

Zarządzenie wewnętrzne Nr 12/2018
Dyrektora Ośrodka Pomocy Społecznej w Radzionkowie
z dnia 22.05.2018r.

w sprawie: wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie

Na podstawie: 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) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2016, poz. 446).

Zarządzam co następuje:

§ 1.

Wprowadzam Politykę Bezpieczeństwa przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2.

Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemów Informatycznych.

§ 3.

Traci moc zarządzenie:

Zarządzenie Dyrektora Ośrodka Pomocy Społecznej w Radzionkowie nr 16/2017 z dnia 19.06.2017 w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie.

§ 4.

Zarządzenie wchodzi w życie z dniem 25.05.2018 r.

DYREKTOR
Ośrodka Pomocy Społecznej
w Radzionkowie
mgr Jolanta Jankowska



Załącznik
do Zarządzenia Nr 12/2018
Dyrektora Ośrodka Pomocy Społecznej w
Radzionkowie w sprawie wprowadzenia
Polityki Bezpieczeństwa przetwarzania danych
osobowych w Ośrodku Pomocy Społecznej w
Radzionkowie z dnia 22.05.2018 r.

**POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
OSOBOWYCH
W OŚRODKU POMOCY SPOŁECZNEJ
RADZIONKOWIE**



Spis treści:

1. Rozdział I. Postanowienia ogólne.
2. Rozdział II. Postępowanie przy upoważnieniu osób do przetwarzania danych osobowych.
3. Rozdział III. Postępowanie w przypadku utworzenia nowego zakresu czynności przetwarzania danych osobowych lub zmian w obrębie zgłoszonego zbioru.
4. Rozdział IV. Obszar przetwarzania danych.
5. Rozdział V. Wykaz i struktura zbiorów danych osobowych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.
6. Rozdział VI. Udostępnianie danych osobowych.
7. Rozdział VII. Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych.
8. Rozdział VIII. Identyfikacja ryzyka
9. Rozdział IX. Organizacyjne i techniczne środki ochrony przetwarzania danych osobowych.
10. Rozdział X. Obowiązek informacyjny i zgody na przetwarzanie danych osobowych.
11. Rozdział XI. Postanowienia końcowe.
12. Wykaz załączników:
 - a) Załącznik nr 1. Wzór upoważnienia,
 - b) Załącznik nr 2. Wzór wniosku o upoważnienie do przetwarzania danych osobowych,
 - c) Załącznik nr 3. Oświadczenie o zachowaniu poufności,
 - d) Załącznik nr 4. Ewidencja osób upoważnionych do przetwarzania danych osobowych,
 - e) Załącznik nr 5. Wzór umowy powierzenia przetwarzania danych osobowych,
 - f) Załącznik nr 6. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
 - g) Załącznik nr 7. Rejestr czynności przetwarzania danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury tych danych,
 - h) Załącznik nr 7a Rejestr wszystkich kategorii czynności przetwarzania
 - i) Załącznik nr 8. Sposób przepływu danych między poszczególnymi systemami,
 - j) Załącznik nr 9. Wzór protokołu z naruszenia bezpieczeństwa ochrony danych osobowych.
 - k) Załącznik nr 10. Instrukcja zarządzania systemem informatycznym Ochrony Danych Osobowych w Ośrodku Pomocy Społecznej w Radzionkowie.
 - l) Załącznik nr 11. Ocena ryzyka.
 - m) Załącznik nr 12. Klauzula Informacyjna,
 - n) Załącznik nr 13. Zgoda na przetwarzanie danych osobowych.

Rozdział I Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa w Ośrodku Pomocy Społecznej w Radzionkowie jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych oraz zakresach czynności przetwarzania administrowanych przez Ośrodek.
2. Podstawą do opracowania dokumentu jest:
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),
3. Administratorem Danych Osobowych (ADO) przetwarzanych w Ośrodku Pomocy Społecznej w Radzionkowie jest Dyrektor Ośrodka.
4. W celu sprawnego nadzorowania prawidłowego przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie, Administrator Danych Osobowych powołuje Inspektora Ochrony Danych Osobowych (IODO).
5. Osobą odpowiedzialną za bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w Ośrodku Pomocy Społecznej w Radzionkowie jest Administrator Systemu Informatycznego (ASI).
6. Kierownicy komórek organizacyjnych, Koordynatorzy w Ośrodku odpowiadają za zgłaszanie zmian w obrębie nowych i dotychczasowych zbiorów danych osobowych, wnioskowanie o nadanie, zmianę lub unieważnienie upoważnienia do przetwarzania danych osobowych dla podległych pracowników, zgłaszanie powierzenia przetwarzania danych osobowych podmiotom zewnętrznym.
7. Przetwarzanie danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie jest dopuszczalne tylko pod warunkiem przestrzegania 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), przepisów krajowych oraz wydanych na ich podstawie przepisów wykonawczych oraz zarządzeń Dyrektora Ośrodka.

§ 2

Ilekość w dokumencie jest mowa o:

- 1) **Rozporządzeniu** – rozumie się 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),
- 2) **OPS** – rozumie się Ośrodek Pomocy Społecznej,
- 3) **Administratorze Danych Osobowych (ADO)** – rozumie się Dyrektora OPS w Radzionkowie, decydującego o celach i środkach przetwarzania danych osobowych,
- 4) **Inspektorze Ochrony Danych Osobowych (IODO)** – rozumie się przez to osobę, którą Administrator Danych Osobowych powołał do wsparcia w wypełnianiu ustawowych

obowiązków. W zależności od powołanego stanowiska dotyczy IODO bądź do czasu jego powołania ABI (Administrators bezpieczeństwa informacji),

- 5) **Administratorze Systemów Informatycznych (ASI)** – rozumie się przez to osobę, której ADO powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją funkcjonującą w systemach informatycznych,
- 6) **danych osobowych** – w rozumieniu ustawy o ochronie danych osobowych za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
- 7) **danych wrażliwych** – rozumie się przez to dane określone w art. 27 ustawy, a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych w postępowaniu sądowym lub administracyjnym,
- 8) **haśle** – rozumie się przez to co najmniej 8 – znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- 9) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez ADO obszarach systemu informatycznego,
- 10) **incydencie bezpieczeństwa** – rozumie się przez to czynności, zdarzenia, zjawiska naruszające przepisy niniejszej polityki bezpieczeństwa oraz pozostałych dokumentów bezpieczeństwa informacji, mogące zagrozić utracie aktywów informacyjnych OPS, ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, mogące stanowić sytuację kryzysową,
- 11) **przetwarzaniu danych** – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, wprowadzanie do systemu, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie,
- 12) **systemie informatycznym** - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych,
- 13) **użytkownika** – rozumie się przez to pracownika OPS, zatrudnionego na podstawie umowy o pracę lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą staż, praktykę studencką, który przetwarza dane osobowe znajdujące się w zbiorach danych,
- 14) **zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

Rozdział II

§ 3

Postępowanie przy upoważnieniu osób do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczeni pracownicy OPS posiadający pisemne upoważnienie do przetwarzania danych, nadane przez Administratora Danych Osobowych. Wzór upoważnienia stanowi **załącznik nr 1** do Polityki bezpieczeństwa.
2. Z wnioskiem o upoważnienie pracownika do przetwarzania danych osobowych występuje jego bezpośredni przełożony. Wzór wniosku stanowi **załącznik nr 2** do Polityki bezpieczeństwa. W sytuacjach szczególnych np. zmiany przepisów prawa, upoważnienia są aktualizowane przez Administratora Danych Osobowych z inicjatywy IODO.
3. W przypadku zmiany stanowiska, zakresu obowiązków pracowniczych lub sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, przełożony zobowiązany jest bezzwłocznie skierować wniosek do Administratora Danych Osobowych o wydanie bądź cofnięcie upoważnienia.
4. Każda osoba mająca dostęp do danych osobowych przetwarzanych w Urzędzie zobowiązana jest do podpisania oświadczenia o zachowaniu poufności tych danych. Wzór oświadczenia stanowi **załącznik nr 3** do Polityki bezpieczeństwa.

§ 4.

Osoby upoważnione do przetwarzania danych osobowych mają obowiązek zabezpieczenia tych danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 5.

Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Inspektor Ochrony Danych Osobowych – zgodnie z **załącznikiem nr 4** do niniejszego zarządzenia.

§ 6.

1. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie na podstawie zawartej na piśmie umowy powierzenia przetwarzania danych osobowych. Wzór umowy stanowi **załącznik nr 5** do Polityki bezpieczeństwa,
2. Ewidencja umów powierzenia przetwarzania danych osobowych prowadzona jest przez IODO,
3. Osoby zawierające w/w umowy mają obowiązek poinformować IODO o fakcie zawarcia umowy oraz przekazać do niego kserokopię umowy.

Rozdział III

Postępowanie w przypadku konieczności aktualizacji zakresu czynności przetwarzania danych osobowych

§ 7.

1. Kierownicy komórek organizacyjnych/Koordynatorzy w OPS, mają obowiązek poinformować ADO/IODO o konieczności utworzeniu nowego zakresu czynności lub zmianie w obrębie już istniejącego.

2. Informacja, o której mowa w ust. 1 powinna zawierać:
 - a) nazwę zakresu (ewidencji),
 - b) podstawę prawną upoważniającą do prowadzenia czynności,
 - c) cel przetwarzania danych,
 - d) opis kategorii osób, których dane dotyczą,
 - e) obszar przetwarzania,
 - f) metodę katalogowania (system komputerowy, metoda tradycyjna),
 - g) zakres danych zawartych w zbiorze (np. imię, nazwisko, PESEL),
 - h) sposób zbierania danych osobowych,
 - i) podmioty, którym dane osobowe będą udostępniane i na jakich zasadach.
3. IODO wpisuje czynności do rejestru czynności.

Rozdział IV

Obszar przetwarzania danych

§ 8

1. Obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania) stanowią wszystkie pomieszczenia biurowe zajmowane przez komórki organizacyjne Ośrodka z wyłączeniem pomieszczeń gospodarczych i korytarzy w budynku przy ul. Kuźaja 19.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 6** do Polityki Bezpieczeństwa.

§ 9.

1. W przypadku konieczności uzyskania dostępu do obszaru przetwarzania danych przez osoby nieuprawnione do przetwarzania danych osobowych, które muszą wykonać prace o charakterze serwisowym lub inne działania doraźne, osoby te zobowiązane są do złożenia oświadczenia o zachowaniu poufności, o którym mowa w § 3 ust. 4.
2. Osoby nieupoważnione mogą przebywać w obszarach określonych jako obszar przetwarzania, wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych lub za pisemną zgodą ADO.
3. Przebywanie w pomieszczeniach serwerowni OPS innych osób niż ASI, dopuszczalne jest tylko w obecności ASI lub za pisemnym upoważnieniem ADO. Zasada ta dotyczy również osób wykonujących czynności serwisowe niezbędne dla funkcjonowania infrastruktury technicznej lub upoważnionych do prowadzenia kontroli.

Rozdział V

Wykaz i struktura danych osobowych oraz sposób przepływu danych pomiędzy poszczególnymi systemami

§ 10

1. Rejestr czynności przetwarzania danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury tych danych określa **załącznik nr 7** do Polityki bezpieczeństwa.
2. Rejestr czynności prowadzony jest na bieżąco przez IODO zgodnie ze wzorem **załącznika nr 7**.

3. Rejestr wszystkich kategorii czynności przetwarzania określa **załącznik nr 7a** do polityki bezpieczeństwa. Rejestr prowadzony jest na bieżąco przez IOD zgodnie ze wzorem.

§ 11.

Sposób przepływu danych między poszczególnymi systemami określa **załącznik nr 8** do Polityki bezpieczeństwa.

Rozdział VI

Udostępnianie danych osobowych

§ 12.

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
 - a) na podstawie wniosku podmiotu uprawnionego do otrzymywania danych osób owych na podstawie przepisów
 - b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych
 - c) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazać ich zakres i przeznaczenie.
4. Osobom, których dane przetwarzane są w zbiorze danych w Urzędzie, przysługuje prawo do kontroli treści ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.
5. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, kierujący komórką organizacyjną jest zobowiązany do ich uzupełnienia, uaktualnienia lub sprostowania.
6. O każdym wniosku o udzielenie informacji oraz ewentualnej konieczności sprostowania danych należy poinformować Inspektora Ochrony Danych Osobowych.

Rozdział VII

Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych

§ 13

Przepisy niniejszego rozdziału stosuje się w przypadku:

1. stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych,
2. podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 14

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

- 1) nieautoryzowany dostęp do danych,
- 2) nieautoryzowane modyfikacje lub zniszczenie danych,
- 3) udostępnienie danych nieautoryzowanym podmiotom,
- 4) nielegalne ujawnienie danych,
- 5) pozyskiwanie danych z nielegalnych źródeł.

§ 15

1. W przypadku stwierdzenia naruszenia zabezpieczenia lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub Inspektora Ochrony Danych Osobowych, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
 - 1) opisanie działania wskazującego na naruszenie ochrony danych osobowych,
 - 2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
 - 3) wskazanie istotnych informacji mogących wskazać na przyczynę naruszenia,
 - 4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 16

1. IODO podejmuje działania mające na celu:
 - 1) minimalizację negatywnych skutków zdarzenia,
 - 2) wyjaśnienie okoliczności zdarzenia,
 - 3) zabezpieczenie dowodów zdarzenia,
 - 4) umożliwienie dalszego bezpiecznego przetwarzania danych.
2. Dla realizacji celów określonych w ust. 1 IODO ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
 - 1) żądania wyjaśnień od pracowników,
 - 2) korzystania z pomocy konsultantów,
 - 3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 17

Odmowa udzielenia wyjaśnień lub współpracy z IODO traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 18

Inspektor Ochrony Danych Osobowych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje protokół z naruszenia bezpieczeństwa informacji, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski i zalecenia ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór protokołu stanowi **załącznik nr 9** do Polityki bezpieczeństwa.



Rozdział VIII

Identyfikacja ryzyka

Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą sporządzana jest przez IODO. Wzór dokumentu stanowi **załącznik nr 11** do Polityki bezpieczeństwa.

Rozdział IX

Organizacyjne i techniczne środki ochrony przetwarzania danych osobowych

§ 19

Pomieszczenia, w których przetwarzane są dane osobowe, mają zabezpieczone wejścia za pomocą zamków, w sposób uniemożliwiający dostęp do nich osób niepowołanych, a pracownicy sprawują nadzór nad powierzonymi kluczami.

§ 20

1. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.
2. W przypadku konieczności zniszczenia papierowych kopii dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się w niszczarkach dokumentów użytkowanych w OPS.

§ 21

1. Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych – w tym danych osobowych (np. interesanci lub inni pracownicy OPS) – winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych.
2. Każdy użytkownik posiadający dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, musi posiadać w tym systemie swój unikalny identyfikator oraz indywidualne hasło.
3. Niedozwolone jest przetwarzanie zbiorów danych osobowych na komputerach przenośnych poza obszarem przetwarzania, o którym mowa w rozdziale IV.
4. Przenośne nośniki danych mogą służyć do przechowywania zbiorów danych osobowych tylko w wyjątkowych sytuacjach za zgodą ASI i tylko po zastosowaniu środków ochrony kryptograficznej.
5. Szczegółowe zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Radzionkowie”.

Rozdział X

Obowiązek informacyjny i zgody na przetwarzanie danych osobowych.

1. Zbieranie danych osobowych podczas wykonywania czynności służbowych odbywa się przy zastosowaniu klauzuli informacyjnej, która musi zostać opatrzona podpisem strony (**załącznik nr 12**).
2. Strona postępowania musi wyrazić zgodę na przetwarzanie danych osobowych jeśli przetwarzanie danych wynika z przyczyn innych niż zadania ustawowe. W takim przypadku wyraża ją podpisując odpowiednią klauzulę zgody (**załącznik nr 13**). Pracownik nie może podjąć wtedy działania przetwarzania danych osobowych bez uzyskania tej zgody.

Rozdział XI

Postanowienia końcowe

§ 23

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością służbowa oraz odpowiedzialnością wskazaną w Rozporządzeniu 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).



Radzionków, dnia

UPOWAŻNIENIE NR/2018

Na podstawie:

.....
.....
(wymienić postawy prawne)

upoważniam:

Pana / Panią

stanowisko:

do przetwarzania danych osobowych w zbiorach/zakresach czynności::

.....
.....

miejsce przetwarzania danych osobowych: **Ośrodek Pomocy Społecznej w Radzionkowie**

data nadania upoważnienia:

Upoważnienie ważne jest do czasu jego cofnięcia.

Rozwiązanie stosunku pracy powoduje wygaśnięcie upoważnienia.

Upoważnienie nie może być przenoszone na inne osoby.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem, o którym mowa wyżej jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
Dyrektor Ośrodka Pomocy Społecznej
w Radzionkowie

.....
data i podpis osoby upoważnionej

Radzionków, dnia

**Dyrektor Ośrodka Pomocy
Społecznej w Radzionkowie**

Wniosek o wydanie/cofnięcie* upoważnienia do przetwarzania danych osobowych

Na podstawie:.....

(wymienić postawy prawne)

wniosuję o wydanie upoważnienia/cofnięcie upoważnienia z dnia*.....:

Pani/Panu

(imię i nazwisko pracownika)

zatrudnionej/emu w

na stanowisku

do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych
z powodu (zaznaczyć właściwe):

- a) podjęcia pracy na stanowisku
- b) zmiany stanowiska
- c) zmiany zakresu obowiązków pracowniczych
- d) utworzenia nowego zbioru danych osobowych
- e) naruszenia zasad i sposobu przetwarzania danych osobowych

1. Nazwa zbioru danych osobowych/ zakresu danych:

.....

2. Rodzaj uprawnień (zaznaczyć właściwe):

- a) pełne – prawo do edytowania, wprowadzania danych
- b) niepełne – prawo do przeglądania

3. Sposób i miejsce przetwarzania danych osobowych

.....

.....
data i podpis

Dyrektora/Kierownika Działu/Koordynatora

OŚWIADCZENIE

1. Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do którym mam lub będę miał/a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Ośrodka Pomocy Społecznej w Radzionkowie. Zachowanie tajemnicy obowiązuje mnie także po zaprzestaniu tych czynności.
2. Zobowiązuję się chronić dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w Ośrodku Pomocy Społecznej w Radzionkowie dotyczących ochrony danych osobowych – w szczególności określonych w Polityce bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
4. Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z: Rozporządzeniem 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),

Jestem świadomy/a odpowiedzialności z tytułu ich nieprzestrzegania

.....
(data i podpis osoby oświadczającej)

9

**Umowa nr/2018
powierzenia przetwarzania danych osobowych**

Zawarta w dniu w Radzionkowie pomiędzy:

Jakubem Janiakim Dyrektorem – reprezentującym Ośrodek Pomocy Społecznej w Radzionkowie z siedzibą w Radzionkowie przy ul. Kuźaja 19, 41-922 Radzionków, NIP: 626-24-44-853, zwanym dalej „Zleceniodawcą”

a

.....
zwaną dalej „Wykonawcą”

§ 1

Powierzenie przetwarzania danych osobowych

1. Zleceniodawca powierza Wykonawcy, w trybie art. 28 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), zwanego w dalszej części „Rozporządzeniem”
(wymienić inne postawy prawne, jeśli dotyczy)
1. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
2. Powierzone dane zawierają informacje o osobach fizycznych.
3. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych jedynie w zakresie określonym w § 2.

§ 2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał dane osobowe, powierzone na podstawie niniejszej Umowy, gromadzone w następujących zakresach danych:
.....
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu:
.....

§ 3

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust. 1, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Wykonawca oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie i zabezpieczenie danych osobowych, a jego system informatyczny odpowiada wymaganiom określonym w Rozporządzeniu RODO.

3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
5. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
 - 1) każdym żądaniu udostępnienia danych osobowych właściwemu organowi lub instytucji,
 - 2) każdym żądaniu osoby, której dane przetwarza,
 - 3) każdym nieupoważnionym dostępie do danych osobowych.
6. Zleceniodawca ma prawo do kontroli sposobu wykonywania Umowy oraz żądania składania przez Wykonawcę pisemnych wyjaśnień.
 - 1) Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
 - 2) Zleceniodawca realizować będzie prawo kontroli w godzinach pracy Wykonawcy i z minimum 7 dniowym jego uprzedzeniem.
 - 3) Wykonawca zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Zleceniodawcę nie dłuższym niż 7 dni.
 - 4) Wykonawca udostępnia Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
7. Wykonawca zobowiązuje się do usunięcia uchybień i poprawy bezpieczeństwa przetwarzania danych osobowych oraz udzielenia odpowiedzi na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych danych osobowych.
8. Wykonawca nie jest uprawniony do powierzenia danych objętych Umową podmiotom trzecim bez uprzedniej zgody Zleceniodawcy, wyrażonej na piśmie pod rygorem nieważności.

§ 4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5

Czas obowiązywania umowy

1. Niniejsza Umowa powierzenia zostaje zawarta na okres.....
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem dniowego okresu wypowiedzenia.

§ 6

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Wykonawca:
 - 1) wykorzystał dane osobowe w sposób niezgodny z Umową,
 - 2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,

- 3) niewłaściwie przetwarza dane osobowe, pomimo uprzedniego wezwania do zmiany sposobu ich przetwarzania,
- 4) nie ma zdolności do dalszego wykonywania Umowy.

§ 7

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia Umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zwróci wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, a także usunie z własnych systemów informatycznych oraz zniszczy dane osobowe przechowywane na własnych nośnikach danych lub w wersji papierowej.

§ 8

Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w Umowie mają zastosowanie przepisy ustawy i przepisów wykonawczych oraz Kodeksu cywilnego.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....
Zleceniodawca

.....
Wykonawca

9

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

Lp.	Dokładny adres jednostki, w której przetwarzane są dane osobowe	Komórka organizacyjna użytkująca pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia
1.	ul. Kuźaja 19 41-922 Radzionków	Ośrodek Pomocy Społecznej w Radzionkowie		Alarm, okratowanie okien na parterze budynku, monitoring
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

	Spis pendłów	w Radzionkowce, Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			
5	MIDOS – dolański męskie kamionki	Dyrektor/ Osrodek Pomocy Społecznej w Radzionkowce Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			
6	PRZECIWDZIA NIEKORUPCYNICZNY RODOZMIANIE	Dyrektor/ Osrodek Pomocy Społecznej w Radzionkowce Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			
7	Familia 300+	Dyrektor/ Osrodek Pomocy Społecznej w Radzionkowce Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			
8	Decyzje potwierdzające prawo do świadczeń opieki zdrowotnej finansowanej ze środków publicznych	Dyrektor/ Osrodek Pomocy Społecznej w Radzionkowce Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			
9	Staż	Dyrektor/ Osrodek Pomocy Społecznej w Radzionkowce Ul. Kuziała 19 41-922 Radzionków REGON: 273-752-731																			

Zmiana pkt. 1043, nr

przebiegi prawa

osoby wnioskujące o podjęcie decyzji

nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu

od osób, których dane dotyczą, z imienną listą

Dane nie są udostępniane

RODS i inne urzędy

Dane nie są przekazywane

DRŚ

DPS

DPS

DKK

10	Praktyki	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list przywołania lub spełnienia obowiązku wynikającego z przepisu prawa ustawy z dnia 26 czerwca 1994 r. (Dz.U. z 2005, Nr 164, poz. 1285, ze zm.)	odpisy praktyki odbiorcy podlegni namacalna uchwała	praktyka	nazwa i imiona, data urodzenia, PESEL, wyszczególnienie, seria i numer dowodu osobistego, nr telefonu, nr wni, nr ucznia, kierunku i elektronicznej	od osób, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DKK
11	Księgowość (Kamry/ Plac)	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list nie dotyczy, do zwaleniowa obowiązków wynikających z przepisów prawa - ustawa o rachunkowości z dnia 29 września 1994 r. (Dz.U. z 1994, Nr 121, poz. 591), ustawa o finansach publicznych z dnia 27 sierpnia 2009 r. (Dz.U. z 2009, Nr 157, poz. 1240)	doposażenie obowiązków w przepisach prawa	dane osób pobierających KOPIS, dane kontrolnych, dane osób zatrudnionych w placówce i inne umowy o pracę	Nazwa i imiona, imiona rodziców, data urodzenia, miejsce pobytu, PESEL, NIP, miejsce pracy, zawód, wyszczególnienie, seria i numer dowodu osobistego, nr urodzenia dziecka lub dzieci pracownika, nr rachunku bankowego pracownika, świadczony wykształcenia	od osób, których dane dotyczą, z innych źródeł niż osoby, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DKK
12	Skargi i wnioski	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list nie dotyczy, do zwaleniowa obowiązków wynikających z przepisów prawa - ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 19, poz. 69, ze zm.)	rozstrzygnięcie skarg i wniosków	osoby fizyczne i prawne	nazwa i imiona, adres zamieszkania lub pobytu, numer telefonu, adres poczty elektronicznej	od osób, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DAO
13	Ewidencja korespondencji	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list nie dotyczy, do zwaleniowa obowiązków wynikających z przepisów prawa - ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 19, poz. 69, ze zm.)	doposażenie obowiązków odebranych w przepisach prawa	listy i odpisy korespondencji	nazwa i imiona, adres zamieszkania lub numer telefonu, adres poczty elektronicznej	od osób, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DAO
14	Składnica Akt	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list nie dotyczy, do zwaleniowa obowiązków wynikających z przepisów prawa - ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 19, poz. 69, ze zm.), ustawa z dnia 13 lipca 1991 r. o archiwalnym i innych aktach (Dz.U. z 2011, Nr 123, poz. 898, ze zm.), ustawa z dnia 15 czerwca 2000 r. o udostępnianiu informacji o działalności państwa lub podległości państwa (Dz.U. z 2013, poz. 592, ze zm.)	doposażenie obowiązków w przepisach prawa	osoby, których dotyczy materiały archiwalne	nazwa i imiona, imiona rodziców, data urodzenia, miejsce pobytu, PESEL, miejsce pracy, zawód, wyszczególnienie, seria i numer dowodu osobistego, nr telefonu, nr wni, nr ucznia, kierunku i elektronicznej, adres poczty elektronicznej, seria i numer dowodu osobistego, nr urodzenia dziecka lub dzieci pracownika, nr rachunku bankowego pracownika, świadczony wykształcenia	od osób, których dane dotyczą, z innych źródeł niż osoby, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DAO
15	Zamówienia Publiczne	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuźajła 19 41-922 Radzionków REGON: 273-752-731			przezwazanie list nie dotyczy, do zwaleniowa obowiązków wynikających z przepisów prawa - ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 19, poz. 69, ze zm.)	doposażenie obowiązków w przepisach prawa	uczestnicy zamawiania o udzielenie zamówienia publicznego	Nazwa i imiona, imiona rodziców, data urodzenia, miejsce pobytu, PESEL, NIP, miejsce pracy, zawód, wyszczególnienie, seria i numer dowodu osobistego, nr telefonu, nr wni, nr ucznia, kierunku i elektronicznej, adres poczty elektronicznej, seria i numer dowodu osobistego, nr urodzenia dziecka lub dzieci pracownika, nr rachunku bankowego pracownika, świadczony wykształcenia	od osób, których dane dotyczą, z innych źródeł niż osoby, których dane dotyczą	Dane nie są udostępniane, nie upoważnione na podstawie przepisów prawa	Dane nie są przetwarzane w systemie publicznym	DAO



16	Karta Dusz Rodziny	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuznia 19 41-922 Radzionków REGON: 273-752-731	przeznaczone jest do wydania w celu realizacji zadań określonych w przepisach prawa- Usługa z dnia 5 grudnia 2014 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2014 poz. 1863 ze zm.)	Wydanie Karty Dusz Rodziny dla prz. 1863/2014	Dane Wydziału	nazwisko, imię, data urodzenia, adres zamieszkania lub pobytu, adres poczty elektronicznej, data przelotu, data przyjazdu, data wyjazdu	od osoby, której dane dotyczą, z tegoż rodzica lub osoby, której dane dotyczą	Dane nie są udostępniane, nie upoważnienie na przepisów prawa	Dane nie są przekazywane państwu	DPS
16	Rekrutacja (Zbiór CV)	Dyrektor/ Osirodek Pomocy Społecznej w Radzionkowach ul. Kuznia 19 41-922 Radzionków REGON: 273-752-731	przeznaczone jest do wydania w celu realizacji zadań określonych w przepisach prawa- Usługa z dnia 5 grudnia 2014 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2014 poz. 1863 ze zm.)	Zamówienie	Dane Wydziału	nazwisko, imię, Adres zamieszkania lub pobytu, adres poczty elektronicznej, data przelotu, data przyjazdu, data wyjazdu	od osoby, której dane dotyczą, z tegoż rodzica lub osoby, której dane dotyczą	Dane nie są udostępniane, nie upoważnienie na przepisów prawa	Dane nie są przekazywane państwu	DKK

REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA W OŚRODKU POMOCY SPOŁECZNEJ W RADZIKOWIE

*Kolorem czerwonym oznaczono informacje wymagane w rozporządzeniu art. 30 ust. 2 ROZDRO

ZAŁĄCZNIK NR 7A DO POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1	2	3	4	5	6	7	8	9	10
Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy)	Nazwa i dane kontaktowe administratora (jeżeli powołano)	Okres przetwarzania	Nazwa państwa, trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiedzialnych za bezpieczeństwo danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Czy nastąpiło dane powierzenie danych?	
Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Administrator			Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1	<p>Zabezpieczenia techniczne:</p> <ol style="list-style-type: none"> 1) Pomieszczenia zamknięte na klucz. 2) Klucze przechowywane w sekrzecie. 3) Szyfry zamknięte na klucz. 4) Kontrola dostępu do systemu informatycznego. Dostęp do danych otrzymują wyłącznie osoby upoważnione przez OPS Radzionków. 5) Program antywirusowy na każdym komputerze. 6) Szyfrowana transmisja danych. 7) Czujki ruchu w każdym pomieszczeniu biurowym oraz na korytarzach - alarm aktywuje automatycznie wzwanie policji i powiadomienie pracownika OPS (3 numery telefonów komórkowych) <p>Zabezpieczenia organizacyjne:</p> <ol style="list-style-type: none"> 1) Polityka Bezpieczeństwa Danych Osobowych. 2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. 3) Nadawanie uprawnień do przetwarzania danych osobowych. 4) Określenie upoważnionej osoby o zachowaniu poufności danych i sposobie zabezpieczenia danych. 	<p>Województwo Śląskie reprezentowane przez Zarząd Województwa Śląskiego, pełniące rolę „Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Śląskiego na lata 2014-2020”</p>	nie dotyczy	nie dotyczy	<p>daneosobowe@slaskie.pl</p>	01.01.2018 r. - 31.12.2020 r.	nie dotyczy	nie dotyczy	NIE
2	<p>Zabezpieczenia techniczne:</p> <ol style="list-style-type: none"> 1) Pomieszczenia zamknięte na klucz. 2) Klucze przechowywane w sekrzecie. 3) Szyfry zamknięte na klucz. 4) Kontrola dostępu do systemu informatycznego. Dostęp do danych otrzymują wyłącznie osoby upoważnione przez OPS Radzionków. 5) Program antywirusowy na każdym komputerze. 6) Szyfrowana transmisja danych. 7) Czujki ruchu w każdym pomieszczeniu biurowym oraz na korytarzach - alarm aktywuje automatycznie wzwanie policji i powiadomienie pracownika OPS (3 numery telefonów komórkowych) <p>Zabezpieczenia organizacyjne:</p> <ol style="list-style-type: none"> 1) Polityka Bezpieczeństwa Danych Osobowych. 2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. 3) Nadawanie uprawnień do przetwarzania danych osobowych. 4) Określenie upoważnionej osoby o zachowaniu poufności danych i sposobie zabezpieczenia danych. 	<p>Województwo Śląskie reprezentowane przez Zarząd Województwa Śląskiego, pełniące rolę „Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Śląskiego na lata 2014-2020”</p>	nie dotyczy	nie dotyczy	<p>daneosobowe@slaskie.pl</p>	01.01.2018 r. - 30.06.2019 r.	nie dotyczy	nie dotyczy	NIE

Rejestr wszystkich kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego

Nazwa	Ośrodek Pomocy Społecznej w Radzionkowie
Adres	ul. Kuźaja 19, 41-922 Radzionków
Email	sekretariat@ops.radzionkow.pl
Telefon	32 286-65-44

Inspektor Ochrony Danych (jeśli wyznaczono)

Imię i Nazwisko	Piotr Lukasik
Adres	
Email	sekretariat@ops.radzionkow.pl
Telefon	32/ 286 65 44 wew. 24 lub 23

Obowiązuje od:

25.05.2018 r.

Obowiązuje do:

Sposób przepływu danych między poszczególnymi systemami

Systemy wewnętrzne		Systemy zewnętrzne	Kierunek przepływu danych osobowych	Sposób przesyłania danych do systemu zewnętrznego
System/Moduł „A”	System/Moduł „B”			
Program Place	Program Płatnik	ZUS	Jednokierunkowo z programu Place do Programu Płatnik/ZUS	Internet
Program QNT	Kadry i Place		Przesyłanie Sprawozdań	Internet
Program QNT	F-K	SJO Bestia	Jednokierunkowo - Przesyłanie Sprawozdań	Internet
System bankowy ING		Bank Odbiorcy	Jednokierunkowo Usługa umożliwiająca przesyłanie poleceń przelewów w formie pliku do banku odbiorcy	Internet
Program HELIOS – Pomoc Społeczna		Centralna Aplikacja Statystyczna	Jednokierunkowe - sprawozdawczość	Internet
Program FAMILIA	Świadczenia Rodzinne	Centralna Aplikacja Statystyczna PUE – ZUS, CBB, e-finance, PESEL, AC Rynek pracy, e-podatki	Jednokierunkowe – sprawozdawczość Dwukierunkowo - zapytania	Internet
Program FAMILIA	500+	Centralna Aplikacja Statystyczna PUE – ZUS, CBB, e-finance, PESEL, AC Rynek pracy, e-podatki	Jednokierunkowe – sprawozdawczość Dwukierunkowo - zapytania	Internet
Program FUNDAL	Zaliczka Alimentacyjna	Centralna Aplikacja Statystyczna PUE – ZUS, CBB, e-finance, PESEL, AC Rynek pracy, e-podatki	Jednokierunkowe – sprawozdawczość Dwukierunkowo - zapytania	Internet

Wzór protokołu naruszenia bezpieczeństwa ochrony danych osobowych w OPS w Radzionkowie

Data: Godzina:

1. Osoba powiadamiająca o zaistniałym zdarzeniu (imię, nazwisko, stanowisko służbowe, identyfikator użytkownika - jeśli występuje):

.....
.....

2. Lokalizacja zdarzenia (np. nr pokoju, nazwa pomieszczenia):

.....
.....

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

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

4. Podjęte działania:

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

5. Przyczyny wystąpienia zdarzenia:

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

6. Postępowanie wyjaśniające:

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

.....
(podpis Inspektora Ochrony Danych Osobowych)



Załącznik nr 10 do
Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Ośrodku Pomocy Społecznej Radzionkowie

**Instrukcja zarządzania
systemem informatycznym
Ochrony Danych Osobowych
w Ośrodku Pomocy Społecznej w
Radzionkowie**

9

Spis treści

Rozdział I	3
Wstęp.....	3
Rozdział II	3
Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej.....	3
Rozdział III.....	4
Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe	4
Rozdział IV.....	4
Procedura dostępu podmiotów zewnętrznych	4
Rozdział V	5
Procedura korzystania z Internetu	5
Rozdział VI.....	5
Procedura korzystania z poczty elektronicznej	5
Rozdział VII	6
Procedura nadawania uprawnień do przetwarzania danych osobowych.....	6
Rozdział VIII.....	7
Metody i środki uwierzytelnienia.....	7
Rozdział IX.....	8
Procedura rozpoczęcia, zawieszenia i zakończenia pracy	8
Rozdział X.....	8
Procedura tworzenia kopii zapasowych	8
Rozdział XI.....	9
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.....	9
Rozdział XII	9
Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi	9
Rozdział XIII.....	11
Procedura wykonywania przeglądów i konserwacji	11

9

Rozdział I

Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

Rozdział II

Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zabezpieczenia infrastruktury przed skutkami awarii zasilania – Stosowane są UPS-y podtrzymujące zasilanie serwerów
2. Zabezpieczenia trwałych elementów infrastruktury, wykorzystywanych do przetwarzania danych osobowych:
 - 1) komputery służące do przetwarzania danych osobowych są połączone z siecią informatyczną;
 - 2) w przypadku, gdy zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego, praca na tym komputerze dopuszczona jest tylko w siedzibie Ośrodka. Każdorazowe przemieszczenie komputera przenośnego poza siedzibę Ośrodka musi być poprzedzone usunięciem wszelkich danych osobowych z tego komputera i zabezpieczenie ich w siedzibie Ośrodka (na dysku serwera, lub innym nośniku elektronicznym). Użytkownicy komputerów przenośnych akceptują i podpisują regulamin użytkowania komputerów przenośnych stanowiący **załącznik nr 1**. Użytkownik samodzielnie sporządza regularną kopię bezpieczeństwa, przechowuje komputer przenośny po zakończeniu pracy w warunkach zapewniających bezpieczeństwo;
 - 3) programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają wymagane licencje.
3. Zabezpieczenia przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji;
 - 1) lokalizacja urządzeń komputerowych (komputerów typu PC, drukarek) powinna uniemożliwiać osobom niepowołanym (np. klientom, pracownikom innych działów) dostęp do nich;
 - 2) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zabezpieczenia sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji);
 - 1) stosuje się środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji VPN;
 - 2) dostęp do środków teletransmisji zabezpieczony jest za pomocą mechanizmów uwierzytelnienia.

9

5. Zabezpieczenia sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych;
 - 1) środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
 - 2) system Firewall do ochrony dostępu do sieci komputerowej;
 - 3) system IDS/IPS do ochrony dostępu do sieci komputerowej.

Rozdział III

Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych:

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. W każdym przypadku powinien być stosowany mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
3. Każdorazowo stosowane są środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
4. Na terenie Ośrodka stosowane są systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Na stanowiskach, na których przetwarzane są dane osobowe zainstalowano wygaszacze ekranów.
6. Na stanowiskach stosuje się mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 15 minutach).
7. Na stanowiskach, na których przetwarzane są dane osobowe każdorazowo stosowany jest system antywirusowy.

Rozdział IV

Procedura dostępu podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne.

- 1) Administrator Danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę o przetwarzaniu danych;
- 2) podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie przetwarzania danych osobowych;
- 3) podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków

technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);

- 4) rejestr podmiotów zewnętrznych z którymi zawarto umowy o poufności prowadzi IODO i stanowi **załącznik Nr 2** - Rejestr podmiotów zewnętrznych.

Rozdział V

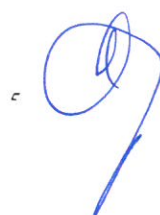
Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów oraz plików pobranych z niewiadomego źródła.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobierane lub instalowane z Internetu oraz za posiadanie materiałów i plików bez licencji lub praw autorskich.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:".

Rozdział VI

Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza instytucję może odbywać się tylko przez osoby do tego upoważnione i tylko służbową skrzynką pocztową.
2. W przypadku przesyłania informacji wrażliwych wewnątrz instytucji bądź wszelkich danych osobowych poza instytucję należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym e-mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.



5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w e-mailach nadesłanych przez podejrzanego nadawcę lub podejrzanym załączników nadanych przez znanego nadawcę.
7. Użytkownicy nie powinni rozsyłać za pośrednictwem e-maila informacji mogących stanowić zagrożenie dla systemu informatycznego, „łańcuszków szczęścia”, itp.
8. Użytkownicy nie powinni rozsyłać e-maili zawierających załączniki o dużym rozmiarze
9. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
10. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.

Rozdział VII

Procedura nadawania uprawnień do przetwarzania danych osobowych.

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione.

1. Zarządzanie uprawnieniami użytkowników
 - 1) wydanie, zmiana, cofnięcie upoważnienia do przetwarzania danych osobowych w systemie informatycznym i/lub papierowym następuje na wniosek bezpośredniego przełożonego użytkownika;
 - 2) każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej zostaje przeszkolony i zapoznany z Polityką Bezpieczeństwa Ochrony Danych Osobowych;
 - 3) za przeprowadzenie szkolenia i zapoznanie z Polityką Bezpieczeństwa odpowiada IODO;
 - 4) po szkoleniu i po zapoznaniu się z Polityką Bezpieczeństwa, użytkownik zobowiązany jest do podpisania „Oświadczenia użytkownika o poufności” - **Załącznik nr 3** do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Ośrodku Pomocy Społecznej Radzionkowie
 - 5) dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań, w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe;
 - 6) projekt upoważnienia do przetwarzania danych osobowych sporządza IODO zgodnie z wnioskiem bezpośredniego przełożonego użytkownika. Upoważnienie wydaje ADO.

- 7) w przypadku upoważnienia do przetwarzania danych w systemie informatycznym w upoważnieniu wpisuje się identyfikator dla użytkownika (wg. wzoru: pierwsza litera imienia, nazwisko bez polskich znaków), po jednoczesnym uzgodnieniu z ASI;
- 8) upoważnienie za potwierdzeniem odbioru otrzymuje osoba upoważniona, IODO, bezpośredni przełożony użytkownika oraz w przypadku wydania upoważnienia do obsługi systemu informatycznego również ASI;
- 9) „Ewidencję osób upoważnionych do przetwarzania danych osobowych” prowadzi IODO;
- 10) za bieżącą aktualizację upoważnień w podległej komórce odpowiada bezpośredni przełożony użytkownika, a za ich realizację odpowiada IODO;
- 11) identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.

2. Zarządzanie uprawnieniami administratorów

Administratorów systemów informatycznych (tzw. Użytkowników uprzywilejowanych) wyznacza pisemnie dyrektor OPS w Radzionkowie.

Rozdział VIII

Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Ogólne zasady postępowania z hasłami
 - 1) ASI informuje ustnie użytkownika o nadaniu pierwszego hasła do systemu;
 - 2) użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła;
 - 3) hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów;
 - 4) użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności;
 - 5) zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
2. Hasła do sieci i serwera
 - 1) hasło dostępu do (serwera / sieci) składa się co najmniej z 8 znaków;
 - 2) hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Hasła do programów przetwarzających dane osobowe
 - 1) hasło dostępu do programów składa się co najmniej z 8 znaków;
 - 2) hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych;
 - 3) zmiana hasła odbywa się raz na 30 dni;

7



- 4) zmiana hasła jest wymuszana przez program. W programach w których takiego wymuszenia nie ma Użytkownicy są zobowiązani do samodzielnej zmiany hasła.
4. Hasła administratorów
 - 1) hasło administratora składa się co najmniej z 8 znaków;
 - 2) hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych;
 - 3) administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 6 miesięcy;
 - 4) w przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
 5. Ogólne zasady postępowania z kartami mikroprocesorowymi/tokenami
 - 1) użytkownik systemu w trakcie pracy w aplikacji może zmienić swój PIN;
 - 2) PIN-y do karty/tokena nie mogą być powszechnie używanymi słowami. W szczególności nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów;
 - 3) użytkownik zobowiązuje się do zachowania PIN-u w poufności, nawet po utracie przez nie ważności;
 - 4) zabronione jest zapisywanie PIN-u w sposób jawny oraz przekazywanie ich innym osobom;
 - 5) użytkownik jest odpowiedzialny za zabezpieczenie swojej karty/tokena;
 - 6) zabronione jest pozostawianie karty/tokena w ogólnie dostępnym miejscu, bez nadzoru;
 - 7) zabronione jest pozostawienie kart/tokenów mikroprocesorowych w klawiaturach komputerowych, czytnikach elektronicznych po zakończeniu pracy;
 - 8) zabronione jest przekazywanie karty/tokena i Pin-u innemu pracownikowi.

Rozdział IX

Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

- 1) użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła;
- 2) w przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi;
- 3) użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu;

9

- 4) przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. W przypadku stosowania karty/tokena należy wyjąć i zabezpieczyć kartę/token. Jeżeli tego nie uczyni – po upływie 15 minut system automatycznie aktywuje wygaszacz;
- 5) po zakończeniu pracy, użytkownik zobowiązany jest:
 - a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
 - b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe,
 - c) zabezpieczyć kartę/token.

Rozdział X

Procedura tworzenia kopii zapasowych

Celem procedury jest zabezpieczenie danych informatycznych w tym osobowych przed utratą.

1. Zabezpieczenie danych informatycznych przetwarzanych na serwach.
Zabezpieczeniem baz danych, konfiguracji zajmuje się administrator systemu. Kopia danych wykonywana jest cyklicznie, a jej częstotliwość dostosowana do wymagań programu lub aplikacji bazodanowej.
2. Za zabezpieczenie danych przetwarzanych przez użytkowników na komputerach lokalnych odpowiadają użytkownicy. Ich obowiązkiem jest wykonanie kopii swoich dokumentów oraz kopii poczty elektronicznej poprzez skopiowanie danych na wydzielony dla każdego udział sieciowy użytkownika.

Rozdział XI

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji

Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pendrive'ami, telefonami komórkowymi, pamięciami typu „flash” na których znajdują się dane osobowe, celem zabezpieczenia ich przed niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

Zabezpieczenie elektronicznych nośników informacji

- 1) nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych itp.);
- 2) w sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
 - a) adresat powinien zostać powiadomiony o przesyłce,
 - b) nadawca powinien sporządzić kopię przesyłanych danych,

9

- c) jeśli dane przekazywane są przez stronę trzecią (poczta, kurier, gońiec itd) powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
 - d) należy stosować bezpieczne koperty depozytowe,
 - e) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
- 3) użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej);
 - 4) podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g Protokołu zniszczenia uszkodzonych nośników – **załącznik nr 3**;
 - 5) nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane i wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar instytucji (np. sprzedaż lub darowizna komputerów stacjonarnych/laptopów). Dyski twarde mogą zostać mechanicznie zniszczone przez firmę posiadającą do tego odpowiedni sprzęt i uprawnienia.

Rozdział XII

Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

1. Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

- 1) za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI
- 2) system antywirusowy zainstalowano na stacjach roboczych;
- 3) system antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików;
- 4) użytkownicy zobowiązani są do skanowania plików programem antywirusowym;
- 5) ASI zapewnia stałą aktywność programu antywirusowego tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe;
- 6) aktualizacja definicji wirusów odbywa się automatycznie przez program antywirusowy.
- 7) w przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

- 1) za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI;
- 2) Na stacjach roboczych powinien być stosowany firewall sprzętowy oraz firewall programowy.

Rozdział XIII

Procedura wykonywania przeglądów i konserwacji

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

1. Przeglądy i konserwacje systemu informatycznego i aplikacji

- 1) przegląd i konserwacja systemu informatycznego powinny być wykonywane w czasie rutynowych prac ASI;
- 2) ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków;
- 3) ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email;
- 4) ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia;
- 5) przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
 - a) wymontować nośniki z danymi osobowymi,
 - b) trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
 - c) nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

2. Aktualizacje oprogramowania

ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stłODOlności nowych wersji (np. aktualizacje, service pack-i, łatki).

3. Archiwizacja oprogramowania

Archiwizacja oprogramowania, odbywa się cyklicznie, na pisemne polecenie Dyrektora Ośrodka.

4. Dziennik administratora

ASI dokumentuje pracę w dzienniku administratora – **załącznik nr 4**.

9

Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.
3. Każdorazowe przemieszczenie komputera przenośnego poza siedzibę Ośrodka musi być poprzedzone usunięciem wszelkich danych osobowych z tego komputera i zabezpieczeniem ich w siedzibie Ośrodka. (na dysku serwera, lub innym nośniku elektronicznym)
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym administratora bezpieczeństwa informacji, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
 - a) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru.
 - b) zabrania się przewożenia komputera przenośnego np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach, zniszczeniem w przypadku nagłego hamowania.
6. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zapoznałem się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuje się do przestrzegania zasad w nim zawartych

Podpis Użytkownika

.....



Załącznik nr 2
do Instrukcji zarządzania systemem informatycznym
Ochrony Danych Osobowych
w Ośrodku Pomocy Społecznej Radzionkowie

Rejestr podmiotów zewnętrznych

Lp.	Nazwa firmy	Zakres świadczonych usług	Numer umowy	Uwagi



Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym
Ochrony Danych Osobowych
w Ośrodku Pomocy Społecznej Radzionkowie

Protokół zniszczenia uszkodzonych nośników

..... dnia

Protokół nr zniszczenia uszkodzonych nośników komputerowych

.....
(jednostka, komórka organizacyjna XXX)

Dnia komisja powołana przez
(data) (imię, nazwisko i stanowisko osoby
powołującej komisję)

w składzie:

1. Przewodniczący:
2. Członkowie:

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

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

9

Załącznik nr 4 do Instrukcji zarządzania systemem informatycznym
Ochrony Danych Osobowych
w Ośrodku Pomocy Społecznej Radzionkowie

Dziennik Administratora Systemu Informatycznego

Lp.	Data	Godzina	Opis wydarzenia w systemie	Podpis administratora

Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą

	Zagrożenie: 1			Zagrożenie: 2			Zagrożenie: 3		
	P	S	R	P	S	R	P	S	R
P-Prawdopodobieństwo incydentu (od 0 do 4)									
S-Skutki wystąpienia incydentu (od 1 do 5)									
R-Ryzyko wystąpienia incydentu (od 0 do 20)									
Formuła: R=P*S									
dyskryminacja									
kradzież tożsamości									
oszustwo dot. tożsamości									
strata finansowa									
naruszenie dobrego imienia									
naruszenie poufności danych osobowych chronionych tajemnicą zawodową									
przypadkowe lub niezgodne z prawem zniszczenie danych									
przypadkowa lub niezgodna z prawem utrata danych									
przypadkowe lub niezgodne z prawem zmodyfikowanie danych									
nieuprawnione ujawnienie danych									
nieuprawniony dostęp do danych									
Złamanie poufności									
Złamanie dostępności									
Złamanie integralności									
Złamanie odporności									

Zagrożenia dla osób fizycznych

1. Uwagi, spostrzeżenia, opis zagrożeń dla danej czynności przetwarzania:

2. Zarządzanie ryzykiem (minimalizacja ryzyka, przeniesienie ryzyka, akceptacja ryzyka):

A handwritten signature in blue ink, consisting of a stylized, cursive letter 'e' with a long tail that loops back to the top of the letter.

Prawdopodobieństwo	Poziom	Opis
Prawie pewne	4	zdarzenie występuje co najmniej raz w miesiącu
Prawdopodobne	3	zdarzenie występuje co najmniej raz w kwartał
Możliwe	2	zdarzenie występuje co najmniej raz pół roku
Mało prawdopodobne	1	zdarzenie występuje co najmniej raz na rok
Rzadkie	0	zdarzenie nie występuje

Skutek	
Bardzo wysoki	5
Wysoki	4
Średni	3
Niski	2
Bardzo niski	1

<ul style="list-style-type: none"> ✓ Poziom ryzyka akceptowany: 0-5 działania utrzymujące akceptowany poziom ryzyka ✓ Poziom ryzyka alarmowy: 6-10 działania mogą zostać przesunięte w czasie, wymaga okresowego monitorowania ✓ Poziom ryzyka nieakceptowalny: 11-15 Działanie może być przesunięte w czasie, ale ryzyko wymaga stałego monitorowania ✓ Poziom ryzyka nietolerowany: 16-20 poziom wymaga natychmiastowego działania
--

KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 13 ust. 1 i ust. 2 oraz art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

- 1) Administratorem Pani/Pana danych osobowych jest Dyrektor Ośrodka Pomocy Społecznej w Radzionkowie z siedzibą w Radzionkowie ul. Kużaja 19.
- 2) Wszelkie informacje w zakresie przetwarzanych danych osobowych można uzyskać w siedzibie Ośrodka Pomocy Społecznej w Radzionkowie ul. Kużaja 19 - Sekretariat I Piętro tel. 32 286-65-44 wew. 24
- 3) Pani/Pana dane osobowe przetwarzane będą w celu: przyznania wnioskowanej w formularzu formy pomocy;
- 4) odbiorcą Pani/Pana danych osobowych będą instytucje prawnie umocowane na podstawie przepisów ustawowych przy udzielaniu wnioskowanej formy pomocy.
- 5) Pani/Pana dane osobowe będą/ nie będą* przekazywane do państwa trzeciego/organizacji międzynarodowej;
- 6) Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do wykonania przedmiotowych czynności administracyjnych. Okres przechowywania dokumentacji jest wskazany w obowiązującym dla OPS Jednolitym Rzeczym Wykazie Akt., za wyjątkiem sytuacji gdzie przepisy szczególne wydłużają ten okres.
- 7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (**jeżeli przetwarzanie odbywa się na podstawie zgody*), którego dokonano na podstawie zgody przed jej cofnięciem;
- 8) ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
- 9) podanie przez Pana/Panią danych osobowych jest (*wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy**). Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie: *brak możliwości przyjęcia wniosku o pomoc*;
- 10) Pani/Pana dane będą przetwarzane papierowo i elektronicznie.

Potwierdzam zapoznanie się z treścią klauzuli informacyjnej:

* niewłaściwe skreślić

.....
Data i podpis



Zgoda na przetwarzanie danych osobowych

Czy zgadzasz się na przetwarzanie Twoich danych osobowych zamieszczonych w niniejszym formularzu przez Ośrodek Pomocy Społecznej w Radzionkowie, z siedzibą w Radzionkowie ul. Kuźaja 19, w celu przyznania wnioskowanej formy pomocy?

TAK

NIE

Artykuł 4.11 RODO

"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;

Artykuł 7 RODO

Warunki wyrażenia zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Preambuła (32) Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

.....
Data i podpis osoby wyrażającej zgodę

