Zarządzenie Nr 13/2018
Kierownika Ośrodka Pomocy Społecznej w Górze Kalwarii
z dnia 28.08.2018 r.

w sprawie wprowadzenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Górze Kalwarii

Na podstawie art. 24 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 zarządza się, co następuje:

§ 1

Wprowadza się instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Górze Kalwarii, zwaną dalej „instrukcją zarządzania systemem informatycznym", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Ośrodka Pomocy Społecznej w Górze Kalwarii do stosowania zasad określonych w instrukcji zarządzania systemem informatycznym.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4

Traci moc zarządzenie Kierownika Ośrodka Pomocy Społecznej w Górze Kalwarii nr 1/2015 z dnia 31.03.2015 r.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania

Kierownik
Ośrodka Pomocy Społecznej
w Górze Kalwarii

mgr Katarzyna Łagowska

ZATWIERDZAM

Egz. nr. 2

.....Kierownik Ośrodka Pomocy Społecznej w Górze Kalwarii

mgr Katarzyna Łagowska

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

OŚRODKA POMOCY SPOŁECZNEJ

GÓRA KALWARIA

Góra Kalwaria sierpień 2018 r.

SPIS TREŚCI

Strona

ROZDZIAŁ I

Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej "Instrukcją", jest uzupełnieniem Polityki bezpieczeństwa i określa sposób zarządzania systemem informatycznym, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.

2. Instrukcja została opracowana zgodnie z wymogami 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. Znaczenie pojęć użytych w instrukcji wyjaśniono w rozdziale I Polityki bezpieczeństwa.

ROZDZIAŁ II

Procedury nadawania uprawnień do przetwarzania danych

1. Uprawnienia do przetwarzania danych osobowych nadaje Kierownik Ośrodka Pomocy Społecznej, poprzez wydanie stosownego upoważnienia. Wzór upoważnienia stanowi załącznik nr 1 do niniejszej Instrukcji.

2. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 3 do niniejszej Instrukcji. Ewidencja podlega bieżącej aktualizacji.

3. Ewidencja zawiera:

1) imię i nazwisko użytkownika,

2) numer upoważnienia,

10. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

11. Hasła muszą odpowiadać następującym wymogom:

l) hasła składają się co najmniej z:

a) dla poziomu bezpieczeństwa podstawowego 6 znaków,

b) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków, i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

2) nie mogą być zapisywane w systemie w postaci jawnej,

3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne, kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

12. Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

13. Hasła me mogą być nigdzie zapisywane, z wyjątkiem haseł Informatyka, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Danych. Koperta złożona jest w zamkniętej szafie, do której dostęp posiada wyłącznie Kierownik i osoby przez niego upoważnione.

14. Hasła informatyka zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez nieupoważnioną osobę. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w ust. 13.

15. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów. Niszczenia dokonuje Informatyk w obecności Kierownika lub osoby przez niego upoważnionej.

16. W sytuacjach kryzysowych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Kierownik udostępnia hasło osobie przez siebie wyznaczonej.

ROZDZIAŁ IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników

1. Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności

wskazujące na naruszenie poufności danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.

3. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.

4. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.

5. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.

6. Informatyk ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Inspektora Ochrony Danych.

7. W czasie pracy użytkownik jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.

8. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z systemu informatycznego lub,

2) poczekać, aż zaktywizuje się blokowany hasłem wygaszacz ekranu.

9. Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

ROZDZIAŁ V

Procedury tworzenia kopii zapasowych

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów, powinny być oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.

2. Kopie zapasowe określone w ust. 1 niniejszego rozdziału sporządza są co najmniej raz na miesiąc.

3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Informatyk.

4. Odpowiada on także za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.

5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

6. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu.
7. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Informatyk w obecności Kierownika lub osoby przez niego wyznaczonej.
8. Z nośników magnetycznych i optycznych wielokrotnego użytku np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
9. Dane zawarte na nośnikach optycznych jednokrotnego użytku np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI

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

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W wypadku przekazywania urządzeń lub nośników zawierających dane osobowe, tzw. "wrażliwe", o których mowa w art. 9 i art. 10 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, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:

   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub

   2) stosowanie metod kryptograficznych, lub

   3) stosowanie odpowiednich zabezpieczeń fizycznych, lub

   4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Dane osobowe zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

5 Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie.

6. Kartoteki przekazywane są do archiwum zgodnie z procedurami archiwizacji dokumentów.

7. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie.

8. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Kierownik.

9. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Inspektor Ochrony Danych lub osoba przez mego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1) data dokonania likwidacji,

2) przedmiot likwidacji (nośniki, kartoteka),

3) przedział czasowy likwidowanych zbiorów danych osobowych,

4) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII

Zabezpieczenie systemu informatycznego

1. System informatyczny zabezpiecza się przed:

1) działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

2) utratą danych spowodowaną:

a) działaniem nieautoryzowanego oprogramowania,

b) awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Informatyk odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.

3. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.

4. Program antywirusowy należy instalować również na komputerach przenośnych.

5. W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

6. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym,

6. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu.
7. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Informatyk w obecności Kierownika lub osoby przez niego wyznaczonej.
8. Z nośników magnetycznych i optycznych wielokrotnego użytku np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
9. Dane zawarte na nośnikach optycznych jednokrotnego użytku np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI

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

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W wypadku przekazywania urządzeń lub nośników zawierających dane osobowe, tzw. "wrażliwe", o których mowa w art. 9 i art. 10 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, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:

   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub

   2) stosowanie metod kryptograficznych, lub

   3) stosowanie odpowiednich zabezpieczeń fizycznych, lub

   4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Dane osobowe zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

jak i do celów instalacyjnych.

7. Na serwerach, w miarę możliwości technicznych oprogramowanie antywirusowe powinno być aktywne cały czas.
8. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.
9. Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.
10. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka.
11. Informatyk usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Inspektora Ochrony Danych o dokonanych czynnościach i rodzaju wirusa.
12. W razie niemożności usunięcia wirusa, Informatyk za zgodą Inspektora Ochrony Danych, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.
13. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
14. Prace określone w ust. 13 są wykonywane pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.
15. Informatyk jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
16. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i dyskietkach.
18. Po usunięciu wirusa Informatyk sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
19. Informatyk sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
    1) nazwę wirusa,
    2) datę wykrycia wirusa,
    3) miejsce zainfekowania,
    4) źródło infekcji.
20. Raport, o którym mowa w ust. 19 przekazywany jest Inspektorowi Ochrony Danych lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.
21. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
22. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 21, obejmują one:

1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,

2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

23. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

24. Informatyk prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

25.Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ VIII

Wymagania dotyczące sprzętu i oprogramowania

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
5. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączanie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.
6. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez min. 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak by przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
7. Zasilaczem awaryjnym powinna być zabezpieczona, co najmniej jedna stacja robocza.

8. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest Informatyk.
9. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
10. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie zabezpieczenie przed przepięciami.
11. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników lub wykonane w specjalnym standardzie.

12. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
13. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.
14. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.
15. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
16. Informatyk odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
17. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
18. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
19. Za spełnienie obowiązku określonego w ust. 18 odpowiadają użytkownicy i kierownicy komórek organizacyjnych.

ROZDZIAŁ IX

Procedury wykonywania przeglądów i konserwacji

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji

służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Informatyk.

2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.

3. Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Inspektora Ochrony Danych przez uprawnionych przedstawicieli tych firm pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

4. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.

5. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

6. Nadzór nad instalowaniem, sprawnym funkcjonowaniem wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk lub osoba wyznaczona przez Administratora Danych.

ROZDZIAŁ X

Postanowienia końcowe

1. Instrukcja jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

2. Użytkownicy są obowiązani zapoznać się z treścią niniejszej Instrukcji.

3. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony 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 oraz wydanymi na jego podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi w Ośrodku Pomocy Społecznej w Górze Kalwarii, a także o zobowiązaniu się do ich przestrzegania.

4. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika 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 oraz wydanymi na tej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi w Ośrodku Pomocy Społecznej w Górze Kalwarii, a także o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 2 do Instrukcji.

5. Oświadczenie przechowywane są w aktach personalnych pracownika.

6. W sprawach nieuregulowanych w niniejszej Instrukcji mają 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 oraz wydanych na jego podstawie aktów wykonawczych.

7. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

INFORMATYK	ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI
.....	.....

Załącznik nr 1 do instrukcji zarządzania systemem informatycznym

ADO.0816. /2018

..... r.

"WZÓR"

WAŻNOŚĆ
od: .....
do: .....

UPOWAŻNIENIE

Na podstawie art. 24 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 upoważniam Panią/Pana

.....
(imię i nazwisko)

do przetwarzania , w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

L.p.	Nazwa zbioru	Postać zbioru	Nazwa programu	Zakres upoważnienia

Zakres upoważnienia:

d – wgląd;
w – wprowadzanie;
m – modyfikacja;
u – usuwanie.

.....
(podpis Administratora Danych)

Załącznik nr 2 do instrukcji zarządzania systemem informatycznym

"WZÓR"

Góra Kalwaria, dn. .... r.

.....

.....

OŚWIADCZENIE

Oświadczam, iż zostałem /zostałam* przeszkolony/ przeszkolona* w zakresie obowiązujących przepisów dotyczących ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz Ustawy z dnia 24 maja 2018 r. (t.j. Dz.U. z 2018 r., poz. 1000), wydanych na jej podstawie aktów wykonawczych oraz obowiązujących instrukcji opracowanych w Ośrodku Pomocy Społecznej w Górze Kalwarii

Jednocześnie zobowiązuję się do ich przestrzegania.

.....

(podpis osoby składającej oświadczenie)

* niepotrzebne skreślić

Załącznik nr 3 do instrukcji zarządzania systemem informatycznym

"WZÓR"

Ewidencja

osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Numer upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login	Uwagi
1	2	3	4	5	6	7	8

Zakres upoważnienia:

d - wgląd;
w – wprowadzanie;
m – modyfikacja;
u – usuwanie.