

## **Polityka Ochrony Danych w Miejskim Ośrodku Pomocy Społecznej w Łławie**

### **I. WSTĘP**

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Miejskim Ośrodku Pomocy Społecznej w Łławie w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

### **II. INWENTARYZACJA DANYCH**

1. Poprzez dane osobowe, zgodnie z art. 4 pkt 1) RODO należy rozumieć wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można w sposób pośredni lub bezpośredni zidentyfikować, z uwzględnieniem identyfikatorów. Dane te mogą dotyczyć pracowników, klientów, kontrahentów lub osoby współpracujące z Miejskim Ośrodkiem Pomocy Społecznej w Łławie.
2. Dane osobowe w Miejskim Ośrodku Pomocy Społecznej w Łławie zorganizowane są w struktury, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO,
3. Dane osobowe opisane są z uwzględnieniem, co najmniej poniższych informacji:
  - 1) nazwę zbioru;
  - 2) opis celów przetwarzania;
  - 3) charakter, zakres, kontekst, dokumentowane dane osobowe;
  - 4) odbiorcy;
  - 5) Funkcjonalny opis operacji przetwarzania;
  - 6) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing);
4. Szczegółowy opis danych osobowych został przedstawiony w **wykazie zbiorów osobowych**.

### **III. ZAPEWNIENIE O PRZETWARZANIU DANYCH OSOBOWYCH ZGODNIE Z PRAWEM**

1. Administrator zapewnia, że:
  - a. dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;
  - b. zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;
  - c. Administrator przechowuje dane osobowe przez konkretnie określony czas, zgodnie z przepisami prawa.

- d. wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12 - 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym”;
  - e. osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano dane kontaktowe w klauzulach informacyjnych;
  - f. obowiązek informacyjny wobec osób których dane są przetwarzane może być wykonany, poprzez umieszczenie na tablicy informacyjnej w budynku Miejskiego Ośrodka Pomocy Społecznej w Łławie i na stronie internetowej;
  - g. Z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty
2. Potwierdzenie zgodnego z prawem przetwarzania danych osobowych znajduje się w **Rejestrze czynności**.

#### **IV. UPOWAŻNIENIA**

1. Administrator do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Łławie dopuszcza jedynie osoby posiadające stosowane upoważnienia. Wzór stosownych upoważnień stanowi **Wzór upoważnienia**.
2. Administrator jest odpowiedzialny za proces nadawania i wycofywania upoważnień do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Łławie .
3. W Miejskim Ośrodku Pomocy Społecznej w Łławie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, w sposób umożliwiający prawidłową identyfikację historii i prawidłowości procesu przetwarzania danych osobowych

#### **V. POUFNOŚĆ PROCESU PRZETWARZANIA DANYCH OSOBOWYCH**

1. Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z Miejskim Ośrodkiem Pomocy Społecznej w Łławie jest zobowiązana do:
  - a. przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało im wydane upoważnienie lub podpisano umowę powierzenia przetwarzania danych osobowych,
  - b. zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,
  - c. niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia lub umowy powierzenia przetwarzania danych osobowych,
  - d. zachowania poufności procesów i metod zabezpieczeń danych osobowych stosowanych w Miejskim Ośrodku Pomocy Społecznej w Łławie,
  - e. ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacją, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób niepożądanych.
2. Osoby dopuszczone do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Łławie, przed przystąpieniem do pracy, powinny odbyć szkolenie z zasad ochrony danych osobowych , o którym mowa szerzej w rozdziale XI
3. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych.

4. Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Stosowana jest zasada tzw. zasada czystego biurka
5. Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez stosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach, itd. .
6. Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarek.
7. Zaleca się szczególne zwrócenie uwagi pracownikom na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, przy kopiarkach, drukarkach itp.
8. Administrator jest zobowiązany do corocznej weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, do których ustały podstawy przetwarzania.

## VI. PROCEDURA ANALIZY RYZYKA I OCENA SKUTKÓW

### 1. Analiza ryzyka

- 1.1 Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
- 1.2 Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.
- 1.3 W trakcie analizy ryzyka należy wyodrębnić następujące elementy:
  - aktywa – są to wszystkie środki i narzędzia mające istotne znaczenie dla podmiotu,
  - zagrożenia – są to przykłady potencjalnych naruszeń systemu
  - skutki – są to niepożądane następstwa zrealizowania się zagrożeń w praktyce
  - ryzyko – jest to prawdopodobieństwo, że zagrożenia się zrealizują i przyniosą konkretny, negatywny skutek dla aktywów.
- 1.4 Wyliczenie poziomu Ryzyka (R) następuje poprzez iloczyn określonego przez Administratora Prawdopodobieństwa (P) wystąpienia zagrożenia w podmiocie i Skutku (S) wystąpienia takiego zagrożenia w Zespole Szkół Ogólnokształcących im. S. Żeromskiego w Łławie tj.  $R = P \times S$ .
- 1.5 Skalę prawdopodobieństwa obrazuje tabela A

Tabela A

Prawdopodobieństwo wystąpienia zagrożenia	Skala
Ekstremalny poziom	4
Wysoki poziom	3
Średni poziom	2
Niskie	1
Brak	0

1.6 Skalę Skutków (S) określa Tabela B. Do określenia skali stosuje się pomocniczo dodatkowe kryteria oceny pozwalające na prawidłowe oszacowanie potencjalnych strat.

Tabela B

<b>Skutki wystąpienia zagrożenia</b>	<b>Skala</b>
Ekstremalny poziom	4
Wysoki poziom	3
Średni poziom	2
Niskie	1
Brak	0

1.7 Administrator, po dokonaniu wyliczenia Ryzyka (R) ma obowiązek odniesienia jego poziomu do skali i podejmuje dalsze działania związane z ryzykiem.

1.8 Skalę Ryzyka w podmiocie określa tabela C.

Tabela C

<b>Poziom ryzyka</b>	<b>Wartość ryzyka <math>R = P \times S</math></b>
Wysokie (należy przeprowadzić czynności mające na celu obniżenie ryzyka)	9 -16
Opcjonalne (Administrator może je obniżyć lub zaakceptować)	5-8
Akceptowalne (pomijane) niewymagające dalszego postępowania. Pozostawienie ryzyka na poziomie określonym w procesie szacowania i zaniechania dalszych działań	1-4

## **2. Reakcja na ryzyko**

2.1 Jeśli ryzyko w podmiocie jest na poziomie akceptowalnym, Administrator potwierdza jedynie, że zastosowane zabezpieczenia są właściwe.

2.2 W przypadku ryzyka na poziomie opcjonalnym Administrator musi ocenić czy jest możliwość obniżenia jego poziomu poprzez zastosowanie stosownych zabezpieczeń lub czy może je zaakceptować. W przypadku akceptacji ryzyka Administrator ma obowiązek jego monitorowania.

2.3 W celu obniżenia poziomu ryzyka Administrator może przeprowadzić następujące czynności:

- a. przeniesienie ryzyka – np. zakup ubezpieczenia, powierzenie procesów przetwarzania podmiotom zewnętrznym,

- b. unikanie ryzyka – np. poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnie niebezpiecznych sytuacji,
  - c. obniżanie ryzyka – np. poprzez zastosowanie dodatkowych zabezpieczeń.
- 2.4 W przypadku, kiedy ryzyko jest na poziomie nieakceptowalnym, Administrator po wprowadzeniu dodatkowych zabezpieczeń, przeprowadza ponowną analizę ryzyka.

**2.5** Analiza ryzyka przeprowadzana jest za pomocą szablonu,

### **3. Ocena skutków dla ochrony danych osobowych**

3.1 Dla zbiorów danych osobowych, w których znajdują się dane osobowe, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO (DPIA)

3.2 Ocena skutków dla ochrony danych osobowych polega na:

- a. opisie planowanych operacji i celów przetwarzania,
- b. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,
- c. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- d. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu.

## **VII. Inspektor Ochrony Danych**

W jednostce istnieje obowiązek wyznaczenia Inspektora Ochrony Danych wynikający z art. 37 ust 1a RODO. W związku z powyższym w Miejskim Ośrodku Pomocy Społecznej w Łławie zostanie wyznaczony Inspektor Ochrony Danych. Za wyznaczenie IOD Odpowiada Administrator.

1. Inspektorem Ochrony Danych Osobowych w podmiocie może być jedynie osoba, która posiada fachową wiedzę na temat prawa i praktyki w jednostce.
2. Inspektor Ochrony Danych nie musi być pracownikiem Miejskiego Ośrodka Pomocy Społecznej w Łławie.
3. Administrator jest zobowiązany do udostępnienia danych kontaktowych Inspektora Ochrony Danych w sposób umożliwiający jego identyfikację i kontakt oraz jest zobowiązany powiadomić o nich organ nadzorczy.
  - 3.1 Poprzez udostępnienie danych Inspektora Ochrony Danych należy rozumieć, co najmniej ich publikację na stronie internetowej administratora oraz w widocznym miejscu, w siedzibie administratora.
4. Administrator ma obowiązek zapewnić Inspektorowi Ochrony Danych możliwość wykonywania jego obowiązków w sposób niezależny i zapewnić mu status, o którym mowa w art. 38 RODO.
5. Zadania Inspektora Ochrony Danych :
  - 5.1 informowanie administratora podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów regulujących tą materię,

- 5.2 monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów,
- 5.3 podejmowanie działań zwiększających świadomość personelu Miejskiego Ośrodka Pomocy Społecznej w Ławie , inicjowanie i organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania,
- 5.4 przeprowadzanie wewnętrznych audytów,
- 5.5 udzielanie na żądanie administratora zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z rozdziałem VI niniejszego dokumentu,
- 5.6 współpraca z organem nadzorczym,
- 5.7 pełnienie funkcji 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. Inspektor Ochrony Danych jest wyznaczony na podstawie stosowanego zarządzenia administratora.
7. Dane kontaktowe Inspektora Ochrony Danych są przekazywane organowi nadzorczemu według trybu i za pomocą narzędzi opracowanych i wdrożonych przez organ nadzoru.

#### **VIII. Rejestr czynności przetwarzania**

1. Dla zbiorów, w których przetwarzane są dane osobowe prowadzony jest rejestr czynności przetwarzania.
2. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO.
3. Rejestr czynności przetwarzania jest prowadzony w oparciu o wzór rejestru czynności.

#### **IX. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH**

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

#### **X. Kontrole wewnętrzne i audyty bezpieczeństwa**

1. Kontrolą systemów służących do przetwarzania danych osobowych zajmuje się Inspektor Ochrony Danych .
2. Kontrole przeprowadzane są regularnie, co najmniej raz do roku, a w przypadku wystąpienia incydentu w podmiocie , kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydem, który wystąpił.
3. Kontrola przeprowadzana jest z zastrzeżeniem wymogów i terminów określonych w RODO.
4. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postępowania, normami i przepisami wewnętrznymi.
5. Inspektor Ochrony Danych może wykonywać kontrole osobiście, może, przy aprobacie Administratora wyznaczyć do tego inną osobę lub podmiot.
6. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie.
7. Proces kontroli musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu kontrolnego.

8. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych w podmiocie, kontroler musi niezwłocznie powiadomić o tym fakcie administratora.
9. Wynik kontroli musi być udokumentowany i przekazany administratorowi w ciągu 14 dni od jej zakończenia.
10. Administrator może zlecić badanie audytowe niezależnemu podmiotowi, po poinformowaniu o tym fakcie Inspektora Ochrony Danych.

## **XI. SZKOLENIA**

1. Każdy pracownik/ współpracownik Miejskiego Ośrodka Pomocy Społecznej w Łławie. , przed przystąpieniem do pracy na zbiorach danych osobowych w podmiocie musi zostać przeszkolony w zakresie przepisów związanych z ochroną danych osobowych.
2. Za przeprowadzenie szkoleń odpowiada Inspektor Ochrony Danych
3. Każde szkolenie musi być udokumentowane listą obecności, na której poza imionami i nazwiskami jego uczestników z ich podpisami musi być opisany zakres szkolenia.
4. Inspektor Ochrony Danych przeprowadza szkolenia w miarę potrzeb, po każdej zmianie przepisów mających znaczenie dla procesów ochrony danych osobowych w podmiocie oraz nie rzadziej niż raz na 12 miesięcy.

## **XII. Monitoring**

W Miejskim Ośrodku Pomocy Społecznej w Łławie znajduje się monitoring wizyjny niezbędny do zapewnienia bezpieczeństwa pracowników i ochrony mienia. Zasady funkcjonowania monitoringu reguluje regulamin wewnętrzny.