Zarządzenie Nr 08.2018
Kierownika
Miejsko-Gminnego Ośrodka Pomocy Społecznej w Okonku
z dnia 09 kwietnia 2018 roku

w sprawie: wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w zakresie Przetwarzania Danych Osobowych.

Na podstawie art.36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. z 2016 r. poz. 922 z późn. zm.) oraz § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

§1

Wprowadzam w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Okonku **Politykę Bezpieczeństwa**, której treść stanowi **załącznik nr 1** do zarządzenia oraz **Instrukcję Zarządzania Systemem Informatycznym**, której treść stanowi **załącznik nr 2** do zarządzenia.

§2

Zobowiązuję wszystkich pracowników Miejsko-Gminnego Ośrodka Pomocy Społecznej w Okonku do zapoznania się, przestrzegania i stosowania Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym pod rygorem konsekwencji służbowych, przewidzianych prawem.

§3

Z dniem wejścia w życie niniejszego zarządzenia traci moc zarządzenie nr 35/2011 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Okonku z dnia 30 grudnia 2011 r. w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Miejsko-Gminnego Ośrodka Pomocy Społecznej w Okonku ".

§3

Zarządzenie wchodzi w życie z dniem podjęcia.

KIEROWNIK
M-GOPS w Okonku
mgr Brygida Kotschy

Załącznik nr 1
do Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

POLITYKA BEZPIECZEŃSTWA

Administrator Danych Kierownik Miejsko – Gminnego Ośrodka Pomocy Społecznej
Dnia 09.04.2018 r. w podmiocie o nazwie Miejsko – Gminny Ośrodek Pomocy Społecznej w Okonku

Zgodnie z **ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI**
z dnia 29 kwietnia 2004 r.

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

wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie z dniem 09.04.2018 r.

§1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Okonku, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę,

o których mowa w art. 3, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych decydujące o celach i środkach przetwarzania danych osobowych,

7. administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w § 1, chyba, że Administrator Danych sam wykonuje te czynności.
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową.

§3

Administrator Danych nie wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§4

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 1.**

§5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa" nr 2.**

§6

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa" nr 3.**

§7

W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§8

Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**. **Administrator Danych** stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, które stanowi **załącznik do „Polityki Bezpieczeństwa" nr 4**. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik do „Polityki Bezpieczeństwa" nr 5.**
2. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - **załącznik do „Polityki Bezpieczeństwa" nr 6.**

§9

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§10

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Wzór umowy stanowi **załącznik do „Polityki Bezpieczeństwa" nr 7.**

§11

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§12

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych, oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

§13

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa danych osobowych i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym wydziałów, placówek, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
5. Celem Polityki jest przetwarzanie - zgodnie z przepisami - danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy

przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.
8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
   b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
   c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
   d) monitorowanie zastosowanych środków ochrony;
   e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
   f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.
9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Okonku
mgr Brygida Kotschy

.....

Podpis

Załącznik nr 1
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Wykaz budynków, pomieszczeń lub części pomieszczeń,
tworzących obszar, w którym przetwarzane są dane osobowe
(zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.)

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Wydział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	MGOPS ul. Leśna 46, 64-965 Okonek	Wydział Świadczeń, Wydział Pomocy Środowiskowej i Wsparcia Rodziny	1	Fizyczne, techniczne.	
		Wydział Świadczeń	2	Fizyczne, techniczne.	
		Wydział Pomocy Środowiskowej i Wsparcia Rodziny	3	Fizyczne, techniczne.	
		Wydział Pomocy Środowiskowej i Wsparcia Rodziny	4	Fizyczne, techniczne.	
		Wydział Księgowości, Kadr i Organizacji	5	Fizyczne, techniczne.	
		Wydział Pomocy Środowiskowej i Wsparcia Rodziny	7	Fizyczne, techniczne.	
		Kierownik MGOPS	8	Fizyczne, techniczne.	
		Wydział Księgowości, Kadr i Organizacji	Zakładowa Składnica Akt	Fizyczne,	
2.	ul. Spokojna 1, 64-965 Okonek	Ośrodek Wsparcia Dzienny Dom „Senior – Wigor"	5	Fizyczne,	
3.	ul. Leśna 40 64-965 Okonek	Warsztaty Terapii Zajęciowej	biuro	Fizyczne, techniczne.	
		Warsztaty Terapii Zajęciowej	Pokój psychologa	Fizyczne, techniczne.	

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Okonku
mgr Bryg[illegible]tschy

.....
podpis

Załącznik nr 2
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Wykaz zbiorów danych osobowych
wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
(zgodnie, z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.)

UWAGA: Wszystkie przetwarzane zbiory danych osobowych występują w postaci papierowej.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Uwagi
1.	Pomoc Społeczna	POMOST Std, SEPI, Wywiad+, World, Progmann Finanse DDJ	
2.	Świadczenia Rodzinne	Sygnity (SR, FA, SW, ST, DM, DE), SEPI	
3.	Dodatki Mieszkaniowe i Energetyczne	Sygnity (SR, FA, SW, ST, DM, DE),	
4.	Zaliczki alimentacyjne	Zbiór w postaci papierowej	Zbiór przechowywany w Zakładowej Składnicy Akt
5.	Fundusz Alimentacyjny	Sygnity (SR, FA, SW, ST, DM, DE),	
6.	Program 500 +	Sygnity (SR, FA, SW, ST, DM, DE),	
7.	Stypendia Szkolne	Sygnity (SR, FA, SW, ST, DM, DE),	
8.	Zespół Interdyscyplinarny Gminy Okonek	Zbiór w postaci papierowej	
9.	Karta Dużej Rodziny	Ewidencja i obsługa wniosku na stronie https://kdr.mpips.gov.pl/start/	
10.	Warsztat Terapii Zajęciowej	Zbiór w postaci papierowej	
11.	Ustawa o wspieraniu rodziny i systemie pieczy zastępczej	Zbiór w postaci papierowej	
12.	Miejsko – Gminna Komisja Rozwiązywania Problemów Alkoholowych w Okonku	Zbiór w postaci papierowej	
13.	Za życiem	Sygnity (SR, FA, SW, ST, DM),	
14.	Wielkopolska Karta Rodziny	Ewidencja i obsługa wniosku na stronie http://www.wkr.rops.poznan.pl/	
15.	Kadry i wynagrodzenia	Finanse DDJ, (Finanse, Kadry, Zlecone, Płace, Wyposażenie, Gratyfikant), HOME BANKING	Zbiór nie podlega zgłoszeniu w GIODO

Administrator Danych Osobowych
KIEROWNIK
M-GOPS w Okonku
.....
mgr Brygida Kotschy
podpis

Załącznik nr 3
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami
(zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.)

Dane osobowe w poniższych zbiorach przetwarzane są w zakresie niezbędnym do realizacji zadań obejmują: Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, nr PESEL, serię i nr dowodu osobistego lub innego dokumentu tożsamości, nr telefonu. Ponadto w poszczególnych zbiorach przetwarzane są następujące dane:

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z internetu)	Uwagi
1.	Pomoc Społeczna	Dane o rodzinie, sytuacja zawodowa, sytuacja finansowa, źródło dochodów, zobowiązania alimentacyjne, zobowiązania finansowe, sytuacja mieszkaniowa, sytuacja majątkowa, nr rachunku bankowego, stan zdrowia, nałogi, informacje dotyczące orzeczeń wydanych w postępowaniach sądowych lub administracyjnym	Wydruk z platformy SEPI, Wydruk list wypłat kasowych i przelewowych z programu POMOST, Przekazanie informacji do ZUS za pośrednictwem programu PŁATNIK, Wydruki księgowe z programu FINANSE DDJ. Realizacja przelewów bankowych poprzez HOME BANKING	
2.	Świadczenia Rodzinne	Stan cywilny, pokrewieństwo, dane o rodzinie, sytuacja finansowa – wysokość dochodów, sytuacja zdrowotna, zawodowa, stan zdrowia, orzeczenia wydane w postępowaniu sądowym lub administracyjnym, nr rachunku bankowego	Wydruk list wypłat kasowych i przelewowych z programu ŚWIADCZENIA RODZINNE (Sygnity SR), Przekazanie informacji do ZUS za pośrednictwem programu PŁATNIK, Wydruki księgowe z programu FINANSE DDJ Realizacja przelewów bankowych poprzez HOME BANKING	
3.	Dodatki Mieszkaniowe i Energetyczne	Dane o osobach zamieszkujących z wnioskodawcą, stan cywilny, pokrewieństwo, wysokość dochodów, sytuacja zawodowa, mieszkaniowa (tytuł prawny do lokalu, warunki mieszkaniowe, wydatki) sytuacja majątkowa, zdrowotna, dane z umów sprzedaży energii elektrycznej, nr rachunku bankowego	Wydruk list wypłat kasowych i przelewowych z programu DODATKI MIESZKANIOWE I ENERGETYCZNE (Sygnity DM i DE), Wydruki księgowe z programu FINANSE DDJ Realizacja przelewów bankowych poprzez HOME BANKING	
4.	Zaliczki alimentacyjne	Imiona rodziców, miejsce urodzenia, stan cywilny, dane o współmałżonku, stan cywilny, dane o współmałżonku,	Zbiór przechowywany w Zakładowej Składnicy Akt	

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z internetu)	Uwagi
		dzieciach, osobach zobowiązanych do alimentacji, sytuacja finansowa – wysokość dochodów, stan i przyczyny bezskutecznej egzekucji, stan zdrowia, orzeczenia wydane w postępowaniach sądowych lub administracyjnych, nr rachunku bankowego		
5.	Fundusz Alimentacyjny	Imiona rodziców, miejsce urodzenia, stan cywilny, dane o współmałżonku, stan cywilny, dane o współmałżonku, dzieciach, osobach zobowiązanych do alimentacji, sytuacja finansowa – wysokość dochodów, stan i przyczyny bezskutecznej egzekucji, stan zdrowia, orzeczenia wydane w postępowaniach sądowych lub administracyjnych, nr rachunku bankowego	Wydruk list wypłat kasowych i przelewowych z programu FUDUSZ ALIMENTACYJNY (Sygnity FA), Wydruki księgowe z programu FINANSE DDJ, Realizacja przelewów bankowych poprzez HOME BANKING, Komunikacja systemu SYGNITY FA z Biurami Informacji Gospodarczej (KBIG, Infomonitor, KRD, ERIF, KIDT)	
6.	Program 500 +	Stan cywilny, pokrewieństwo, dane o rodzinie, sytuacja finansowa – wysokość dochodów, sytuacja zdrowotna, zawodowa, stan zdrowia, orzeczenia wydane w postępowaniu sądowym lub administracyjnym, nr rachunku bankowego	Wydruk list wypłat kasowych i przelewowych z programu FUDUSZ ALIMENTACYJNY (Sygnity FA), Wydruki księgowe z programu FINANSE DDJ, Realizacja przelewów bankowych poprzez HOME BANKING	
7.	Stypendia Szkolne	Dane o osobach wspólnie zamieszkujących, sytuacja dochodowa rodziny, sytuacja zawodowa, miejsce pobierania nauki, nr rachunku bankowego, sytuacja zdrowotna	Wydruk list wypłat kasowych i przelewowych z programu STYPENDIA SZKOLNE (Sygnity ST), Wydruki księgowe z programu FINANSE DDJ, Realizacja przelewów bankowych poprzez HOME BANKING,	
8.	Zespół Interdyscyplinarny Gminy Okonek	Stan cywilny, obywatelstwo, dane o współmałżonku, dzieciach, sytuacja mieszkaniowa, informacje o interwencjach policji, pobytach w izbach wytrzeźwień, nałogach, informacje dotyczące skazań, orzeczeń o ukaraniu innych orzeczeń wydanych w postepowaniu sądowym lub administracyjnym	Zbiór ma charakter ewidencji w postaci papierowej	
9.	Karta Dużej	informacje o współmałżonkach oraz	Komunikacja ze stroną (obsługa	

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z internetu)	Uwagi
	Rodziny	dzieciach, dane o miejscy nauki, informacje o niepełnosprawności,	wniosku oraz ewidencja) https://kdr.mpips.gov.pl/start/ oraz wydruki danych z tej strony	
10.	Warsztat Terapii Zajęciowej	Miejsce zamieszkania, dane dotyczące niepełnosprawności, informacje o sytuacji mieszkaniowej, warunkach bytowych, dane opiekunów prawnych i faktycznych, nr telefonów	Zbiór ma charakter ewidencji w postaci papierowej	
11.	Ustawa o wspieraniu rodziny i systemie pieczy zastępczej	Imiona rodziców, sytuacja zawodowa, stan cywilny, źródła dochodu, dane o warunkach mieszkaniowych, sytuacji prawnej, stan zdrowia, nałogi, dane z orzeczeń sądowych lub administracyjnych w tym o ukaraniu.	Zbiór ma charakter ewidencji w postaci papierowej	
12.	Miejsko – Gminna Komisja Rozwiązywania Problemów Alkoholowych w Okonku	Dane z orzeczeń sądowych lub administracyjnych, informacje o działaniach policji, Zespołu Interdyscyplinarnego ds. Przeciwdziałania Przemocy w Rodzinie, informacje o nałogach	Zbiór ma charakter ewidencji w postaci papierowej	
13.	Za życiem	Stan cywilny, pokrewieństwo, dane o rodzinie, sytuacja zdrowotna, zawodowa, stan zdrowia, orzeczenia wydane w postępowaniu sądowym lub administracyjnym, nr rachunku bankowego	Wydruk list wypłat kasowych i przelewowych z programu ŚWIADCZENIA RODZINNE (Sygnity SR), Wydruki księgowe z programu FINANSE DDJ, Realizacja przelewów bankowych poprzez HOME BANKING	
14.	Wielkopolska Karta Rodziny	informacje o współmałżonkach oraz dzieciach, dane o miejscy nauki, informacje o niepełnosprawności,	Komunikacja ze stroną (obsługa wniosku oraz ewidencja) http://www.wkr.rops.poznan.pl/ oraz wydruki danych z tej strony	
15.	Kadry i wynagrodzenia	Imiona rodziców, stan cywilny, zawód, wykształcenie, wysokość wynagrodzenia, nr rachunku bankowego, dane o przebiegu zatrudnienia i o zwolnieniach lekarskich, dane o dzieciach, związkach małżeńskich, stan zdrowia.	Realizacja przelewów bankowych poprzez HOME BANKING, Przekazanie informacji do ZUS za pośrednictwem programu PŁATNIK, Wydruki księgowe z programu FINANSE DDJ	

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Okonku

.....

podpis

mgr Brygida Kotschy

Załącznik nr 4
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Upoważnienie do przetwarzania danych osobowych
zgodnie z art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Kierownik Miejsko – Gminnego Ośrodka Pomocy Społeczne w Okonku jako Administrator Danych

dnia ..... nadaje upoważnienie do przetwarzania danych osobowych

w podmiocie **MIEJSKO – GMINNY OŚRODEK POMOMCY SPOŁECZEJ W OKONKU** dla:

Imię i nazwisko: .....

Adres zamieszkania:.....

Nr PESEL: .....

Stanowisko służbowe:.....

Upoważniony otrzymuje dostęp do poniższych zbiorów danych (nazwa zgodnie z załącznikiem nr 3 do **„Polityki Bezpieczeństwa"**) osobowych w celu ich przetwarzania:

.....

.....

Upoważnienie nadaje się do dnia .....

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Administrator Danych Osobowych

.....
podpis

Użytkownik

KIEROWNIK
M-GOPS w Okonku
mgr Brygida Kotsdny

.....
podpis

Załącznik nr 5
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie
(zgodnie z art 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.)

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*
1.	Krzysztof Kobacki	Kierownik WPŚiWR			Zbiory nr 1,8,9,11,14 wg załącznika nr 2	kkobacki – POMOST STD 3031053_user05 - https://kdr.mpips.gov.pl/start/
2.	Monika Kubacka	Asystent Rodziny			Zbiory nr 8,9,11,14 wg załącznika nr 2	3031053_user03 - https://kdr.mpips.gov.pl/start/ MKubacka - http://www.wkr.rops.poznan.pl/
3.	Piotr Słojewski	Pracownik socjalny			Zbiór nr 1 wg załącznika nr 2	slojewski – POMOST STD ZLO_MGOPSOK- SEPI
4.	Katarzyna Czapilińska	Specjalista pracy socjalnej			Zbiór nr 1 wg załącznika nr 2	Czaplińska – POMOST STD kczaplińska - SEPI
5.	Teresa Popowicz	Specjalista pracy socjalnej			Zbiór nr 1 wg załącznika nr 2	Popowicz – POMOST STD
6.	Izabela Wajda	Pracownik socjalny			Zbiór nr 1 wg załącznika nr 2	wajda – POMOST STD
7.	Małgorzata Barejko	Specjalista pracy socjalnej			Zbiór nr 1 wg załącznika nr 2	barejko – POMOST STD
8.	Dorota Jasnowska	Starszy Inspektor			Zbiory nr 2,3,4,5,6,7,12 wg załącznika nr 2	DJ – Sygnity (SR, FA, SW, ST, DM),
9.	Agnieszka Chwieduk	Starszy Inspektor			Zbiory nr 2,4,5,6,13 wg załącznika nr 2	SR - Sygnity (SR, FA, SW, ST, DM), 82051309949 - INFOMONITOR
10.	Ewa Gubow	Kierownik Wydziału Świadczeń			Zbiory nr 2,3,4,5,6,7,13 wg załącznika nr 2	EG - Sygnity (SR, FA, SW, ST, DM), egubow – SEPI, 277E72132E – KRD 82122206061 - INFOMONITOR

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*
11.	Danuta Noga	Główny Księgowy			Zbiory nr 1,2,3,4,5,6,7,13,15 wg załącznika nr 2	Nadzorca – HOME BANKING MGOPS-DDJ (Finanse)
12.	Aneta Pluchrat	Starszy Inspektor			Zbiory nr 1,2,3,4,5,6,7,13,15 wg załącznika nr 2	-
13.	Krsytyna Hark	Kierownik WTZ			Zbiory nr 10,15 wg załącznika nr 2	
14.	Danuta Adamczyk	Księgowa WTZ			Zbiory nr 10,15 wg załącznika nr 2	Ad – HOME BANKING administrator – DDJ(Finanse) Szef Jakub –DDJ (Gratyfikant)
15.	Beata Srebr	Instruktor Terapii Zajęciowej - Koordynator domu			Zbiór nr 1, wg załącznika nr 2	-
16.	Magdalena Balicka	Instruktor Terapii Zajęciowej			Zbiór nr 10, wg załącznika nr 2	-
17.	Anna Korzeniowska	Instruktor Terapii Zajęciowej			Zbiór nr 10, wg załącznika nr 2	-
18.	Maja Andrzejewska	Instruktor Terapii Zajęciowej			Zbiór nr 10, wg załącznika nr 2	-
19.	Elżbieta Mikita	Psycholog			Zbiór nr 10, wg załącznika nr 2	-
20.	Karolina Szwałek	Instruktor Terapii Zajęciowej - Opiekun domu			Zbiór nr 1, wg załącznika nr 2	-
21.	Natalia Herudaj	Instruktor Terapii Zajęciowej			Zbiór nr 10, wg załącznika nr 2	-
22.	Krzysztof Jędrzejowski	Pomoc administracyjna			Zbiór nr 1,2,6 wg załącznika nr 2	jędrzejowski – POMOST STD

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Opatówku
mgr Brygida Kotschy

.....
podpis

Załącznik nr 6
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
(zgodnie z art. 36 ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.)

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. ADO wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie stosują adekwatne środki techniczne i organizacyjne (środki ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.
3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ADO.
4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
5. Środki ochrony, zastosowane przez ADO dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring),
   - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS),
   - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym).

6. Zastosowane środki ochrony fizycznej pomieszczeń:
   a) MGOPS w Okonku wyposażono w elektroniczny system antywłamaniowy z całodobowym monitoringiem sygnału alarmu. System został objęty stałym nadzorem specjalistycznym firmy ochroniarskiej.
   b) Główne wejście do budynków lub obszarów budynków zajmowanych przez MGOPS w Okonku zamykane są przy użyciu drzwi antywłamaniowych zamykanych na dwa zamki mechaniczne.
   c) Zakładowa Składnica Akt zamykana jest przy użyciu drzwi antywłamaniowych zamykanych na dwa zamki mechaniczne.
   d) Drzwi do pomieszczeń w których znajdują się zbiory danych, serwery oraz węzły sieci wyposażono w zamki mechaniczne.
   e) Papierowe zbiory danych osobowych, oraz serwery i komputery przenośne przechowywane są w zamykanych na zamek w szafach.

7. Zastosowane środki techniczne obejmują:
   a) serwery plików oraz wybrane urządzenia systemu informatycznego są zabezpieczone przed krótkotrwałym brakiem zasilania z sieci elektrycznej poprzez zasilacze awaryjne UPS,
   b) wszystkie stacje robocze systemu informatycznego zabezpiecza się poprzez zainstalowanie programu antywirusowego oraz poprzez zainstalowanie oprogramowania firewall (zapora sieciowa).

8. Zastosowane środki organizacyjne obejmują:
   a) wprowadzenie Instrukcji zarządzania systemem informatycznym w tym w szczególności zasad tworzenia kopii zapasowych danych oraz zasad postępowania z hasłami uwierzytelniania dostępu dla osób upoważnionych do przetwarzania zbiorów danych osobowych,
   b) zapoznanie osób upoważnionych do przetwarzania zbiorów danych osobowych ze sposobami postępowania

dotyczącego ochrony danych osobowych przed osobami postronnymi oraz ich zabezpieczeniem we własnym zakresie na stanowisku pracy.

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.
W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogą ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Okonku
mgr Brygida Kotschy

.....

podpis

Załącznik nr 7
do „Polityki Bezpieczeństwa"
Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

Wzór
Umowa powierzenia przetwarzania danych osobowych nr.....

Załącznik do umowy Nr.....

Zawarta w dniu ..... r. w ..... pomiędzy:

.....
.....
.....
.....
zwanym w dalszej części niniejszej umowy „Zleceniodawcą"

reprezentowanym przez:

.....

a

.....
.....
.....
.....
zwanym w dalszej części niniejszej umowy „Wykonawcą"

reprezentowanym przez:

.....

o następującej treści:

§1

Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy (.....)a (.....), o ..... (np. świadczeniu usług kadrowych) Zleceniodawca powierza Wykonawcy trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2014 r. poz. 1182 z późn. zm.) zwanej dalej „ustawą" przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o ..... (np. pracownikach).
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w §2.

§2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   a) imię i nazwisko,
   b) numer ewidencyjny PESEL,
   c) seria i numer dowodu osobistego,
   d) ..... .
2. Celem przetwarzania danych jest ..... (np. realizacja obsługi kadrowo-płacowej).
3. Zakres przetwarzania obejmuje ..... (wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie) danych osobowych.
4. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 1 ust.1 i w sposób zgodny z niniejszą Umową.

§3

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w §2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39a ustawy.
2. Wykonawca oświadcza, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
   a) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   b) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają określony w Rozporządzeniu poziom bezpieczeństwa,
   c) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem

z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca,

d) do wykonania czynności objętych umową dopuszcza jedynie osoby posiadające imienne upoważnienia wraz z klauzulą poufności i posiadające odpowiednią wiedzę z zakresu ochrony danych osobowych.

3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
   a) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
   b) każdym nieupoważnionym dostępie do danych osobowych,
   c) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
9. Wykonawca może „pod powierzyć" usługi objęte umową, o której mowa w §1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy.

§4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie, ujawnienie, przekazanie 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 powierzenia

1. Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia ..... .

§6

Warunki wypowiedzenia i rozwiązania Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   a) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   b) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   c) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   d) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.

2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

3. Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8

Postanowienia końcowe

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu cywilnego.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

za Zleceniodawcę za Wykonawcę

KIEROWNIK
M-GOPS w Ciechanowcu
mgr Brygida Kotschy

Załącznik nr 2
do Zarządzenia Nr 08.2018
Kierownika M-GOPS w Okonku
z dnia 09 kwietnia 2018 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych **Kierownik Miejsko-Gminnego Ośrodka Pomocy Społecznej w Okonku**

Dnia 09.04.2018 r. w podmiocie o nazwie **Miejsko – Gminny Ośrodek Pomocy Społecznej**

Zgodnie z **ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI**
z dnia 29 kwietnia 2004 r.

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem 09.04.2018 r.

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.);
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§1

Za przestrzeganie w podmiocie **Miejsko – Gminny Ośrodek Pomocy Społecznej w Okonku** zapisów „instrukcji" odpowiedzialny jest Administrator Danych.

§2

W związku z tym, że w podmiocie **Miejsko – Gminny Ośrodek Pomocy Społecznej w Okonku** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1) W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

   w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   - poprzez zainstalowanie programu antywirusowego,
   - poprzez zainstalowanie firewall (zapora sieciowa),
   - poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2) W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na miesiąc.

4) Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym (nr pokoju, nazwa działu) pokój nr 5 „Księgowość i Kadry" zaopatrzonym w system alarmowy oraz monitoring realizowany przez Centrum Monitorowania i Grupę Interwencyjną „EXPERT" R. Kowalski i M. Kowalska Sp. jawna. ul. Królowej Jadwigi 36, 77-400 Złotów

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu,

b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2) Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4) W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku

braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Danych monitoruje i zapewnia realizację przeglądów technicznych sprzętu informatycznego w podmiocie oraz dba o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok.

§6

W przypadku stwierdzenia przez **Administratora Danych** uchybień dotyczących przetwarzania danych w podmiocie wprowadza takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§7

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Administrator Danych Osobowych

KIEROWNIK
M-GOPS w Okonku
mgr Brygida Kotschy

.....

podpis