru systemów przetwarzających stanowi załącznik nr 15.

Każdy system przetwarzający dane osobowe musi zostać zweryfikowany przez IOD raz na pięć lat, chyba, że zaszły znaczące zmiany, które mogą wpływać na bezpieczeństwo przetwarzania danych osobowych.

Każdy nowy system przed rozpoczęciem użytkowania podlega analizie bezpieczeństwa, która wykonywana jest przez IOD. IOD przedstawia swoją rekomendację do ADO, który na tej podstawie podejmuje decyzję o rozpoczęciu użytkowania danego rozwiązania.

Dział IT lub osoba odpowiedzialna za procesy wykorzystujące zewnętrzne systemy jest zobowiązana do zgłaszania zmian lub nowych rozwiązań do IOD.

#### 6.3.2. Zasady ochrony danych osobowych przetwarzanych w systemach informatycznych

Zasady dotyczące bezpieczeństwa przetwarzania danych osobowych w systemach i urządzeniach teleinformatycznych zostały opisane w Polityce bezpieczeństwa danych osobowych w IT.

## **7. OCHRONA DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA**

### **7.1. Zasady ochrony danych w fazie projektowania (Privacy by design)**

- 1) ADO planując nowe zadania, projekty lub usługi oraz wykonując już funkcjonujące zapewnia środki organizacyjne i techniczne służące bezpieczeństwu danych osobowych.
- 2) W fazie planowania nowych zadań, projektów lub usług ADO analizuje w konsultacji z IOD:
  - a. czy przetwarzanie danych osobowych będzie spełniało wymagania RODO, w szczególności czy zapewnione jest spełnienie podstawowych zasad przetwarzania danych osobowych, o których mowa w art. 5 RODO ,
  - b. czy możliwa będzie realizacja praw i wolności podmiotów danych, którzy będą korzystali z nowego zadania, projektu lub usługi,
  - c. czy ADO jest w stanie zapewnić odpowiednie środki organizacyjne i techniczne, w tym pseudonimizację i minimalizację, zapewniające bezpieczeństwo przetwarzanych danych w kontekście zidentyfikowanych ryzyka.
- 3) Uwzględnienie ochrony danych osobowych w fazie projektowania należy stosować także w sytuacji, gdy dokonywane są zakupy lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

Każdą zmianę w procesach (uwzględniając zmiany w obszarze aktywów wspierających) w których są przetwarzane dane osobowe należy skonsultować z IOD w celu określenia, czy nie wpływają one na bezpieczeństwo przetwarzanych danych osobowych. Wraz z IOD należy przeprowadzić analizę ryzyka w obszarze planowanych zmian oraz w razie konieczności przeprowadzić ocenę skutków dla ochrony danych. Przed wdrożeniem zmian należy wdrożyć stosowne zabezpieczenia, które zostały zidentyfikowane podczas przeprowadzonej analizy ryzyka i oceny skutków.

Każdą zmianę w zakresie zbieranych i przetwarzanych danych osobowych należy skonsultować z IOD. Przed rozpoczęciem zmian w zakresie przetwarzanych danych osobowych należy przeprowadzić stosowną analizę ryzyka oraz w uzasadnionych przypadkach należy dokonać oceny skutków. Przed rozpoczęciem wprowadzania zmian w zakresie zbieranych danych osobowych należy wdrożyć stosowne zabezpieczenia zidentyfikowane podczas analizy ryzyka i oceny skutków.

### **7.2. Zasada domyślnej ochrony danych (Privacy by default)**

Podczas zbierania danych osobowych należy stosować zasadę minimalnego zakresu i minimalnej ilości, w celu zminimalizowania zagrożeń dla osoby, której dane osobowe dotyczą.

Dostęp do danych osobowych podczas ich przetwarzania należy minimalizować, ilość danych przetwarzanych powinna być zminimalizowany do celu danego przetwarzania.

## **8. PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ**

### **8.1. Zasady ogólne**

Każdej osobie, których dane dotyczą przysługują następujące prawa na podstawie RODO:

- Prawo dostępu do danych – art. 15 RODO;
- Prawo do sprostowania danych – art. 16 RODO;
- Prawo do usunięcia danych („prawo do bycia zapomnianym”) – art. 17 RODO;
- Prawo do ograniczenia przetwarzania – art. 18 RODO;
- Prawo do przenoszenia danych – art. 20 RODO;
- Prawo do sprzeciwu – art. 21 RODO.

Osoba, która chciałaby skorzystać z powyższych praw musi złożyć stosowny wniosek w postaci papierowej lub elektronicznej do Administratora Danych. Jednakże złożenie takiego wniosku musi być tak samo łatwe jak było zebranie danych od tej osoby.

Każde takie zgłoszenie musi zostać zarejestrowane oraz niezwłocznie zgłoszone do IOD. W ciągu 30 dni od momentu zgłoszenia wpłynięcia wniosku do ADO, należy udzielić odpowiedzi. Jeżeli czynności będą wymuszały wydłużenie terminu o następne maksymalnie 30 dni, także należy o tym fakcie powiadomić zgłaszającego. Administrator udziela odpowiedzi lub realizuje zgłoszenie przy współpracy z IOD.

Prawa opisane w niniejszym rozdziale mogą zostać ograniczone, ale może to być tylko i wyłącznie na podstawie przepisów prawa. O takim ograniczeniu ze wskazaniem na przepis prawa należy powiadomić wnioskodawcę udzielając odpowiedzi na zgłoszenie.

Realizacja powyższego odbywa się tylko w stosunku do danych osobowych gdzie organizacja jest Administratorem Danych, w sytuacji otrzymania takiego zgłoszenia odnośnie danych osobowych, które zostały powierzone należy niezwłocznie przekazać takie zgłoszenie do IOD danego Administratora Danych zgodnie z zawartą umową powierzenia.

### **8.2. Identyfikacja zgłaszającego**

Osoba zgłaszająca wniosek o realizację przysługujących mu praw określonych w zasadach ogólnych musi zostać jednoznacznie zidentyfikowana. Identyfikacja takiej osoby, musi się opierać na informacjach, które są znane ADO oraz osobie zgłaszającej a nie są dostępne publicznie.

Jeżeli zgłoszenie nastąpiło drogą mailową lub drogą tradycyjnej poczty, oraz zgłoszenie samo nie zawierało wymaganych informacji w celu identyfikacji danej osoby, należy wysłać do takiej osoby prośbę o wypełnienie informacji brakujących z wykorzystaniem formularza stanowiącego załącznik nr 16 do niniejszej procedury.

Identyfikację można także wykonać drogą telefoniczną (jeżeli jest dostępny numer telefonu do kontaktu), z prośbą o podanie informacji określonych w skrypcie rozmowy telefonicznej, który stanowi załącznik nr 16 do niniejszej procedury.

### 8.3. Rejestracja zgłoszenia

Każde zgłoszenie, o którym jest mowa powyżej, zostaje zarejestrowane zgodnie z zasadami obiegu dokumentów obowiązującymi u Administratora.

Zgłoszenie powinno zostać przekazane niezwłocznie do IOD, po dokonaniu prawidłowej identyfikacji osoby zgłaszającej przez ADO lub osobę wyznaczoną. IOD prowadzi własny oddzielny rejestr zgłoszeń. Każdemu zarejestrowanemu zgłoszeniu jest nadawany stosowny kolejny numer identyfikacyjny.

### 8.4. Opracowanie odpowiedzi

Po otrzymaniu zgłoszenia ADO wskazuje osobę odpowiedzialną za przygotowanie stosownej odpowiedzi. IOD wspiera przygotowanie odpowiedzi poprzez udzielanie stosownych rekomendacji.

Po przygotowaniu odpowiedzi przez osobę wskazaną, IOD weryfikuje przygotowaną odpowiedź, jeżeli tego wymaga sytuacja.

Przygotowana odpowiedź zatwierdzana i podpisywana jest przez Administratorowi Danych. Po zatwierdzeniu jest przekazywana do wysłania zgodnie z przyjętą procedurą obiegu dokumentów.

### 8.5. Bezpieczeństwo przekazywanych odpowiedzi

Odpowiedzi na zgłoszenia przekazywane są drogą korespondencji tradycyjnej, wysłanej na adres do korespondencji. Wysłanie odpowiedzi odbywa się listem poleconym za zwrotnym potwierdzeniem odbioru.

W sytuacji konieczności przesłania danych w postaci elektronicznej należy nagrać płytę CD/DVD z wymaganymi danymi, które muszą zostać przed nagraniem na nośnik zaszyfrowane.

Informację o dacie wysyłki oraz o dacie potwierdzenia odbioru należy przekazać do IOD, który zobowiązany jest dokonać aktualizacji rejestru.

## 9. POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

### 9.1. Zasady ogólne dot. naruszenia ochrony danych osobowych

Naruszenie ochrony danych osobowych, zgodnie z art. 4 ust. 1 pkt 12 RODO, oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Każde naruszenie ochrony danych osobowych, w którym prawdopodobne jest wystąpienie ryzyka naruszenia praw lub wolności osób fizycznych, należy bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłosić do UODO. Zasady zgłoszenia naruszenia ochrony danych osobowych oraz wskazanie elementów, które powinny być zawarte w treści zgłoszenia określa art. 33 RODO.

Każde naruszenie ochrony danych osobowych musi zostać zgłoszone do IOD, który wspiera ADO w procesie identyfikacji i określenia skutków takiego naruszenia.

Każde naruszenie u podmiotów przetwarzających, a dotyczących powierzonych danych osobowych, należy niezwłocznie zgłosić do IOD, ale nie później niż w ciągu 48 godzin po stwierdzeniu naruszenia. Zapisy dotyczące kwestii zgłaszania naruszeń muszą się znajdować w umowach między ADO, a podmiotem przetwarzającym.

### 9.2. Zasady komunikacji

Każdy pracownik/współpracownik w momencie zauważania lub podejrzenia naruszenia ochrony danych osobowych musi zgłosić to do Administratora lub do bezpośredniego przełożonego. Administrator / bezpośredni przełożony jest zobowiązany niezwłocznie powiadomić IOD.

IOD jest odpowiedzialny za wsparcie podczas zebrania informacji dotyczących stanu faktycznego oraz zaproponowanie działań minimalizujących skutki danego naruszenia.

IOD przygotowuje zgłoszenie do UODO. Ostateczną decyzję o zgłoszeniu podejmuje Administrator Danych po zasięgnięciu rekomendacji od IOD oraz prawnika.

ADO zgłasza do UODO sytuację, jeżeli uzna, że nastąpiło naruszenie ochrony danych osobowych nawet w sytuacji niemożliwości konsultacji z IOD.

### 9.3. Zasady raportowania

IOD odpowiada za sporządzenie odpowiedniego raportu. Wzór takiego raportu stanowi załącznik nr 17 do niniejszej polityki. IOD odpowiada za raportowanie do Administratora Danych postępu prac dotyczących analizy zaistniałego incydentu oraz stanu wdrożonych działań korygujących.

Administrator raportuje do UODO zgodnie z przyjętymi zasadami przez UODO.

## **10. ODPOWIEDZIALNOŚĆ KARNA ZA NARUSZENIE OCHRONY DANYCH OSOBOWYCH**

Nieprzestrzeganie zasad określonych w niniejszym dokumencie skutkuje sankcjami karnymi przewidzianymi Kodeksie Karnym art. 266 – 269,287.

Niezależnie od odpowiedzialności przewidzianych w przepisach karnych, postępowanie wbrew obowiązującym u ADO zasadom ochrony danych osobowych może również być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych, co stanowi podstawę do rozwiązania stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

Ponadto, zgodnie z art. 82 RODO, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia ogólnego rozporządzenia o ochronie danych, ma prawo uzyskać od Administratora Danych lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

## **11. WYKAZ ZAŁĄCZNIKÓW**

- Załącznik nr 1 – Wyciąg polityki bezpieczeństwa danych osobowych dla podmiotów zewnętrznych;
- Załącznik nr 2 – Rejestr czynności przetwarzania danych osobowych;
- Załącznik nr 3 – Rejestr kategorii czynności przetwarzania;
- Załącznik nr 4 – Wzór obowiązku informacyjnego;
- Załącznik nr 5 – Wzór klauzuli zgody przetwarzania danych osobowych;
- Załącznik nr 6 – Wzór umowy powierzenia przetwarzania danych osobowych;
- Załącznik nr 7 – Kwestionariusz pytań dla podmiotu przetwarzającego dane osobowe;
- Załącznik nr 8 – Rejestr podmiotów poddanych analizie;
- Załącznik nr 9 – Wykaz obszarów przetwarzania danych osobowych;
- Załącznik nr 10 – Wykaz zastosowanych środków ochrony fizycznej;
- Załącznik nr 11 – Wzór upoważnienia do przetwarzania danych osobowych
- Załącznik nr 12 – Wzór oświadczenia o zachowaniu poufności osoby upoważnionej do przetwarzania danych osobowych;
- Załącznik nr 13 – Wzór rejestru osób upoważnionych do przetwarzania danych osobowych;
- Załącznik nr 14 – Program audytów;
- Załącznik nr 15 – Wzór rejestr systemów przetwarzających dane osobowe;
- Załącznik nr 16 – Formularz dla osoby, która zgłasza chęć skorzystania z praw jej przysługujących;
- Załącznik nr 17 – Raport z incydentu naruszenia ochrony danych osobowych.

## 12. DOKUMENTY ZWIĄZANE

Instrukcja zarządzania systemem informatycznym w Starostwie Powiatowym w Żyrardowie

Metodyka analizy ryzyka i oceny skutków.

WICESTAROSTA

Krzysztof Dziwisz