**ZARZĄDZENIE NR 06A/2018**
**KIEROWNIKA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ W POSTOMINIE**
z dnia 25 maja 2018 r.

**w sprawie ustalenia i wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Gminnym Ośrodku Pomocy Społecznej w Postominie oraz Instrukcji zarządzania systemem informatycznym Gminnego Ośrodka Pomocy Społecznej.**

Na podstawie postanowienia 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), zarządzam co następuje:

**§ 1.**

Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Gminnym Ośrodku Pomocy Społecznej w Postominie" w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.

**§ 2.**

Wprowadza się „Instrukcję zarządzania systemem informatycznym w Gminnym Ośrodku Pomocy Społecznej w Postominie" w brzmieniu stanowiącym załącznik Nr 2 do niniejszego zarządzenia.

**§ 3.**

Zobowiązuje się pracowników przetwarzających dane osobowe do przestrzegania reguł zawartych w dokumentach wymienionych w § 1 oraz § 2.

**§ 4.**

Traci moc Zarządzenie Nr 10/2015 Kierownika Gminnego Ośrodka Pomocy Społecznej w Postominie z dnia 09 czerwca 2015r. w sprawie ustalenia i wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Gminnym Ośrodku Pomocy Społecznej w Postominie oraz instrukcji zarządzania systemem informatycznym.

**§ 5.**

Zarządzenie wchodzi w życie z dniem podjęcia.

Kierownik
Gminnego Ośrodka Pomocy
Społecznej w Postominie
Krystyna Ślebioda

Załącznik Nr 1
do Zarządzenia Nr 06A/2018
Kierownika Gminnego Ośrodka
Pomocy Społecznej w Postominie
z dnia 25 maja 2018r.

# Polityka bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Gminnym Ośrodku Pomocy Społecznej w Postominie

## I. Część ogólna

### § 1

Realizując postanowienia 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) ustanawia się „Politykę bezpieczeństwa danych osobowych i danych wrażliwych w Gminnym Ośrodku Pomocy Społecznej w Postominie” , zwaną dalej „Polityką bezpieczeństwa”.

### § 2

Ilekroć w niniejszym dokumencie jest mowa o:

1. Ośrodku - należy przez to rozumieć Gminny Ośrodek Pomocy Społecznej w Postominie;
2. Rozporządzeniu – należy rozumieć 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), o którym mowa §1 niniejszej części;
3. ADO - należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy, Administratorem Danych jest Gminny Ośrodek Pomocy Społecznej w Postominie;
4. IOD – należy przez to rozumieć Inspektora Ochrony Danych;
5. ASI - należy przez to rozumieć Administratora Systemów Informatycznych;
6. Polityka - należy przez to rozumieć „Politykę bezpieczeństwa”, obowiązująca w Gminnym Ośrodku Pomocy Społecznej w Postominie;
7. Instrukcja – należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Postominie;
8. PUODO – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych;
9. Sprawdzenie - należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzanych danych osobowych z przepisami o ochronie danych osobowych;
10. Użytkownik systemu – należy przez to rozumieć osobę upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Ośrodku, osoba wykonująca pracę na podstawie umowy – zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Ośrodku;

11. System informatyczny – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych;
12. Przetwarzanie danych – należy przez to rozumieć 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;;
13. Zabezpieczenie danych w systemie informatycznym – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
14. Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
15. Dane genetyczne - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
16. Dane biometryczne - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne Zgoda na przetwarzanie danych osobowych - należy przez to rozumieć zgodę osoby, której dane dotyczą – rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Wyrażenie zgody na przetwarzanie danych osobowych jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie: odrębnych przepisów prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej) lub innych przesłanek (np. w celu realizacji umowy);
17. Usuwanie danych osobowych - należy przez to rozumieć zniszczenie danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usuwanie danych oznacza, więc takie procedury, których zastosowanie pozbawi administratora danych możliwości jakiegokolwiek dalszego przetwarzania danych osobowych.
18. Strona trzecia - 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;

19. Zgoda - 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;
20. Odbiorca - 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;
21. Profilowanie - 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;
22. Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
23. Naruszenie ochrony danych osobowych - 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;

**§ 3**

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym odpowiadają w Gminnym Ośrodku Pomocy Społecznej w Postominie:

a) Administrator Danych Osobowych,
b) Administrator Systemów Informatycznych,
c) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora Danych Osobowych, na podstawie upoważnienia ADO.

## II. Zasady przetwarzania i ochrony danych osobowych

**§ 1**

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Ośrodku jest zobowiązana do zapoznania się z niniejszym dokumentem.

**§2**

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Ośrodek, przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

**§ 3**

Polityką bezpieczeństwa objęte są dane osobowe, którymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

**§ 4**

Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych obowiązują także w przypadku przetwarzania danych poza zbiorem danych.

**§ 5**

Integralną częścią polityki bezpieczeństwa są niniejsze dokumenty:

1. Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe i dane wrażliwe (Załącznik nr 1);
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (Załącznik nr 2);
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (Załącznik nr 3);
4. Sposób przepływu danych pomiędzy poszczególnymi systemami (Załącznik nr 4);
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (Załącznik nr 5);
6. Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych i danych wrażliwych wynikające z potrzeby zapewnienia ochrony danych osobowych (Załącznik nr 6).

**§ 6**

Osoby, które przetwarzają w Ośrodku dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO (załącznik nr 7) zawierające oświadczenie o zachowaniu poufności tych danych.

Osoby upoważnione do przetwarzania danych mają obowiązek:

a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem,
b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
c) zabezpieczać je przed zniszczeniem,

**§ 7**

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 6, które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni umowę powierzenia (załącznik nr 8).

**§ 8**

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych zgodnie z art. 31 ustawy. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

**§ 9**

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego. Dane osobowe mogą być udostępniane osobom i podmiotom, zgodnie z przepisami prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

**§ 10**

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

a) adresat wniosku (administrator danych),
b) wnioskodawca,
c) podstawa prawna (wskazanie potrzeby),
d) wskazanie przeznaczenia,
e) zakres informacji.

**§ 11**

Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

**§ 12**

Każda osoba fizyczna, której dane są przetwarzane w Ośrodku, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w Art.. 13 - 22 rozporządzenia prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

**§ 13**

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuje odpowiedź niezwłocznie.

**§ 14**

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych Osobowych (lub osoba przez niego wyznaczona) jest obowiązany:

a) podać swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
d) kategorie odnośnych 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 odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

**2.** Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
**a)** okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
**b)** jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
**c)** 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;
**d)** jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
**e)** informacje o prawie wniesienia skargi do organu nadzorczego;
**f)** źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
**g)** informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

**3.** Informacje, o których mowa w ust. 1 i 2, administrator podaje:
**a)** w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – 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 osobą, której dane dotyczą; lub

**c)** jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

**4.** Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

**§ 15**

Nadzór nad przetwarzaniem danych osobowych w Ośrodku sprawuje IOD wyznaczony przez ADO. ADO jest zobowiązany zgłosić do rejestracji GIODO powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od jego powołania lub odwołania.

**§ 16**

Do zadań IOD należy w szczególności:

1. Informowanie 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. Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
4. Współpraca z Prezesem Urzędu Ochrony Danych Osobowych,
5. Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
6. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

**§ 17**

ADO prowadzi również następujące wykazy:

a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 11),
b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1),
c) wykaz zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (załącznik nr 2),
d) wykaz podmiotów i osób, którym udostępniono dane (załączniki nr 12),
e) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 13).

**§18**

Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym sprawuje ASI.

**§19**

Funkcję ASI pełni osoba wyznaczona przez ADO. ADO może każdorazowo odwołać ASI. W przypadku niewyznaczenia osoby na stanowisko ASI obowiązki dla niego przewidziane wykonuje IOD.

**§20**

Do zadań ASI należy w szczególności:

1.Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym;

2.Nadzór nad właściwym zabezpieczeniem sprzętu, w których przetwarzane są dane osobowe;

3.Nadzór nad wykorzystywaniem w Gminnym Ośrodku Pomocy Społecznej w Postominie oprogramowania i jego legalnością;

4.Przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przechowywane są dane osobowe;

5.Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych;

6.Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych;

7.Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych;

8.Nadzór nad wykorzystywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem przydatności;

9. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

## III. Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami

### §1

### Procedura DPIA
### *(Data Protection Impact Assessment)*

1. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych z wykorzystaniem załącznika nr .
2. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana sposobu przetwarzania danych.
3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

### §2

### Procedura analizy ryzyka i plan postępowania z ryzykiem

1. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie z wykorzystaniem załącznika .
2. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
3. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
4. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
5. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr … lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA zgodnie z załącznikiem nr …..

### §3

### Procedura współpracy z podmiotami zewnętrznymi

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem ….
2. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.

**§4**

**Procedura domyślnej ochrony danych**

1. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.
2. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

**§18**

**Procedura zarządzania incydentami**

1. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
3. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, przez zamieszczenie stosownego komunikatu zgodnie z załącznikiem nr … na swojej stronie internetowej .....
4. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.

## IV. Tryb i sposób nadzoru nad dokumentacją przetwarzania danych

**§ 1**

Sprawując nadzór, IOD dokonuje weryfikacji:

a) opracowania i kompletności dokumentacji przetwarzania danych,
b) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa,
c) stanu faktycznego w zakresie przetwarzania danych osobowych,
d) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych,
e) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

**§ 2**

IOD przeprowadza weryfikację:

a) w sprawdzeniach,
b) poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

## V. Instrukcja alarmowa
## (postępowanie w przypadku naruszenia ochrony danych osobowych)

**§1**

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

a) próby naruszenia ochrony danych osobowych:
   - z zewnątrz- włamania do systemu, podsłuch, kradzież danych,
   - z wewnątrz- nieumyślna lub celowa modyfikacja danych, kradzież danych.
b) programy destrukcyjne:
   - wirusy,
   - konie trojańskie,
   - makra,
   - bomby logiczne
c) awarie sprzętu lub oprogramowania,
d) zabór sprzętu lub uszkodzenie oprogramowania,
e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
f) usiłowanie zakłócenia działania systemu informatycznego.

**§2**

W przypadku stwierdzenia faktu nieprawidłowego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieupoważnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik Ośrodka, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa jest zobowiązany fakt ten niezwłocznie zgłosić IOD. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji należy powiadomić osobę przez niego upoważnioną.

**§3**

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych lub danych wrażliwych IOD lub upoważnionej przez niego osoby, należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyny lub sprawców,
b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

c) zaniechać - o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
g) udokumentować wstępnie zaistniałe naruszenie,
h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

**§4**

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych i danych wrażliwych, IOD lub osoba go zastępująca:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO,
d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami z jednostki nadrzędnej (Urząd Gminy) lub pracownikami z firm specjalistycznych.

IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 14, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
b) określenie czasu i miejsca naruszenia i powiadomienia,
c) określenie okoliczności towarzyszących i rodzaju naruszenia,
d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
e) wstępna ocenę przyczyn wystąpienia naruszenia,
f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

**§6**

Raport, o którym mowa w § 5, IOD niezwłocznie przekazuje ADO, a w przypadku jego nieobecności osobie uprawnionej.

## VI. Szkolenie użytkowników

**§1**

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

**§2**

Za przeprowadzenie szkolenia oraz jego zorganizowanie odpowiada IOD.

**§3**

Przeszkolenie odbywa się poprzez zapoznanie użytkowników z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

## VII. Postanowienia końcowe

**§1**

Użytkownicy są obowiązani zapoznać się z treścią polityki oraz do jej stosowania przy przetwarzaniu danych osobowych.

**§2**

Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

**§3**

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszczęć postępowanie dyscyplinarne.

**§ 4**

Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

**§5**

W sprawach nieuregulowanych w niniejszej polityce mają zastosowanie przepisy ustawy oraz wydanej na jej podstawie akty wykonawcze.

**Załącznik Nr 1.1**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

# Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

| Lp | Pomieszczenia, w których przetwarzane są dane osobowe | Jednostka organizacyjna przetwarzająca zbiór | Nazwa zbioru danych osobowych | Uwagi |
|---|---|---|---|---|
| 1 | Pokój nr 1 | Urząd Gminy<br>Postomino<br>Postomino 30<br>76-113 Postomino | Świadczenia rodzinne<br>Fundusz Alimentacyjny/ zaliczka alimentacyjna<br>Pomoc materialna dla uczniów o charakterze socjalnym<br>Dziennik korespondencyjny<br>Karta Dużej Rodziny<br>Świadczenia Wychowawcze | |
| 2 | Pokój nr 5 | Urząd Gminy<br>Postomino<br>Postomino 30<br>76-113 Postomino | Świadczeniobiorcy GOPS<br>Zespół interdyscyplinarny | |
| 3 | Pokój nr 6 | Urząd Gminy<br>Postomino<br>Postomino 30<br>76-113 Postomino | Świadczeniobiorcy GOPS<br>Dziennik korespondencji | |
| 4 | Pokój nr 7 | Urząd Gminy<br>Postomino<br>Postomino 30<br>76-113 Postomino | Świadczeniobiorcy GOPS<br>Zakres danych osobowych uczestników projektu | |
| 5 | Pokój nr 8 | Urząd Gminy<br>Postomino<br>Postomino 30<br>76-113 Postomino | Świadczeniobiorcy GOPS<br>Dodatki mieszkaniowe<br>Dodatki energetyczne | |

**Załącznik Nr 1.2**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

# Wykaz zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

| Lp. | Zbiór danych | Programy zastosowane do przetwarzania/ forma rejestru | Lokalizacja zbioru/ miejsce przetwarzania danych | Osoby upoważnione do przetwarzania danych w zbiorze |
|---|---|---|---|---|
| 1. | Świadczenia rodzinne | Program „Świadczenia rodzinne” | Pokój nr 1 | Marzena Musur<br>Wiesława Pająk<br>Aleksandra Kirschenstein |
| 2. | Fundusz alimentacyjny | Program „Fundusz Alimentacyjny” | Pokój 1 | Marzena Musur<br>Wiesława Pająk<br>Aleksandra Kirschenstein |
| 3. | Pomoc materialna dla uczniów o charakterze socjalnym | „Pomoc materialna dla uczniów o charakterze socjalnym” w formie dokumentu Word | Pokój 1 | Marzena Musur<br>Wiesława Pająk |
| 4. | Świadczeniobiorcy GOPS | nOpieka | Pokój 5, 6, 8 | Grażyna Jędrzejewska<br>Sylwester Pająk<br>Bożena Jarzębska<br>Ewa Borowiec<br>Anita Mikołajczyk |
| 5. | Zakres danych osobowych uczestników projektu | PEFS | Pokój 7 | Monika Górnik-Wojciechowska |
| 6. | Dodatki mieszkaniowe | Program „Dodatki mieszkaniowe” | Pokój 8 | Anita Mikołajczyk |
| 7. | Zespoły interdyscyplinarne | Zespoły interdyscyplinarne w formie dokumentu Word | Pokój 5 | Sylwester Pająk |
| 8. | Dziennik korespondencyjny | Dziennik korespondencji w formie papierowej | Pokój 1, 6, 7, | Marzena Musur<br>Aleksandra Kirschenstein |
| 9. | Dodatki energetyczne | ENERGIA | Pokój 8 | Anita Mikołajczyk |
| 10. | Karta Dużej Rodziny | Karta Dużej Rodziny na platformie P.W.P.W. w Warszawie | Pokój 1 | Marzena Musur |
| 11. | Program Operacyjny Pomoc Żywnościowa 2014-2020 | Załączniki do umowy na realizację programu w formie Word i Excel | Pokój 5, 7 | Grażyna Jędrzejewska<br>Anita Mikołajczyk<br>Sylwester Pająk<br>Bożena Jarzębska |
| 12. | Zachodniopomorska Karta Rodziny | Załączniki do umowy na realizację | Pokój 7 | Aleksandra Kirschenstein |

| | | | | |
|---|---|---|---|---|
| | | programu w formie Word | | |
| 13. | Zachodniopomorska Karta Seniora | Załączniki do umowy na realizację programu w formie Word | Pokój 7 | Aleksandra Kirschenstein |
| 14. | SEPI- na podstawie umowy powierzenia danych do przetwarzania danych osobowych | SEPI- System Sygnity S.A. | Pokój 1,5, | Sylwester Pająk Marzena Musur |
| 15. | Świadczenia wychowawcze | Rodzina 500+ moduł do aplikacji Świadczenia rodzinne | Pokój 1 | Marzena Musur Wiesława Pająk Aleksandra Kirschenstein |
| 16. | Regionalny Program Operacyjny Województwa Zachodniopomorskiego 2014-2020 | Załączniki do umowy na realizację programu w formie Word, SL2014 | Pokój 7 | Monika Górnik-Wojciechowska |

**Załącznik Nr 1.3**
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej w Postominie

# Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

| Lp. | Nazwa zbioru danych | Określenie zakresu danych (nazwa tablicy) | Programy służące do przetwarzania/ forma rejestru | Uwagi |
|---|---|---|---|---|
| 1. | Świadczenia rodzinne/ Świadczenia wychowawcze | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, seria i numer dowodu osobistego, numer telefonu, stan cywilny, obywatelstwo, stopień niepełnosprawności, wysokość dochodów, stan rodzinny, stan zdrowia, | Program „Świadczenia rodzinne”/ Rodzina 500+ | |
| 2. | Fundusz alimentacyjny | nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, stan cywilny, obywatelstwo, stopień niepełnosprawności, wysokość dochodów, stan rodzinny, stan zdrowia, skazania, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym, | Program „Fundusz Alimentacyjny” | |
| 3. | Pomoc materialna dla uczniów o charakterze socjalnym | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, seria i numer dowodu osobistego, stan cywilny, obywatelstwo, stopień niepełnosprawności, wysokość dochodów, stan rodzinny, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym, miejsce nauki, imiona i nazwiska rodziców (opiekunów prawnych), rodzaj świadczenia o jakie ubiega się wnioskodawca, dane uzasadniające przyznanie pomocy, wysokość dochodów, informacja o korzystaniu z pomocy OPS, informacja o alimentach, ciężka choroba, niepełnosprawność, leczenie szpitalne, potwierdzenie zdarzenia losowego, nr rachunku bankowego, ilość ha prowadzonego gospodarstwa rolnego lub aktualny nakaz płatniczy, uzależnienia, dowody opłacenia składek ZUS, podatku, informacja o wychowywaniu w rodzinie niepełnej | „Pomoc materialna dla uczniów o charakterze socjalnym” w formie dokumentu Word | |
| 4. | Świadczeniobiorcy GOPS | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, płeć, stan cywilny, stopień pokrewieństwa, obywatelstwo, stopień niepełnosprawności, wysokość dochodów, zobowiązania alimentacyjne, sytuacja majątkowa, stan zdrowia, nałogi, inne orzeczenia wydane w postępowaniu sadowym lub administracyjnym | Program „nOpieka” | |

| | | | | |
|---|---|---|---|---|
| 5. | Zakres danych osobowych uczestników projektu | nazwisko i imię, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, numer telefonu, pochodzenie etniczne, płeć, wiek w chwili przystąpienia do projektu, opieka nad dziećmi do lat 7 lub osobą zależną, adres poczty elektronicznej, status na rynku pracy, rodzaj przyznanego wsparcia, osoba niepełnosprawna, migrant, stan zdrowia **oraz dane zgodne ze zbiorem projekty RPO WZ 2014-2020 w załączeniu** | PEFS | |
| 6. | Dodatki mieszkaniowe | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, seria i numer dowodu osobistego, stan Cywiny, wysokość uzyskiwanych dochodów, koszt utrzymania lokalu | Program „Dodatki mieszkaniowe” | |
| 7. | Zespoły interdyscyplinarne | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, przekonania religijne, przekonania filozoficzne, przynależność wyznaniową, stan zdrowia, nałogi, życie seksualne, skazania, mandaty karne, orzeczenia o ukaraniu, inne orzeczenia wydane w postępowaniach sądowych lub administracyjnych | Zespoły interdyscyplinarne w formie dokumentu Word | |
| 8. | Dziennik korespondencyjny | nazwiska i imiona, adres zamieszkania | Dziennik korespondencyjny w formie papierowej | |
| 9. | Dodatki energetyczne | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, seria i numer dowodu osobistego, stan cywilny, wysokość uzyskiwanych dochodów, koszt utrzymania lokalu | ENERGIA | |
| 10. | Karta Dużej Rodziny | imię i nazwisko, PESEL, data urodzenia, adres zamieszkania (wnioskodawcy) imię i nazwisko, PESEL, data urodzenia, adres zamieszkania, stopień niepełnosprawności (członkowie rodziny) | Karta Dużej Rodziny na platformie P.W.P.W. w Warszawie | |

W załączeniu:

1. opis struktur tabel systemów „nOpieka”, „Świadczenia rodzinne”, „Fundusz Alimentacyjny” „Dodatki mieszkaniowe” „PEFS”, „ENERGIA”, Karta Dużej Rodziny
2. użytkownicy systemów „nOpieka”, „Świadczenia rodzinne”, „Fundusz Alimentacyjny”, „Dodatki Mieszkaniowe” „PEFS”, „ENERGIA”, Karta Dużej Rodziny
3. zakres danych osobowych – Zbiór Projekty RPO WZ 2014 – 2020.

**Załącznik Nr 1.4**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

## Przepływ danych pomiędzy systemami

1. Systemy, w których przetwarzane są dane osobowe są niezależne i posiadają samodzielne bazy danych.

**Załącznik Nr 1.5**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

## Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

**§ 1**

Dane osobowe z użyciem systemu informatycznego i w formie papierowej są przetwarzane w godzinach pracy Gminnego Ośrodka Pomocy Społecznej w Postominie. Poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu zgody administratora danych i powiadomieniu administratora bezpieczeństwa informacji.

**§ 2**

W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby zainteresowane przetwarzanymi danymi, Inspektor Ochrony Danych, Administrator Systemu Informatycznego oraz inne osoby indywidualnie upoważnione do tego przez Administratora Danych Osobowych. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

**§ 3**

Pomieszczenia w obszarze przetwarzania danych osobowych są zamykane na zamek w czasie nieobecności pracowników. Klucze są przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione do przetwarzania danych osobowych.

**§ 4**

Dokumenty papierowe przechowywane są w szafach zamykanych na klucz. Przechowywane są zgodnie z Instrukcją kancelaryjną. Klucze do szaf z dokumentami przechowują osoby upoważnione do przetwarzania danych osobowych

**§ 5**

Monitory komputerów, na których odbywa się przetwarzanie danych osobowych w sposób informatyczny są zlokalizowane w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych. Konfiguracja wyświetlania obrazu na monitorach komputerów musi zawierać włączenie wygaszacza ekranu po zadanym czasie (5 minut) lub w przypadku braku wygaszacza ekranu wyłączenie monitora w przypadku braku aktywności użytkownika (5 minut). Zaleca się, aby powrót do pracy po okresie bezczynności wymagał podania hasła dostępu (np. hasło wygaszacza ekranu).

**§ 6**

Dyski HDD i inne nośniki elektroniczne zawierające dane osobowe z przeznaczone do likwidacji, naprawy są przed opuszczeniem Gminnego Ośrodka Pomocy Społecznej w Postominie pozbawiane zapisu lub niszczone fizycznie (jeżeli nie ma innej metody zlikwidowania zapisu).

**§ 7**

Sieć komputerowa Gminnego Ośrodka Pomocy Społecznej w Postominie podłączona jest do własnej sieci Internetu Urzędu Gminy Postomino oraz zapasowego łącza Firmy ORANGE. Dostęp do zasobów sieci Internet posiadają tylko osoby, którym jest to konieczne do wykonywania obowiązków służbowych.

**§ 8**

Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji są niszczone w sposób bezpowrotny tak, aby nie było możliwości odczytania zamieszczonych na nich informacji poprzez zniszczenie w niszczarce.

**§ 9**

W celu ochrony antywirusowej stosuje się oprogramowanie antywirusowe z codzienną aktualizacją baz wirusów.

**Załącznik Nr 1.6**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

# Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych wynikające z przyczyn zapewnienia ochrony danych osobowych

**§ 1**

Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do zbiorów danych osobowych.

**§ 2**

Naruszenie zasad ochrony danych osobowych, w szczególności umyślne lub nieumyślne udostępnianie danych osobowych osobie nieupoważnionej, jest naruszeniem obowiązków pracowniczych. W tym przypadku zastosowanie maja przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000)

**§ 3**

Kierownik Gminnego Ośrodka Pomocy Społecznej w Postominie zobowiązany jest do:

1. Kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników;
2. Zapewnienia, że przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych w zakresie indywidualnych obowiązków pracowniczych.

**§ 4**

Osoba upoważniona przez Administratora Danych Osobowych jest zobowiązana do:

1. zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;
2. stosowania określonych przez administratora danych procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
3. zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych;
4. przestrzegania ustalonych zasad i procedur w zakresie ochrony danych osobowych.

**Załącznik Nr 1.7**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

Postomino, dn. ..... 20..... r.

**UPOWAŻNIENIE NR ……**
**DO PRZETWARZANIA DANYCH OSOBOWYCH W GMINNYM OŚRODKU POMOCY SPOŁECZNEJ W POSTOMINIE**

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) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** − nadaję upoważnienie Pani/Panu:

…….
*(imię i nazwisko)*

……..
*(stanowisko)*

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.
Upoważnienie obejmuje uprawnienie do przetwarzania danych:
.....
Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2018 poz. 1000), innych aktami prawnymi, a także z Polityką ochrony danych osobowych.
Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Gminnym Ośrodku Pomocy Społecznej w Postominie.
Okres ważności
od:
do:

.....
**podpis Kierownika**

Data wygaśnięcia ……..……..

Odwołano, dnia …….

**Załącznik Nr 1.8**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

# OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Gminnego Ośrodka Pomocy Społecznej w Postominie.

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami 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

……

Data i podpis osoby składającej oświadczenie

**Załącznik Nr 1.9**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

WZÓR REJESTRU ZBIORÓW DANYCH OSOBOWYCH

| | |
|---|---|
| Nazwa zbioru danych | |
| Oznaczenie administratora danych i adres jego siedziby | |
| Oznaczenie przedstawiciela danych osobowych, o którym mowa w art. 31a ustawy, adres jego siedziby lub miejsca zamieszkania- w przypadku wyznaczenia takiego podmiotu | |
| Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy, i jego adres siedziby lub miejsca zamieszkania- w przypadku powierzenia przetwarzania danych temu podmiotowi | |
| Podstawa prawna upoważniająca do prowadzenia zbioru danych | |
| Cel przetwarzania danych w zbiorze | |
| Opis kategorii osób, których dane są przetwarzane w zbiorze | |
| Zakres danych przetwarzanych w zbiorze | |
| Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą | |
| Sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż uprawnione na podstawie przepisów prawa | |
| Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane | |
| Informacja dotycząc ewentualnego przekazywania danych do państw trzecich | |
| Data wpisu zbioru do rejestru | |
| Data ostatniej aktualizacji | |

HISTORIA ZMIAN W ZBIORZE

| | |
|---|---|
| Informacja o rodzaju zmiany (nowy wpis, aktualizacja wykreślenie) | |
| Data dokonania zmian | |
| Informacja o zakresie zmian | |

**Załącznik Nr 1.10**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

# EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

| L.p. | Imię i Nazwisko | Stanowisko/komórka organizacyjna | Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem numer do Polityki Bezpieczeństwa)* | Data nadania upoważnienia | Data ustania upoważnienia | Identyfikator/Login w danym systemie informatycznym |
|---|---|---|---|---|---|---|
| **1.** | | | | | | |
| **2.** | | | | | | |
| **3.** | | | | | | |
| **4.** | | | | | | |
| **5.** | | | | | | |
| **6.** | | | | | | |
| **7.** | | | | | | |

**Załącznik Nr 1.11**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

## WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

| **L.p.** | **Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)* | **Data udostępnienia** | **Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)* | **Cel udostępnienia** *(podstawa prawna/numer umowy)* | **Zakres udostępnionych danych** *(jakie dane zostały udostępnione)* | **Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)* |
|---|---|---|---|---|---|---|
| **1.** | | | | | | |
| **2.** | | | | | | |
| **3.** | | | | | | |
| **4.** | | | | | | |
| **5.** | | | | | | |
| **6.** | | | | | | |
| **7.** | | | | | | |
| **8.** | | | | | | |

**Załącznik Nr 1.12**
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Ośrodku Pomocy Społecznej
w Postominie

## WYKAZ PODMIOTÓW KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

| L.p. | Nazwa podmiotu, któremu powierzono dane | Data powierzenia | Cel powierzenia oraz numer umowy powierzenia | Zakres powierzonych danych *(jakie dane zostały powierzone)* | Określenie zbioru/zasobu |
|---|---|---|---|---|---|
| **1.** | | | | | |
| **2.** | | | | | |
| **3.** | | | | | |
| **4.** | | | | | |
| **5.** | | | | | |
| **6.** | | | | | |
| **7.** | | | | | |

**Załącznik Nr 1.13**
do Polityki bezpieczeństwa przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Postominie

# RAPORT
## z naruszenia bezpieczeństwa systemu informatycznego w Gminnym Ośrodku Pomocy Społecznej w Postominie

1. Data: …… Godzina: ……..
(dd.mm.rr.) (gg.mm.)

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

2. Lokalizacja zdarzenia:

……
(np. nr pokoju, nazwa pomieszczenia)

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……
……
……
……

4. Przyczyna wystąpienia zdarzenia:
……
……
……
……
……

5. Podjęte działania:
……
……
……

6. Postępowanie wyjaśniające:
……
……
……..

……..
(data, podpis Inspektora Ochrony Danych)

**Załącznik Nr 2**
do Zarządzenia Nr 06A/2018
Kierownika Gminnego Ośrodka
Pomocy Społecznej w Postominie
z dnia 25 maja 2018r.

# Instrukcja zarządzania systemem informatycznym Gminnego Ośrodka Pomocy Społecznej w Postominie

## I. Część ogólna

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

**§ 1**

1) Instrukcja zarządzania systemem informatycznym Gminnego Ośrodka Pomocy Społecznej w Postominie, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.
2) Niniejsza Instrukcja realizuje „Politykę bezpieczeństwa przetwarzania danych osobowych" obowiązującą w Gminnym Ośrodku Pomocy Społecznej w Postominie.

**§ 2**

Ilekroć w niniejszym dokumencie jest mowa o:

1) Ośrodku - należy przez to rozumieć Gminny Ośrodek Pomocy Społecznej w Postominie.
2) Rozporządzeniu – należy przez to rozumieć 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
3) ADO - należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy, Administratorem Danych jest Gminny Ośrodek Pomocy Społecznej w Postominie. W imieniu Administratora Danych obowiązki określone w Ustawie pełni Kierownik Ośrodka.
4) IOD- należy przez to rozumieć Inspektora Ochrony Danych w rozumieniu Rozporządzenia.
5) ASI - należy przez to rozumieć Administratora Systemów Informatycznych.
6) Polityka – należy przez to rozumieć „Politykę bezpieczeństwa", obowiązująca w Gminnym Ośrodku Pomocy Społecznej w Postominie.
7) Instrukcja – należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Postominie.

8) PUODO- należy przez to rozumieć PUODO – Prezesa Urzędu Ochrony Danych Osobowych.
9) Incydent - należy przez to rozumieć naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
10) Użytkownik systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Ośrodku, osoba wykonująca pracę na podstawie umowy – zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Ośrodku.
11) Identyfikator użytkownika – należy przez to rozumieć ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
12) Sieć lokalna – należy przez to rozumieć połączenie komputerów pracujących w Ośrodku, w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
13) Sieć publiczna – należy przez to rozumieć sieć telekomunikacyjna, niebędąca siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych, w rozumieniu ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz. U. z 2016 poz. 1489 ze zm.).
14) Sieć telekomunikacyjna – należy przez top rozumieć urządzenia telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną, w rozumieniu ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz. U. z 2016 poz. 1489 ze zm.).System informatyczny – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych.
15) Słabość systemu- należy przez to rozumieć zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.
16) Działanie korygujące- należy przez to rozumieć działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności/ incydentu lub innej potencjalnej sytuacji.
17) Działanie zapobiegawcze - należy przez to rozumieć działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnych niezgodności/ incydentów lub innej potencjalnej sytuacji niepożądanej.
18) Przetwarzanie danych – należy przez to rozumieć 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;
19) Zabezpieczenie danych w systemie informatycznym – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
20) Teletransmisja – należy przez to rozumieć przesyłanie informacji za pomocą sieci telekomunikacyjnej.

21) Aplikacja – należy przez to rozumieć program komputerowy, wykonujący konkretne zadanie.
22) Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
23) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
24) Tożsamość – oznacza cechy, które stanowią o tym, kim dana osoba jest, czym różni się od innych. Na tak rozumianą tożsamość składa się nie tylko to, kim się jest obecnie, ale także to, kim się było, a nawet zamierzenia na przyszłość, wszystko to powoduje, że dana osoba różni się od innej.
25) Zgoda na przetwarzanie danych osobowych - należy przez to rozumieć zgodę osoby, której dane dotyczą – rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Wyrażenie zgody na przetwarzanie danych osobowych jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie: odrębnych przepisów prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej) lub innych przesłanek (np. w celu realizacji umowy).
26) Usuwanie danych osobowych – należy przez to rozumieć zniszczenie danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usuwanie danych oznacza, więc takie procedury, których zastosowanie pozbawi administratora danych możliwości jakiegokolwiek dalszego przetwarzania danych osobowych.
27) Korekcja - należy przez to rozumieć działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
28) Kontrola (audyt) - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.

**§ 3**

ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni IOD lub osoba pełniąca funkcję IOD. Wzór upoważnienia ASI stanowi załącznik nr 2.1 do niniejszego dokumentu. ASI jest również

zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 8 do Polityki Bezpieczeństwa.

**§ 4**

ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego. Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

**§ 5**

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w jednostce organizacyjnej system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

## II. Część szczegółowa

**§ 1**

Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

- rozporządzeniem,
- polityką,
- niniejszym dokumentem,

oraz posiadać upoważnienie do przetwarzania danych osobowych. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik Nr 2.2.

**§ 2**

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:

1) użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 7 do Polityki, oraz podpisaniu oświadczenia stanowiącego załącznik nr 8 do Polityki, składa wniosek o nadanie dostępu do systemu informatycznego stanowiącego załącznik nr 2.3,
2) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 7 do Polityki Bezpieczeństwa, ASI zobowiązany jest do dopełnienia czynności

uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły,

3) przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakres dostępu danych i operacji,
4) ASI zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

**§ 3**

Stosuje się następujące metody oraz środki uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem:

1) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI,
2) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 30 dni,
3) przy wyborze hasła obowiązują następujące zasady:
    a) minimalna długość hasła 8 znaków,
    b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL, itp.),
    c) należy stosować: hasła zawierające kombinacje liter i cyfr, hasła zawierające znaki specjalne (.,():'@,#,& itp.) o ile system informatyczny i oprogramowanie na to pozwala,
    d) zmiany hasła nie wolno zlecać innym osobom.
4) użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich,
5) pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony,
6) pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7) odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika GOPS z podaniem daty oraz przyczyny odebrania uprawnień,
8) Kierownik GOPS zobowiązany jest pisemnie informować IOD o każdej zmianie dotyczącej pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
9) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło,
10) identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.

11) hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
12) ASI zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. Rejestr stanowi załącznik Nr 2.4.

**§ 5**

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1) rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu,
2) przed opuszczeniem stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego,
3) system jest skonfigurowany w taki sposób, aby po okresie 10 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu hasła,
4) przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu,
5) niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

**§ 6**

Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1) za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ASI,
2) kopie bezpieczeństwa wykonywane są codziennie,
3) kopie bezpieczeństwa wykonywane są na serwerze głównym GOPS.

**§ 7**

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków:

1) Elektroniczne nośniki informacji:
   a) dane osobowe w postaci elektronicznej – za wyjątkiem kopii bezpieczeństwa – zapisane na płytach CD/DVD czy dyskietkach twardych nie mogą opuścić obszaru przetwarzania danych osobowych,
   b) elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych, w zamkniętych szafach,
   c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny,

d) elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika,
e) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2) Kopie zapasowe:
   a) kopie bezpieczeństwa są przechowywane na serwerze GOPS w budynku Urzędu Gminy w Postominie,
   b) dostęp do danych opisanych w punkcie 1 ma ASI oraz upoważnieni pracownicy.
3) Wydruki:
   a) w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym,
   b) pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy,
   c) wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

**§ 8**

System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania, o jakim mowa w lit. a niniejszego paragrafu:

a) oprogramowaniem antywirusowym stosowanym w Ośrodku jest ESET NOD32 Antivirus Business Edittion,
b) użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI
c) za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w lit. a oraz oprogramowania firewall, określonego w lit. b niniejszego paragrafu, odpowiada ASI

**§ 9**

Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

a) ASI w terminach określonych przez producenta sprzętu wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji;
b) w przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w lit. a niniejszego paragrafu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania;

c) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej;
d) o fakcie ujawnienia nieprawidłowości należy zawiadomić ASI;
e) konserwacja baz danych osobowych przeprowadzona jest zgodnie z zaleceniami twórców poszczególnych programów;
f) ASI zobowiązany jest uaktywnić mechanizm zaliczania nieudanych prób dostępu do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.

**§ 10**

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie:

1) urządzeń UPS,
2) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami.

**§ 11**

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) przekazanie podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych,
3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

**§ 12**

W przypadku jakichkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić bezpośredniego przełożonego, który zawiadamia IOD w celu:

1) W przypadku włamania lub podejrzenia włamania do systemu administrator danego systemu podejmuje działania w celu zabezpieczenia systemu i danych:
   a) zmienia hasło administracyjne,
   b) określa rodzaj i sposób włamania,
   c) podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
   d) szacuje straty w systemie,
   e) przywraca stan systemu przed włamaniem.
2) W przypadku uszkodzenia sprzętu lub programów z danymi administrator danego systemu podejmuje działania w celu:
   a) określenie przyczyn uszkodzenia,

b) oszacowanie strat wynikłych z w/w uszkodzenia,
c) naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytanie danych z ostatniej kopii zapasowej.

3) W przypadku uszkodzenia danych administrator systemu podejmuje następujące działania:
   a) ustala przyczynę uszkodzenia danych,
   b) określa wielkość i jakość uszkodzonych danych,
   c) podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

**§ 13**

W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić administratora sieci, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

**§ 14**

Wszystkie działania konserwacyjne, awarie oraz napraw powinny być rejestrowane w prowadzonym „Dzienniku systemu informatycznego GOPS". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku Nr 2.5. Wpisów do dziennika może dokonywać Administrator Danych Osobowych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

## III. Postanowienia końcowe

**§ 1**

W sprawach nieuregulowanych niniejszą Instrukcją znajdują zastosowanie przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

**Załącznik Nr 2.1**
do Instrukcji zarządzania systemem informatycznym
w Gminnym Ośrodku Pomocy Społecznej w Postominie

.....
*miejscowość, data*

**UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)**

Na podstawie części I §3 Instrukcji Zarządzania Systemem Informatycznym, z dniem ..... wyznaczam Administratora Systemu Informatycznego (ASI), powierzając tę funkcję Panu/Pani ..... posługującemu/-ej się numerem PESEL: .....

.....

podpis Administratora Bezpieczeństwa Informacji
lub Administratora Danych Osobowych

---

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ze szczególnym uwzględnieniem obowiązków przewidzianych w części I § 4 Instrukcji Zarządzania Systemem Informatycznym.

.....

podpis Administratora Systemu Informatycznego (ASI)

**Załącznik Nr 2.2**
do Instrukcji zarządzania systemem informatycznym
w Gminnym Ośrodku Pomocy Społecznej w Postominie

# Oświadczenie

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. 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
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100 poz. 1024),
3. Polityki bezpieczeństwa przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Postominie,
4. Instrukcji zarządzania systemem informatycznym Gminnego Ośrodka Pomocy Społecznej w Postominie.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

1. Zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Gminnego Ośrodka Pomocy Społecznej w Postominie, zabezpieczenia przed udostępnieniem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
2. Zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.

Postomino, dn. …….  …….
(podpis pracownika)

**Załącznik Nr 2. 3**
do Instrukcji zarządzania systemem informatycznym
w Gminnym Ośrodku Pomocy Społecznej w Postominie

# Wniosek o nadanie uprawnień w systemie informatycznym

Rodzaj zmiany w systemie informatycznym:

☐ Nowy użytkownik ☐ Modyfikacja uprawnień ☐ Odebranie uprawnień

| | |
|---|---|
| Imię i nazwisko użytkownika | |
| Opis zakresu uprawnień użytkownika w systemie informatycznym | |

Data wystawienia: ……..

…… (podpis Kierownika GOPS)

……. (Akceptacja ABI)

**Załącznik Nr 2.4**
do Instrukcji zarządzania systemem informatycznym
w Gminnym Ośrodku Pomocy Społecznej w Postominie

# Ewidencja osób upoważnionych do pracy w systemie informatycznym oraz upoważnionych do przetwarzania danych osobowych

| Lp. | Nazwisko i imię (Identyfikator) | System/aplikacja/zbiór danych osobowych | Data nadania upoważnienia | Data ustania upoważnienia |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Załącznik Nr 2.5**
do Instrukcji zarządzania systemem informatycznym
w Gminnym Ośrodku Pomocy Społecznej w Postominie

# Dziennik systemu informatycznego
# Gminnego Ośrodka Pomocy Społecznej w Postominie

Dziennik zawiera opis wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- w przypadku awarii – opis awarii, przyczynę awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

| Lp. | Data i godzina zdarzenie | Opis zdarzenia | Podjęte działania | Podpis |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |