Załącznik Nr 1 do Zarządzenia Nr 14/2018
Kierownika Gminnego Ośrodka Pomocy Społecznej w Raszynie
z dnia 25 maja 2018r.

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

I- Część ogólna

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

1. „Dane osobowe" – oznacza informacje o zidentyfikowanej lub możliwej do identyfikacji 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 badź kilka szczególnych czynników określajacych fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczna, kulturową lub społeczna tożsamość osoby fizycznej;

2. „Zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych wg określonych kryteriów, niezaleznie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

3. „Przetwarzanie" – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

4. „Administrator" oznacza to osobę fizyczną, organ publiczny, jednostkę lub inny podmiot który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, jeżeli cele i sposoby takiego przetwarzania są określone w prawie;

5. „Podmiot przetwarzajacy" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

6. „Strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzajacy, czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

7. „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 dotyczacych jej danych osobowych;

8. „Naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzace do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostepu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

9. „Dane zwykłe”- pojęcie to obejmuje dane osobowe, których nie zalicza się do danych wrażliwych. Zalicza się do nich np. imię, nazwisko, adres zamieszkania, adres poczty elektronicznej, nr PESEL, stan zadłużenia, wizerunek, adres IP.

10. „Dane wrażliwe” – dane szczególnie chronione- pochodzenie rasowe, etniczne, poglądy polityczne,światopoglad, przynalezność do związków zawodowych, dotyczace stanu zdrowia, dane genetyczne, biometryczne, orientacji seksualnej, stanu zdrowia, przetwarzanie danych dotyczących wyroków skazujacych oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, rejestry wyroków skazujących.

11. „Ośrodku” - należy przez to rozumieć Gminny Ośrodek Pomocy Społecznej w Raszynie,

12. „Administrator” - należy przez to rozumieć organ publiczny który ustala cele i sposoby przetwarzania danych osobowych.

13. IOD- należy przez to rozumieć Inspektora ochrony danych osobowych,

14. RPE – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporzadzenie o ochronie danych);

15. Polityka – należy przez to rozumieć „Politykę bezpieczeństwa”, obowiązującą w Gminnym Ośrodku Pomocy Społecznej w Raszynie;

16. Instrukcja – należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym”, służącym do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Raszynie;

17. Organ nadzorczy- należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych,

18. „Odbiorca” oznacza osobe 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 nie są jednak uznawane za odbiorców.

19. System informatyczny – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych;

20. Zabezpieczenie danych w systemie informatycznym – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

§ 2

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RPE, Polityką Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym odpowiadają w Gminnym Ośrodku Pomocy Społecznej w Raszynie:

a) Administrator,
b) Inspektor Ochrony Danych,
c) Pracownicy przetwarzający,
d) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora, która uzyskała upoważnienie do przetwarzania danych osobowych.

II- Zasady przetwarzania danych osobowych

Dane osobowe

§ 3

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

§ 4

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

§ 5

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

§ 6

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.

§ 7

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).

§ 8

Osoby, które przetwarzają w Ośrodku dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora danych (Załącznik nr 7) wraz z oświadczeniem o zachowaniu poufności tych danych (Załącznik nr 12).
Osoby upoważnione do przetwarzania danych mają obowiązek:
a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z RPE,
b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
c) zabezpieczać je przed zniszczeniem.

§ 9

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych zgodnie z art. 28 RPE.

§ 10

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.

§ 11

1. Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
− adresat wniosku (administrator danych),
− wnioskodawca,
− podstawa prawna (wskazanie potrzeby),
− wskazanie przeznaczenia,
− zakres informacji.
2. Udostępnienie danych osobowych drogą internetową może nastąpić po ich zaszyfrowaniu.

§ 12

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

§ 13

W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator jest obowiązany poinformować tę osobę o:
- adresie swojej siedziby i pełnej nazwie,
- informację o danych osobowych i adresie, kontakcie telefonicznym i poczty elektronicznej IOD
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych
- okresie przechowywania danych,
- uprawnieniach osoby której dane dotyczą
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. (Załącznik nr 13)

§ 14

Uprawnienia osób których dane dotyczą:
1. prawo do bycia poinformowanym art. 13 RPE

2. prawa dostępu do danych osobowych art. 15 RPE,
3. prawo do sprostowania art.16 RPE
4. prawo do ograniczenia przetwarzania (oznacza to takie oznaczenie przechowywanych danych aby ograniczyć ich przyszłe przetwarzanie) art. 18 RPE,
5. prawo do przenoszenia danych art. 20 RPE,
6. prawo do sprzeciwu – może być złożone w każdym momencie przez osobę której dane dotyczą z przyczyn zwiazanych z jej szczególna sytuacją. Po złożeniu sprzeciwu dane nie mogą być dalej przetwarzane, art. 21 RPE
7. prawo do tego, by nie podlegać profilowaniu art. 22 RPE.

III Administrator i Inspektor danych osobowych`

§ 15

Obowiazkiem Administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zabezpiecznia ochrony danych osobowych przetwarzanych w Ośrodku, oraz ich uaktualnianie.
Administrator prowadzi następujące wykazy:
a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 10);
b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1);
c prowadzenie rejestru zbiorów danych przetwarzanych przez Ośrodek (Załącznik nr 9)
d) rejestr zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (załącznik nr 2);
e) wykaz podmiotów i osób, którym udostępniono dane (załącznik nr 11).

§ 16

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

§ 17

1. Nadzór nad przetwarzaniem danych osobowych w Ośrodku sprawuje IOD wyznaczony przez Administratora. Administrator jest zobowiązany zgłosić do organu nadzorczego powołanie i odwołanie IOD w terminie 14 dni od jego powołania lub odwołania. Upoważnienie wyznaczające IOD stanowi załącznik nr 8 do niniejszego dokumentu. IOD jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik do niniejszego dokumentu.
2. Administrator przy wyznaczaniu inspektora ma kierować się jego kwalifikacjami zawodowymi oraz wiedzą specjalistyczną z zakresu prawa ochrony danych, praktyką i zdolnością do wykonywania zadań.
3. Administrator danych jest zobowiazqany do włączania IOD w sposób terminowy i właściwy we wszystkie kwestie dotyczace ochrony danych osobowych w Ośrodku. IOD będzie wykonywał swoje obowiazki i zadania niezależnie oraz nie będzie otrzymywał od Administratora żadnych poleceń dotyczacych pełnienia swojej funkcji.
4. IOD wypełnia swoje zadania z należytym uwzglednieniem ryzyka związanego z operacjami przetwarzania, majac na uwadze charakter, zakres, kontekst i cele przetwarzania.
5. IOD podlega bezpośrednio Administratorowi.

§ 18

Do zadań IOD należy w szczególności:
a) informowanie administratora, podmiotu przetwarzajacego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RPE i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania RPE, polityki bezpieczeństwa GOPS, prowadzenie działań zwiększajacych świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania, prowadzenie audytu;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RPE;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RPE.

IV- Postępowanie w przypadku naruszenia ochrony danych osobowych.

§ 19

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.

§ 20

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 Administratorowi.

§ 21

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych lub danych wrażliwych Administrator 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 (załącznik nr 2 do Instrukcji),
h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IODO lub osoby upoważnionej.

§ 22

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych i danych wrażliwych, IODO 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 Administratora,
d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami z jednostki nadrzędnej (Urząd Gminy) lub pracownikami z firm specjalistycznych.
e) Obowiązek nie powstaje w przypadku, kiedy istnieje małe prawdopodobieństwo, że incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 23

Administrator dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2 do Instrukcji, 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.

§ 24

Pracownik ma obowiązek poinformować o naruszeniu Administratora i IOD w terminie 24 godzin.

§ 25

W przypadku kiedy Administrator oceni, że nastąpiło naruszenie praw lub wolności osób fizycznych, w terminie 72 godzin po stwierdzeniu naruszenia przekazuje informację IOD oraz organowi nadzorczemu o naruszeniu oraz wszystkim osobom których naruszenie danych dotyczy.

V- Postanowienia końcowe

§ 26

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

§ 27

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

§ 28

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 wszcząć postępowanie dyscyplinarne.

§ 29

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.

§ 30

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