**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

Dotyczy przetwarzania danych osobowych za pośrednictwem systemów informatycznych.

**Dokumentację opracowano zgodnie z:**

* Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2015 r.
poz. 2135 z późn. zm.*).
* Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.
(*Dz. U. z 2004 r. nr 100, poz. 1024*) w sprawie dokumentacji przetwarzania danych osobowych
oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

 Zatwierdził

 . . . . . . . . . . . . . . . . . . . .

 Podpis Administratora

Danych Osobowych

**Spis treści:**

1. Postanowienia ogólne . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 03

2. Użyte w instrukcji określenia . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 03

3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie

 informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności . . . . . . . . . . . . . . . . . . . . . . 04

4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem
 i użytkowaniem . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 04

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu . . 05

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem

 jest uzyskanie nieuprawnionego dostępu . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 06

7. Sposób realizacji wymogów odnotowania informacji o odbiorcach . . . . . . . . . . . . . . . . . . . . . . . . . . . 07

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do

 przetwarzania danych . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 07

9. Tworzenie oraz przechowywanie kopii zapasowych . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 08

10. Załączniki . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 09

**1. Postanowienia Ogólne**

**§ 1**

Niniejsza instrukcja dotyczy wszystkich zbiorów danych osobowych przetwarzanych w . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . za pośrednictwem systemów informatycznych.

Administrator Danych Osobowych stale nadzoruje procedury określone w dokumentacji Instrukcji Zarządzania Systemem Informatycznym pod kątem aktualności, poprawności, spójności i zgodności z przepisami prawa.

Każda osoba przetwarzająca dane osobowe za pośrednictwem systemów informatycznych zobowiązana jest do zapoznania się z treścią Instrukcji Zarządzania Systemem Informatycznym oraz do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień w nich zawartych.

Osoba przetwarzająca dane osobowe w systemie informatycznym zobowiązana jest złożyć oświadczenie o tym, że została zaznajomiona z obowiązującą Instrukcją Zarządzania Systemem Informatycznym. Administrator Danych Osobowych ewidencjonuje oświadczenia osób zaznajomionych z zasadami określonymi w Instrukcji Zarządzania Systemem Informatycznym *(wzór ewidencji określa* ***załącznik nr 3*** *dokumentacji Instrukcji Zarządzania Systemem Informatycznym*).

Dostęp do pomieszczeń, w którym przetwarzane są dane osobowe w systemie informatycznym jest zabezpieczony przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych poprzez wprowadzenie środków technicznych i organizacyjnych określonych w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

Dokładną lokalizację stacji roboczych służących do przetwarzania danych osobowych, określa **załącznik nr 2** dokumentacji Instrukcji Zarządzania Systemem Informatycznym*.*

**2. Użyte w Instrukcji określenia oznaczają:**

**§ 2**

1. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. **Administrator Danych Osobowych (ADO)** – Ośrodek Pomocy Społecznej reprezentowany przez Kierownika Ośrodka Pomocy Społecznej
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie,
5. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie,
6. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Bezpieczeństwa Informacji dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (*wzór upoważnienia stanowi* ***załącznik nr 5*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)* oraz wykazana w ewidencji upoważnień *(wzór ewidencji stanowi* ***załącznik nr 6*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych),*
7. **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych
w systemie informatycznym,

3

1. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(tekst jednolity: Dz. U.
2015 r. poz. 2135 z późn. zm.*).
2. **Rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji
z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. *(Dz. U. 2004 r. nr 100, poz. 1024).*

**3. Procedury nadawania uprawnień** **do przetwarzania danych i rejestrowania tych uprawnień** **w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności**

**§ 3**

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (*wzór upoważnienia stanowi* ***załącznik nr 5*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)*.

Administrator danych osobowych jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych *(wzór ewidencji stanowi* ***załącznik nr 6*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)*. Zgodnie z art. 39 ust. 1 Ustawy taka ewidencja zawiera:

* + 1. imię i nazwisko osoby upoważnionej,
		2. przypisany tej osobie identyfikator,
		3. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego odpowiada Administrator Danych Osobowych.

Administrator Danych Osobowych może pisemnie upoważnić inną osobę, która będzie zarządzała tworzeniem i przydzielaniem identyfikatorów, modyfikowaniem uprawnień użytkowników oraz usuwaniem nieaktywnych kont.

Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego pracownika.

**4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem
i użytkowaniem**

**§ 4**

1. System informatyczny służący do przetwarzania danych osobowych posiada mechanizm uwierzytelniający użytkownika, mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
2. Dostęp do systemu informatycznego, w którym użytkownik systemu będzie przetwarzał dane osobowe może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

4

1. Identyfikator wpisuje się do ewidencji prowadzonej przez administratora danych osobowych wraz z imieniem i nazwiskiem użytkownika.
2. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika
z systemu informatycznego nie może być przydzielany innej osobie. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników.
3. Hasła są poufne i muszą być zmieniane nie rzadziej niż raz na 30 dni przez użytkownika. Ponadto hasło musi składać się przynajmniej z ośmiu znaków, zawierać przynajmniej jedną wielką i małą literę oraz cyfry lub znaki specjalne.
4. W przypadku braku możliwości uzyskania dostępu do systemu informatycznego, użytkownik systemu zobowiązany jest powiadomić Administratora Danych Osobowych, który w zależności od mechanizmu działania systemu korzysta z opcji przypomnienia hasła, bądź nadania nowego.
5. W sytuacji podejrzenia naruszenia bezpieczeństwa działania systemu informatycznego służącego do przetwarzania danych osobowych (brak możliwości zalogowania pomimo wprowadzenia poprawnego identyfikatora oraz hasła lub stwierdzenie fizycznej ingerencji) użytkownik zobowiązany jest powiadomić Administratora Danych Osobowych, który przeprowadza sprawdzenie doraźne zgodnie z procedurą określoną w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

**5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla u**ż**ytkowników systemu**

**§ 5**

Przed rozpoczęciem pracy w systemie informatycznym służącym do przetwarzania danych osobowych oraz w jej trakcie każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora
i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu. Wznowienie pracy możliwe jest wyłącznie po ponownym podaniu danych użytkownika.

W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut następuje automatyczni wylogowanie aktywnego użytkownika. Wznowienie pracy możliwe jest wyłącznie po ponownym podaniu hasła.

Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jeden identyfikator. W przypadku, gdy przerwa w pracy na stacji roboczej ma trwać dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne monitory stanowisk dostępu do danych są ustawione w taki sposób żeby uniemożliwić tym osobom wgląd w dane.

Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika
z systemu.

5

**6. Sposób zabezpieczenia systemu informatycznego przed działalnością** **oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu.**

**§ 6**

W związku z tym, że system informatyczny narażony jest na działanie szkodliwego oprogramowania,
którego celem jest zniszczenie, zmienienie, lub umożliwienie osobom nieupoważnionym do danych osobowych konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

* + 1. nieuprawniony dostęp bezpośrednio do danych osobowych,
		2. uszkodzenie kodu aplikacji umożliwiającej dostęp danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
		3. przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci internet,
		4. przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
		5. uszkodzenie lub zafałszowanie danych osobowych przez szkodliwe oprogramowanie zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

Potencjalnymi źródłami przedostawania się szkodliwego oprogramowania na stacje robocze są :

1. załączniki do poczty elektronicznej,
2. przeglądane strony internetowe,
3. pliki i aplikacje pochodzące z sieci internet lub z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

W celu zapewnienia ochrony przed szkodliwym oprogramowaniem Administrator Danych Osobowych, lub osoba przez niego wyznaczona zarządzająca systemami informatycznymi na mocy pisemnego upoważnienia jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym szkodliwe oprogramowanie. System ten jest skonfigurowany w następujący sposób:

1. rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) jest stale włączony,
2. skaner ruchu internetowego (zapora ogniowa) jest stale włączony,
3. monitor zapewniający ochronę przed wirusami makr w arkuszach kalkulacyjnych oraz edytorach tekstu jest stale włączony,
4. skaner poczty elektronicznej jest stale włączony.

System skonfigurowany jest w taki sposób, iż nie rzadziej niż raz dziennie automatycznie dokonuje sprawdzenia możliwości aktualizacji bazy wirusów oraz szkodliwego oprogramowania i automatycznie jej dokonuje

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy użytkownik zobowiązany jest powiadomić Administratora Danych Osobowych, który podejmuje działania zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować :

1. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

6

1. samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji
lub po skonsultowaniu się z zewnętrznymi ekspertami.

Działania te może również wykonać osoba zarządzająca systemami informatycznymi wyznaczona przez Administratora Danych Osobowych na mocy pisemnego upoważnienia.

**7. Sposób realizacji wymogów odnotowania informacji o odbiorcach**

**§ 7**

1. System informatyczny odnotowuje:
	1. datę pierwszego wpisu do systemu;
	2. identyfikator użytkownika wprowadzającego dane osobowe do systemu;
	3. źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
	4. informacje o odbiorach danych osobowych.
	5. informacji o wniesieniu sprzeciwu wobec przetwarzania danych osobowych,
2. Odnotowanie to odbywa się automatycznie.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego następujące informacje:
	1. datę pierwszego wpisu do systemu;
	2. identyfikator użytkownika wprowadzającego dane osobowe do systemu;
	3. źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
	4. informacji o wniesieniu sprzeciwu wobec przetwarzania danych osobowych.

**§ 8**

**8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych**

Częstotliwość prac związanych z naprawą i konserwacją systemów informatycznych zależna jest od specyfiki danej stacji roboczej, zainstalowanego na niej systemu operacyjnego, oprogramowania, ilości użytkowników oraz częstotliwości wykorzystywania.

Wszelkie prace związane z naprawami i konserwacją systemów informatycznych przetwarzających dane osobowe muszą uwzględniać zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe prowadzone w tym zakresie mogą być wykonywane wyłącznie przez upoważnione do tego przez Administratora Danych Osobowych osoby.

Przed rozpoczęciem prac serwisowych przez osoby postronne konieczne jest potwierdzenie tożsamości serwisantów. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe,

przeznaczone do:

* 1. likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
	2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
	3. naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.

7

**9. Tworzenie oraz przechowywanie kopii zapasowych**

**§ 9**

Wszystkie dane osobowe przetwarzane w systemie informatycznym zabezpieczone są przed utratą lub zmienieniem poprzez wykonywanie okresowych kopii zapasowych.

Nośniki optyczne, magnetyczne oraz elektroniczne zawierające kopie zapasową zbiorów danych osobowych przechowywane są w innych pomieszczeniach niż systemy informatyczne, na których zostały utworzone w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione.

Wszystkie kopie zapasowe zbiorów danych osobowych przetwarzanych za pośrednictwem systemów informatycznych wykonuje się metodą kopii pełnej.

W zależności od systemu informatycznego kopię danych osobowych wykonuje się manualnie, półautomatycznie lub automatycznie.

Kopię zapasową przechowuje się do momentu wykonania nowej kopii zapasowej.

Częstotliwość dokonywania kopii zapasowej poszczególnych zbiorów, rodzaj nośnika, na którym przechowywane są dane osobowe oraz miejsce przechowywania nośnika, określa **załącznik nr 1** dokumentacji Instrukcji Zarządzania Systemem Informatycznym.

8

**Załącznik nr 1**

do Instrukcji Zarządzania Systemem Informatycznym

*w Ośrodku Pomocy Społecznej*

ZESTAWIENIE INFORMACJI DOTYCZĄCYCH WYKONYWANIA ORAZ PRZECHOWYWANIA KOPII ZAPASOWYCH

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp.: | Nazwa zbioru: | Częstotliwość wykonywania kopii zapasowej | Rodzaj nośnika: | Sposób wykonania kopii zapasowej: | Miejsce przechowywania: |
| 1 | Pomoc społeczna | codziennie  | oddzielny serwer | automatycznie | Pomieszczenie Urzędu Gminy |
| 2 | Świadczenia rodzinne | codziennie | oddzielny serwer | automatycznie | Pomieszczenie Urzędu Gminy |
| 3 | Fundusz alimentacyjny | codziennie | oddzielny serwer | automatycznie | Pomieszczenie Urzędu Gminy |
| 4 | Rejestr korespondencji |  | papierowo |  |  |
| 5 | Rejestr wyjść |  | papierowo |  |  |
| 6 | Stypendia szkolne i zasiłki szkolne | codziennie | Oddzielny serwer | automatycznie | Pomieszczenie Urzędu Gminy |
| 7 | Przeciwdziałanie przemocy w rodzinie |  | papierowo |  |  |
| 8 | Karta Dużej Rodziny |  |  |  | Portal internetowywww.kdr.mpips.gov.pl |
| 9 | Wspieranie rodziny i piecza zastępcza |  | papierowo |  |  |
| 10 | Rejestr pracowników zatrudnionych w OPS |  |  |  |  |
| 11 | Przeciwdziałanie uzależnieniom |  | papierowo |  |  |
| 12 | Zbiór danych kontrahentów w OPS zawiera informację o kontrahentach w OPS wartości i przedmiocie umowy |  |  |  |  |
| 13 | Rodzina 500+ | codziennie | oddzielny serwer | automatycznie | Pomieszczenie Urzędu Gminy |

**Załącznik nr 2**

do Instrukcji Zarządzania Systemem Informatycznym

*w Ośrodku Pomocy Społecznej*

LOKALIZACJA STACJI ROBOCZYCH SŁUŻĄCYCH

DO PRZETWARZANIA DANYCH OSOBOWYCH

|  |  |  |
| --- | --- | --- |
| Lp.: | Lokalizacja stacji roboczej: | Zastosowana metoda dostępu: |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Załącznik nr 3**

do Instrukcji Zarządzania Systemem Informatycznym

*w Ośrodku Pomocy Społecznej.*

**EWIDENCJA OSÓB**

zapoznanych z „Instrukcją Zarządzania Systemem Informatycznym”

w Ośrodku Pomocy Społecznej Kobylin-Borzymy

**PRZYJĄŁEM/AM DO WIADOMOŚCI I STOSOWANIA ZAPISY**

**INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwisko i imię | Data i podpis |
| 1 | Sikorska Urszula |  |
| 2 | Kurzyna Małgorzata |  |
| 3 | Choińska Magda |  |
|  |  |  |
|  |  |  |
|  |  |  |