Zarządzenie Nr 6/2018

Kierownika Miejskiego Ośrodka Pomocy Społecznej w Brzezinach

z dnia 14 września 2018 r.

w sprawie wprowadzenia w Miejskim Ośrodku Pomocy Społecznej w Brzezinach zasad ochrony przetwarzania danych osobowych

Na podstawie § 7 Regulaminu organizacyjnego Miejskiego Ośrodka Pomocy Społecznej w Brzezinach oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 24 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 WE (ogólne rozporządzenie o ochronie danych), zarządzam, co następuje:

§ 1.

Zasady ochrony przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Brzezinach określone zostały w załącznikach do niniejszego zarządzenia:

1. Obowiązki Administratora Danych Osobowych – zał. nr 1.
2. Klauzula informacyjna dot. wprowadzenia w MOPS zasad przetwarzania i ochrony danych osobowych opartych o Rozporządzenie o Ochronie Danych Osobowych - zał. nr 2.
3. Instrukcja zarządzania Systemem informatycznym w MOPS - zał. nr 3.
4. Wykaz budynków i pomieszczeń, gdzie prowadzi się przetwarzanie danych osobowych, zał. nr 4.
5. Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym MOPS Brzeziny – zał. nr 5.
6. Upoważnienie do przetwarzania danych osobowych z oświadczeniem o zachowaniu poufności – zał. nr 6.
7. Odwołanie upoważnienia do przetwarzania danych osobowych – zał. nr 7.
8. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych w MOPS Brzeziny – zał. nr 8.
9. Upoważnienie do przetwarzania danych osobowych w pracach Zespołu Interdyscyplinarnego lub grupy roboczej wraz z oświadczeniem o zachowaniu poufności - zał. nr 9.
10. Opis struktury zbioru danych osobowych stanowiący zał. nr 10.
11. Wykaz zbiorów danych osobowych - zał. nr 11.
12. Regulamin korzystania z zasobów informatycznych MOPS Brzeziny - zał. nr 12.
13. Zasoby techniczne i organizacyjne ochrony przetwarzania danych osobowych – zał. nr 13.
14. Procedura sprawdzenia czytelności nośników kopii zapasowych – zał. nr 14.
15. Zasady korzystania ze sprzętu komputerowego i oprogramowania – zał. nr 15.
16. Umowa powierzenia przetwarzania danych osobowych – zał. nr 16 .

§ 2.

Nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz zabezpieczenia obiektu, pomieszczeń i sprzętu służącego do przetwarzania danych osobowych w MOPS Brzeziny powierzam Inspektorowi Ochrony Danych Osobowych.

§ 3.

Traci moc Zarządzenie Nr 10/2014 z dnia 21 listopada 2014r. w sprawie wprowadzenia Polityki Bezpieczeństwa w Miejskim Ośrodku Pomocy Społecznej w Brzezinach.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

Kierownik MOPS Brzeziny
Administrator Danych

Zał. nr 1.

Obowiązki Administratora Danych Osobowych

Administrator Danych osobowych zobowiązany jest do:

1. Zapewnienia, aby dane osobowe były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów,
   c) merytorycznie poprawne i adekwatne w stosunku do celów.
2. Wyznaczenia Inspektora Ochrony Danych Osobowych, odpowiedzialnego za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowania instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określenia budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowania instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzenia ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizowania szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Określania w zakresach czynności osób zatrudnionych przy przetwarzania danych osobowych odpowiedzialność tej osoby za:
   a) ochronę danych przed niepowołanym dostępem,
   b) nieuzasadnioną modyfikację lub zniszczenie danych,
   c) nielegalne ujawnienie danych.
9. Prowadzenia rejestr zbiorów danych osobowych.

Zał. nr 2

KLAUZULA INFORMACYJNA

Niniejszym informujemy, że Administratorem Danych Osobowych jest Miejski Ośrodek Pomocy Społecznej Brzeziny z siedzibą w Brzezinach przy ulicy Św. Anny nr 57 (zwany dalej „MOPS").

W MOPS wyznaczono Inspektora Ochrony Danych Osobowych, z którym można skontaktować się pod numerem telefonu (46) 874 12 95, następującym adresem korespondencyjnym: IODO MOPS Brzeziny, 95-060 Brzeziny ul. Św. Anny nr 57 lub za pośrednictwem adresu e-mail: mopsbrzeziny@brzeziny.pl

MOPS będzie przetwarzać Pani (Pana) dane:

- w celu realizowania obowiązków ustawowych na podstawie art. 6 ust. 1 lit. c ,d, e rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych (Dz.Urz.UE.L Nr 119, str. 1; zwane dalej „RODO"). Administrator wymaga podania wyłącznie danych osobowych niezbędnych do realizacji swoich zadań;
- podstawą prawną dla przetwarzania Pani (Pana) danych osobowych jest :
  - wypełnienie obowiązku ciążącego na Administratorze,
  - ochrona żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
  - wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Podanie przez Panią (Pana) danych osobowych jest dobrowolne, ale stanowi warunek niezbędny do rozpatrzenia Pani (Pana) sprawy przez MOPS.

Konsekwencją nie podania tych danych będzie brak możliwości wykonywania przez MOPS obowiązków ustawowych.

Państwa dane osobowe przechowywane będą przez okres niezbędny do zrealizowania uprawnień lub spełnienia obowiązku wynikającego z przepisów prawa i rozliczeń po jego zakończeniu; wykonywania obowiązków prawnych przez MOPS; w którym przepisy nakazują nam przechowywać dane; w którym możemy ponieść konsekwencje prawne niewykonania obowiązków wynikających z przepisów prawa.

W niektórych sytuacjach mamy prawo przekazywać Pani (Pana) dane, jeśli będzie to konieczne do dochodzenia praw i obowiązków wynikających z obowiązujących przepisów prawa.

Dane osobowe mogą być przekazywane wyłącznie osobom upoważnionym przez MOPS tj. pracownikom i współpracownikom, którzy muszą mieć dostęp do danych aby wykonywać swoje obowiązki, podmiotom przetwarzającym, którym zlecimy to zadanie, innym odbiorcom danych np. kurierom (placówkom pocztowym), bankom, ubezpieczycielom, kancelariom prawnym lub instytucjom upoważnionym z mocy prawa do otrzymania przedmiotowych danych.

Informujemy, że przysługuje Pani (Panu) prawo do żądania dostępu do gromadzonych przez MOPS danych osobowych, ich sprostowania oraz prawo do wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do przenoszenia danych.

Na czynności MOPS związane z przetwarzaniem danych osobowych można wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych.

Udostępnione przez Panią (Pana) dane nie będą podstawą do zautomatyzowanego podejmowania decyzji, w tym nie będą podlegały profilowaniu.

Informujemy także, że nie mamy zamiaru przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Zał. nr 3

Instrukcja zarządzania Systemem informatycznym do przetwarzania danych osobowych.

§ 1

Instrukcję opracowano na podstawie art.13 i 29 Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r.w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego „RODO".

§ 2

1. W Miejskim Ośrodku Pomocy Społecznej w Brzezinach funkcję Administratora Danych pełni Kierownik Ośrodka.
2. Administrator Danych wykonuje czynności organizacyjno – prawne związane z ochroną danych osobowych.
3. Administrator Danych wydaje upoważnienia do przetwarzania danych osobowych..
4. Administrator Danych wyznacza Administratora Systemu.
5. Administrator Danych wyznacza Inspektora Ochrony Danych Osobowych (w skrócie IODO).
6. Administrator Danych prowadzi rejestr zbiorów zawierających dane osobowe.
7. W terminie 14 dni od chwili powstania nowych zbiorów zawierających dane osobowe pracownicy poszczególnych komórek zgłaszają do IODO ten fakt na piśmie w celu wpisania ich do rejestru danych osobowych.
8. Administrator Danych prowadzi kontrolę papierowych zbiorów danych osobowych.

§ 3

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych, które zapoznały się z przepisami dotyczącymi ochrony danych osobowych oraz podpisały stosowne oświadczenie.
2. Upoważnienia do przetwarzania danych osobowych wydaje i prowadzi ich ewidencję Administrator Danych.
3. Zastępca Kierownika, pracownicy Ośrodka oraz IODO informują Administratora Danych o wszelkich sytuacjach powodujących konieczność cofnięcia upoważnienia do przetwarzania danych osobowych w celu zablokowania w systemie możliwości przetwarzania danych.
4. Ewidencja wydanych upoważnień do przetwarzania danych osobowych zawiera:
   a) imię i nazwisko osoby upoważnionej,
   b) datę nadania oraz zakres upoważnienia do przetwarzania danych osobowych,
   c) identyfikator, jeżeli dane osobowe są przetwarzane w systemie informatycznym.
5. Na podstawie wydanego upoważnienia Administrator Danych dokonuje rejestracji uprawnień w systemie informatycznym.
6. Osoby, które zostały upoważnione do przetwarzania danych są obowiązane do zachowania w tajemnicy te dane oraz sposób ich zabezpieczenia.

§ 4

1. Dla każdego użytkownika upoważnionego do przetwarzania danych osobowych w systemie informatycznym Administrator Systemu ustala odrębny identyfikator i hasło.
2. Użytkownik po otrzymaniu hasła zobowiązany jest do niezwłocznej jego zmiany podczas pierwszej rejestracji w Systemie, funkcja ta jest ustawiona w Systemie i wymuszana jest automatycznie.
3. Bezpośredni dostęp do danych osobowych przetwarzanych w Systemie może mieć miejsce przez podanie własnego identyfikatora i prawidłowego hasła.
4. Długość hasła nie może być krótsza niż 8 znaków.
5. Zmiana hasła następuje nie rzadziej niż co 30 dni, funkcja jest ustawiona w Systemie i wymusza dokonanie jego zmiany po wygaśnięciu okresu obowiązywania, w przypadku nie dokonania zmiany hasła, System automatycznie blokuje konto użytkownika podczas próby 3 logowania.
6. W razie problemów z logowaniem do Systemu użytkownik powinien zwrócić się do Administratora Systemu.
7. Identyfikator nie jest zmieniany i nie może być przydzielony innemu użytkownikowi w przypadku wyrejestrowania użytkownika z Systemu.
8. Wyrejestrowanie użytkownika z Systemu następuje przez unieważnienie jego hasła.
9. Hasła dostępu do Systemu użytkownicy mają zachować w ścisłej tajemnicy.
10. Zabrania się przechowywania haseł w biurkach, szufladach, na karteczkach w pobliżu komputera oraz przekazywania ich innym osobom.
11. W przypadku utraty tajności hasła należy dokonać jego natychmiastowej zmiany.
12. Identyfikator Administratora Systemu oraz hasło ma być przechowywane w szafie metalowej.

§ 5

1. Godziny rozpoczęcia i zakończenia pracy w MOPS Brzeziny określa Regulamin Pracy.
2. Rozpoczęcie przetwarzania danych w Systemie następuje poprzez włączenie komputera i podanie własnego identyfikatora i prawidłowego hasła. W przypadku chwilowej przerwy w pracy użytkownik powinien wylogować się z Systemu celem uniemożliwienia dostępu do Systemu osób do tego nieupoważnionych, zaleca się także stosowanie wygaszacza ekranu zabezpieczonego hasłem.

§ 6

1. Kopie zapasowe w Systemie informatycznym powinny być wykonywane codziennie w cyklu tygodniowym przez Administratora Systemu lub przez osobę przez niego wyznaczoną.
2. Dane z serwerów zapisywane są na płytach, dane archiwalne z bazą programów finansowo-księgowych i kadrowo-płacowych zapisywane są codziennie na płytach CD.

3. Kopie programów służących do przetwarzania danych osobowych powinny być przechowywane w szafie metalowej.
4. Kopie zapasowe powinny być przechowywane w szafach zamykanych.
5. Elektroniczne nośniki informacji, wydruki z systemu zawierające dane osobowe przechowuje się w szafach zamykanych a po utracie ważności okresu przechowywania lub przydatności powinno się usunąć ich zawartość w sposób trwały, uniemożliwiający ich ponowne odtworzenie.
6. Minimalny okres przechowywania danych archiwalnych wynosi co najmniej 5 lat.

§ 7

1. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do Systemu informatycznego przez:
   a) wydzielenie sieci wewnętrznej bez dostępu do Internetu, w której przetwarzane są dane osobowe,
   b) wprowadzenie zakazu samodzielnej instalacji przez użytkowników dowolnego oprogramowania,
   c) instalację na serwerze i stacjach roboczych oprogramowania antywirusowego,
   d) wprowadzenie systemu identyfikatorów i haseł dostępu do sieci wewnętrznej i programów przetwarzających dane osobowe.
2. Odczyt danych z wymiennych nośników informatycznych (np. stacji CD, stacji dyskietek, przenośnych dysków, kart pamięci itp.) dopuszcza się wyłącznie poprzez wcześniejsze sprawdzenie zawartości na obecność wirusów komputerowych oraz innego, szkodliwego oprogramowania na komputerach posiadających oprogramowanie antywirusowe.
3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie na serwerze oraz przy stacjach roboczych zasilaczy awaryjnych.
4. Dopuszcza się przetwarzanie danych osobowych na komputerach przenośnych, użytkowanych wyłącznie do celów służbowych i zabezpieczonych przez ich zaszyfrowanie.
5. Przynoszenie na teren Ośrodka i podłączanie do sieci wewnętrznej prywatnych urządzeń komputerowych jest zabronione.

§ 8

Konserwacja i naprawa baz danych zawierających dane osobowe dokonywana jest na podstawie odrębnych umów. Naprawa i konserwacja dokonywana jest w przypadkach konieczności dokonania zmian w strukturze bazy, w oprogramowaniu wynikających z dostosowania do zmieniających się przepisów, modyfikacją rozszerzającą funkcjonalność lub naprawy błędów mogących wystąpić w trakcie pracy. W przypadku konieczności przekazywania do naprawy urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe, Administrator Systemu pozbawia wcześniej zapis tych danych w sposób uniemożliwiający ich odzyskanie.

Zał. nr 4

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

Lp.	Dokładny adres	Nazwa pomieszczenia	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	**Miejski Ośrodek Pomocy Społecznej w Brzezinach ul. Św. Anny 57**				
		Sekcja świadczeń rodzinnych i wychowawczych	2	Pomieszczenie wyposażone w system alarmowy przeciwwłamaniowy, zamykane na klucz	
		Fundusz alimentacyjny	3	Pomieszczenie wyposażone w system alarmowy przeciwwłamaniowy, zamykane na klucz	
		Pracownicy socjalni	4	Pomieszczenie wyposażone w system alarmowy, przeciwwłamaniowy, zamykane na klucz	
		Pracownicy socjalni Asystent rodziny	5	Pomieszczenie wyposażone w system alarmowy przeciwwłamaniowy, zamykane na klucz	

Lp.	Dokładny adres	Nazwa pomieszczenia	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
		Pracownicy socjalni	6	Pomieszczenie wyposażone w system alarmowy, przeciwwłamaniowy, zamykane na klucz	
		Sekcja świadczeń pomocy społecznej	7	Pomieszczenie wyposażone w system alarmowy, przeciwwłama-niowy, zamykane na klucz	
		Księgowość	8	Pomieszczenie wyposażone w system alarmowy, przeciwwłama- niowy, zamykane na klucz	
		Kierownik Ośrodka	9	Pomieszczenie wyposażone w system alarmowy przeciwwłamaniowy, zamykane na klucz	
		Sekcja świadczeń pomocy społecznej Sekretariat	10	Pomieszczenie wyposażone w system alarmowy, przeciwwłama- niowy, zamykane na klucz	
2	**Świetlica Środowiskowo – Terapeutyczna „Świetlik" w Brzezinach ul. Sienkiewicza 11**				
				Pomieszczenie z oknem okratowanym,	

Lp.	Dokładny adres	Nazwa pomieszczenia	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
		Pomieszczenie wychowawców	1	zamykane na klucz	
3	**Dzienny Dom „Senior +" w Brzezinach ul. Sportowa 1**				
		Pokój pielęgniarski (administracja Domu)	1	Pomieszczenie wyposażone w system alarmowy, zamykane na klucz, wejście do Domu zabezpieczone zamkiem kodowanym	
		Pokój indywidualnej terapii zajęciowej	2	Pomieszczenie wyposażone w system alarmowy, zamykane na klucz, wejście do Domu zabezpieczone zamkiem kodowanym	

Zał. nr 5

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym MOPS Brzeziny

lp.	nazwisko i imię pracownika	identyfikator użytkownika	data uzyskania dostępu	zakres dostępu	podpis	data utraty dostępu	podpis
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Zał. Nr. 6

Upoważnienie do przetwarzania danych osobowych

Administrator Danych ..... dnia .....

nadaje upoważnienie do przetwarzania danych osobowych

w Miejskim Ośrodku Pomocy Społecznej w Brzezinach dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

.....

.....

.....

.....

Upoważnienie ważne jest na czas zatrudnienia w Miejskim Ośrodku Pomocy Społecznej w Brzezinach na określonym stanowisku pracy bądź do odwołania.

Upoważniony zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych. Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń zarówno w okresie zatrudnienia jak i po jego ustaniu.

.....

Data i podpis Administratora Danych

Zał. Nr 7

IDENTYFIKATOR .....

Odwołanie Upoważnienia do przetwarzania danych osobowych

Administrator Danych ..... dnia .....

Odwołuje upoważnienie do przetwarzania danych osobowych
w Miejskim Ośrodku Pomocy Społecznej w Brzezinach dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Nadane dnia ..... dotyczące dostępu do zasobów danych osobowych
.....

.....

.....

.....

Data i podpis Administratora Danych

Zał. nr 8

Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych w MOPS Brzeziny.

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik MOPS w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora danych lub Inspektora Ochrony Danych Osobowych.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku naruszenia ochrony danych osobowych, Administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 rozporządzenia RODO, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
6. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi danych.
7. Zgłoszenie o którym mowa w ust. 5, musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

8. Administrator danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
9. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
10. Zawiadomienie, o którym mowa w ust.1, niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c), i d) rozporządzenia RODO.
11. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
    1) Administrator danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
    2) Administrator danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 5.
    3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
12. Jeżeli Administrator danych nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że został spełniony jeden z warunków, o których mowa w ust. 11.
13. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych lub Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
    1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
    2) inicjuje ewentualne działania dyscyplinarne,
    3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
    4) dokumentuje prowadzone postępowania.
14. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych lub Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
    1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
    2) zabezpiecza ewentualne dowody,
    3) ustala osoby odpowiedzialne za naruszenie,
    4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
    5) inicjuje działania dyscyplinarne,
    6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
    7) dokumentuje prowadzone postępowania.

Zał. nr 9

Brzeziny, dnia.....

UPOWAŻNIENIE
do przetwarzania danych osobowych w pracach Zespołu Interdyscyplinarnego lub grupy roboczej.

Na podstawie art. 9 c ustawy z dnia 26 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (Dz.U. 2005.1390 j.t.) oraz art. 29 Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego „RODO" upoważniam Panią/Pana :

.....
(imię i nazwisko członka Zespołu Interdyscyplinarnego lub grupy roboczej)

.....
(nazwa instytucji, placówki, którą reprezentuje)

do przetwarzania danych osobowych w związku z prowadzeniem prac Zespołu lub grupy roboczej.

.....
Kierownik MOPS Brzeziny
Administrator Danych Osobowych

Zał. nr 10

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

Lp.	Nazwa zbioru danych	Struktura zbiorów	Przepływ danych	Uwagi
1.	Świadczenia Rodzinne i Fundusz Alimentacyjny	Opisana jest na stronie www.empatia.mpips.gov.pl	Opisany jest na stronie www.empatia.mpips.gov.pl	
2.	Pomoc społeczna	Opisana jest na stronie www.empatia.mpips.gov.pl www.agemasi.pl www.zus.pl	Opisana jest na stronie www.empatia.mpips.gov.pl www.agemasi.pl www.zus.pl	

Zał. nr 11

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych	Uwagi
1.	Świadczenia rodzinne	SYGNITY – oprogramowanie Świadczenia Rodzinne i Fundusz Alimentacyjny	
		HOME BANKING	
		Płatnik	
2	Pomoc społeczna	POMOST STD	
		Płatnik	
		SJO Bestia	
		AGEMA HR (Kadry płace)	
		AGEMA – FK (finansowo księgowy)	
		HOME BANKING	

.....

Kierownik MOPS. Administrator Danych Osobowych

Zał. nr 12

Regulamin korzystania z zasobów Informatycznych Ośrodka

	Regulamin obowiązuje wszystkich pracowników Miejskiego Ośrodka Pomocy Społecznej w Brzezinach, mający dostęp do systemu informatycznego	

Pkt.		Dotyczy
	1. Zasady ogólne	
1.1	Regulamin korzystania z zasobów Informatycznych Ośrodka obowiązuje wszystkich pracowników Ośrodka bez względu na formę zatrudnienia jak i osoby wykonujące prace na rzecz Ośrodka oraz wszystkie osoby korzystające z zasobów informatycznych Ośrodka.	Wszyscy
1.2	Pracownicy Ośrodka zobowiązują się do nie ujawniania informacji umieszczonych w bazach danych (w jakiejkolwiek formie), które stanowią tajemnicę służbową. Zachowanie tajemnicy obowiązuje każdego pracownika, również po ustaniu zatrudnienia.	Wszyscy
1.3	Do zasobów informatycznych mogą być dopuszczone jedynie osoby, które zostały zapoznane z przepisami dot. ochrony danych osobowych i obowiązującymi w tym zakresie instrukcjami. Fakt ten musi być potwierdzony podpisaniem przez pracownika stosownego oświadczenia. Podpisane oświadczenie przekazuje się do akt osobowych pracownika.	Pracownik prowadzący dokumentację kadrową
1.4	Zasoby informatyczne Ośrodka składają się wyłącznie z dopuszczonych do eksploatacji elementów. Zabrania się dołączania i używania sprzętu elektronicznego i nośników informacji nie będących własnością Ośrodka.	Wszyscy
1.5	Wszelkie czynności konfiguracyjne (zmiany ustawień, parametrów, modernizacja, instalacja) zarówno w sprzęcie informatycznym jak i oprogramowaniu może wykonywać tyko Administrator Systemu Informatycznego lub wyznaczona przez niego osoba/podmiot zewnętrzny.	Wszyscy
1.6	Zasoby informatyczne Ośrodka mogą być wykorzystywane wyłącznie do celów służbowych w ramach przydzielanych zadań i obowiązków.	Wszyscy
1.7	Informacje wysyłane i otrzymywane przez zasoby informatyczne a także wysyłane i otrzymywane za pomocą służbowej poczty elektronicznej, stanowią własność Ośrodka, dlatego też Ośrodek zastrzega sobie prawo do ich kontroli. Dotyczy to zarówno informacji i danych zawartych w służbowych komputerach oraz na służbowych nośnikach informacji, a także służbowej poczty elektronicznej.	Wszyscy
1.8	Zabrania się użytkownikom zasobów informatycznych pokonywania zabezpieczeń dostępu do jej zasobów, w tym również stosowania narzędzi programowych ułatwiających pokonywanie tych zabezpieczeń. Działania tego typu będą podlegały surowym sankcjom dyscyplinarnym.	Wszyscy
1.9	Opuszczenie stanowiska pracy na okres dłuższy niż 15 minut, powinno wiązać się ze stosownym zabezpieczeniem zasobów informatycznych (zablokowanie komputera lub wylogowanie, zamknięcie pomieszczenia, zapisanie danych w komputerze itp...)	Wszyscy

1.10	Dostęp do zasobów informatycznych Ośrodka następuje na wniosek bezpośredniego przełożonego pracownika.	Wszyscy
1.11	Administrator Systemu Informatycznego może w uzasadnionych przypadkach zablokować dostęp do poszczególnych zasobów pracownikom naruszającym niniejszy regulamin.	Administrator systemu
1.12	W pomieszczeniach w których przebywają osoby postronne, monitory komputerowe muszą być ustawione w sposób uniemożliwiający takiej osobie podejrzenie zawartości ekranu.	Wszyscy
1.13	Zabrania się udostępniania komputerów Ośrodka oraz wszelkich innych zasobów informatycznych osobom trzecim nie mającym zezwolenia lub upoważnienia Administratora Systemu. Dotyczy to również firm wykonujących wszelkie usługi na rzecz Ośrodka.	Wszyscy
	2. Oprogramowanie	
2.1	Można korzystać wyłącznie z oprogramowania i systemów dopuszczonych w Ośrodku do eksploatacji.	Wszyscy
2.2	Dopuszczone jest stosowanie lub wprowadzanie do systemu informatycznego aplikacji pod warunkiem przestrzegania warunków umowy licencyjnej oraz uzyskania pisemnej lub mailowej zgody od Administratora Systemu Informatycznego.	Wszyscy
2.3	Zabrania się korzystania z programów i systemów nie będących własnością Ośrodka lub nie dopuszczonych przez Ośrodek do użytkowania. Dotyczy to w szczególności: a) nielegalnego oprogramowania naruszającego prawa autorskie b) legalnego oprogramowania ale bez ważnej licencji c) programów załączonych do gazet, czasopism itp. instalowanych bez konsultacji z Administratorem Systemu Informatycznego	Wszyscy
2.4	Instalacji bądź deinstalacji oprogramowania może dokonać tylko Administrator Systemu Informatycznego bądź wyznaczona przez niego osoba.	Wszyscy
2.5	Na użytkowanie oprogramowania będącego własnością Ośrodka poza jej terenem może wyrazić zgodę tylko i wyłącznie Kierownik Ośrodka	Wszyscy
2.6	Każda instalacja bądź uruchomienie nowego oprogramowania musi być poprzedzone kontrolą antywirusową.	wszyscy

3. Hasła dostępu do systemów i sprzętu informatycznego		
3.1	Każdy użytkownik zasobów informatycznych musi posiadać unikalny identyfikator i hasło.	Administrator Systemu
3.2	Taki sam identyfikator użytkownika ze względu na historię nie może być przydzielony w przyszłości żadnej innej osobie.	Administrator Systemu
3.3	Zgłoszenie zapotrzebowania na założenie konta użytkownika do serwisów informatycznych musi zostać zatwierdzone przez Kierownika Ośrodka.	Wszyscy
3.4	Hasło użytkownika zna tylko i wyłącznie dany użytkownik. Zabrania się ujawniania haseł innym osobom, bez względu na funkcję i rangę.	Wszyscy
3.5	Jeżeli zaistniało podejrzenie ujawnienia hasła lub zostało ono ujawnione należy natychmiast zmienić je samemu (jeżeli jest taka możliwość) lub zgłosić ten fakt Administratorowi Systemu Informatycznego.	Wszyscy
3.6	Hasło użytkownika musi być zmieniane minimum raz na 30 dni i składać się z co najmniej z 8 znaków.	Wszyscy
3.7	Hasła powinny zostać zastosowane do: a) systemu operacyjnego (bezwzględnie) b) aplikacji (jeżeli zawiera ona dane osobowe bądź inne informacje podlegające ochronie w Ośrodku)	wszyscy
3.8	Nie zaleca się stosowania prostych haseł, które łatwo mogą być kojarzone z danym użytkownikiem typu: nazwisko, imię, numer samochodu, nazwa psa, imię dziecka itp. Tworząc hasło zaleca się włączenie do niego znaku numerycznego bądź z górnego rejestru oraz co najmniej jednej dużej oraz jednej małej litery Wq34u!a*	Wszyscy
3.9	Zabrania się zapisywania haseł w miejscach łatwo dostępnych takich jak na biurku, w szufladach na karteczkach w pobliżu komputera.	Wszyscy
3.10	Za ujawnienie hasła i wszystkie związane z tym konsekwencje ponosi odpowiedzialność użytkownik, którego hasło zostało ujawnione.	Wszyscy
3.11	Wprowadzając hasło użytkownik musi mieć pewność, że nie zostanie ono podejrzane przez osoby znajdujące się w pobliżu.	Wszyscy
3.12	Nowe hasło musi być różne od dwóch poprzednio używanych.	Wszyscy
3.13	Hasła administracyjne dotyczące szczególnie wysokich uprawnień powinny być zdeponowane w opisanych kopertach i przechowywane w sejfie.	wszyscy
3.14	Konta nieużywane przez okres dłuższy od 60 dni, zostaną automatycznie zablokowane lub usunięte. Odblokowanie lub stworzenie nowego konta użytkownika, powinno być poprzedzone zgłoszeniem do Administratora Systemu Informatycznego.	Wszyscy

4. Procedura rozpoczęcia, zawieszenia i zakończenia pracy		
4.1	Dane służbowe, których administratorem jest Miejski Ośrodek Pomocy Społecznej, mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań firmowych.	Wszyscy
4.2	Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu za pomocą identyfikatora i hasła).	Wszyscy
4.3	Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji lub w przypadku braku takiej w dokumentacji wg zasad opracowanych przez Administratora Systemu Informatycznego.	Wszyscy
4.4	Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz upewnieniu się, że stacja robocza została poprawnie wyłączona.	Wszyscy
4.5	Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.	Wszyscy
4.6	Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych a na których przetwarzane są dane osobowe powinny być ustawione w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.	Wszyscy
4.7	Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (niszczarka dokumentów).	Wszyscy
4.8	Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.	Wszyscy
4.9	Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.	Wszyscy
4.10	Użytkownik niezwłocznie powiadamia Administratora Systemu Informatycznego w przypadku braku możliwości zalogowania się na swoje konto.	Wszyscy

5. Poczta elektroniczna i zasady użytkowania		
5.1	Zabrania się używania prywatnych kont pocztowych bez zgody Administratora Systemu Informatycznego z wyłączeniem kont dostępnych poprzez przeglądarki WWW.	Wszyscy
5.2	Firmowe konto pocztowe może być wykorzystywane tylko i wyłącznie w celach służbowych.	Wszyscy
5.3	Zabrania się używania i podawania nazwy firmowego konta pocztowego na forach publicznych, grupach dyskusyjnych, blogach oraz innych serwisach, w których wymagana jest rejestracja użytkownika z podaniem firmowego adresu mailowego.	Wszyscy
5.4	Zabrania się stosowania mechanizmów poczty do lawinowego rozsyłania wiadomości.	Wszyscy
5.5	Zabrania się otwierania załączników poczty niewiadomego pochodzenia lub/i od nieznanego nadawcy.	Wszyscy
5.6	Podejrzane załączniki powinny być wykasowywane bez otwierania ich lub sprawdzone przed otwarciem aktualnym programem antywirusowym.	Wszyscy
5.7	Zabrania się wykorzystywania konta pocztowego do przesyłania plików uzyskanych z naruszeniem praw autorskich, bądź nie będącego własnością Ośrodka.	Wszyscy
5.8	Zalecane jest aby wielkość przesyłanych drogą mailową załączników była nie większa niż 5 MB.	Wszyscy
6. Internet		
6.1	Korzystanie z Internetu powinno służyć głownie do realizacji celów przydzielonych zadań służbowych w Ośrodku.	Wszyscy
6.2	Zabrania się pobierania z Internetu następujących plików i programów: a) z naruszeniem praw autorskich b) nie dopuszczonych w Ośrodku do eksploatacji c) dużej objętości mogących mieć wpływ na przeciążenie sieci d) wszelkich plików multimedialnych chronionych prawami autorskimi e) plików z sieci P2P (peer – 2 – peer) f) plików z sieci P2M (peer – 2 – mail) g) plików chronionych prawami autorskimi z portali, które umożliwiają hostowanie plików np. Megaupload, Rapidshare itp.	Wszyscy
6.3	Pobrane pliki i programy przed uruchomieniem muszą być sprawdzone aktualnym programem antywirusowym.	Wszyscy
6.4	Zabrania się wykorzystywania serwerów PROXY i stron świadczących usługi PROXY bez pozwolenia Administratora Systemu Informatycznego.	Wszyscy

7. Przenośny sprzęt informatyczny i nośniki elektroniczne		
7.1	Na terenie Ośrodka można używać wyłącznie nośników i sprzętu elektronicznego będącego własnością Ośrodka.	Wszyscy
7.2.	Zabrania się wnoszenia na teren Ośrodka prywatnego sprzętu i nośników elektronicznych lub urządzeń nie będących własnością Ośrodka. Tym samym nie zezwala się na korzystanie z przenośnych urządzeń takich jak pendrive, dysk USB, karty pamięci, laptop i innych, które nie należą do Ośrodka lub innych na których używanie nie wyraził zgody Kierownik Ośrodka.	Wszyscy
7.3	Przenośne urządzenia elektroniczne i nośniki danych powinny być szczególnie zabezpieczone podczas transportu. W szczególności: a) przechowywane w specjalnie dla nich stworzonych torbach, kasetach, pudełkach itp. b) nie pozostawiane bez opieki, w miejscach umożliwiających ich łatwe przejęcie. c) jeżeli urządzenie ma taką możliwość to powinno być zabezpieczone hasłem lub szyfrowane. d) nie narażane na szkodliwe dla nich czynniki takie jak silne pole elektromagnetyczne, wilgoć, ciepło itp.	Wszyscy
7.4	Przenośny sprzęt elektroniczny może być wykorzystywany poza Ośrodkiem tylko i wyłącznie za zgodą Kierownika Ośrodka.	Wszyscy
7.5	Utrata (zaginięcie, kradzież itp.) przenośnego sprzętu elektronicznego musi być niezwłocznie zgłoszona Kierownikowi Ośrodka .	Wszyscy
7.6	Przenośne komputery powinny mieć w miarę możliwości na bieżąco aktualizowaną ochronę antywirusową oraz polisy grupowe wprowadzane przez Administratora Systemu Informatycznego.	wszyscy
7.7	Uszkodzone elektroniczne nośniki informacji muszą być zdawane Kierownikowi Ośrodka.	Wszyscy
7.8	Zabrania się pozostawiania w Ośrodku nie zabezpieczonych przenośnych nośników i urządzeń elektronicznych.	Wszyscy

8. Bezpieczeństwo komputerowego stanowiska pracy		
8.1	W szczególności podczas codziennego użytkowania komputera powinno unikać się następujących sytuacji: a) spożywanie posiłków przy stanowisku pracy nad klawiaturą b) zasłanianie otworów wentylacyjnych sprzętu elektronicznego c) narażanie sprzętu elektronicznego na awarie wynikające z długotrwałego działania promieni słonecznych d) nieprawidłowego rozłożenie okablowania sieciowego i strukturalnego, które może stanowić zagrożenie dla sprzętu jak i użytkownika e) stawianie komputera w pozycji innej, niż fabrycznie zalecanej do pracy f) stawianie cieczy blisko urządzeń elektronicznych g) kładzenie przedmiotów na klawiaturze h) nie uprawnione otwieranie urządzeń elektronicznych z wyłączeniem sprzętu, który wymaga wymiany materiałów eksploatacyjnych i) podłączanie do tej samej sieci co urządzenia informatyczne przedmiotów takich jak czajniki elektryczne, dmuchawy, wentylatory itp. j) własnoręczne naprawy sprzętu elektronicznego	Wszyscy
9. Procedura złomowania sprzętu dla pracowników		
9.1	W przypadku awarii sprzętu elektronicznego należy niezwłocznie podjąć następujące kroki: a) zawiadomić o awarii Kierownika Ośrodka b) w przypadku nieobecności kierownika, należy zawiadomić zastępcę kierownika lub osobę pełniącą obowiązki, c) fizycznego odłączenia sprzętu elektronicznego może dokonać Administrator Systemu lub osoba przez niego upoważniona, d) każdy sprzęt komputerowy należy zdawać do Administratora Systemu/ kierownika Ośrodka, e) sprzęt będący na gwarancji należy zgłaszać zgodnie z zasadami przewidzianymi w dokumentacji gwarancyjnej, f) sprzęt pogwarancyjny w przypadku braku możliwości naprawy, powinien być zdawany Administratorowi Systemu,	Wszyscy

.....

Kierownik MOPS.

Administrator Danych Osobowych

Zał. nr 13

I. Zasoby organizacyjne i techniczne zapewniające ochronę przetwarzania danych osobowych

W celu właściwego zabezpieczenia przetwarzania danych osobowych wykorzystuje się następujące środki organizacyjne:

1. Administratorem Danych osobowych jest kierownik Ośrodka .
2. Administrator Danych wyznacza Inspektora Ochrony Danych Osobowych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych.
3. Administrator Danych wydaje upoważnienia do przetwarzania danych.
4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych.
5. Odwołanie upoważnienia do przetwarzania danych osobowych następuje na piśmie.
6. Dane przetwarzane są wyłącznie na terenie Ośrodka.
7. Osoby przetwarzające dane osobowe zobowiązane są do znajomości przepisów w tym zakresie.

II.

W celu właściwego zabezpieczenia przetwarzania danych osobowych wykorzystuje się następujące środki techniczne:

1. Zbiory danych osobowych przechowywane są w pomieszczeniach wyposażonych w system alarmowy przeciwwłamaniowy i zamkniętych na klucz.
2. Zbiory danych przetwarzane są na serwerze zabezpieczonym w szafie RACOWEJ w pomieszczeniu zamykanym drzwiami ognioodpornymi, antywłamaniowymi wyposażonymi w dwa zamki (kodowy i spustowy).
3. Zbiory danych przechowywane są w szafach zamkniętych.
4. Kopie zapasowe /archiwalne przechowywane są w szafach zamkniętych.
5. Zbiory danych osobowych są przetwarzane przy użyciu komputerów stacjonarnych.
6. Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową.
7. Dostęp do systemu operacyjnego komputera w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia przy użyciu identyfikatora użytkownika oraz hasła.
8. Zastosowano środki ochrony przed szkodliwym oprogramowaniem w postaci programów antywirusowych.

Zał. nr 14

Procedura sprawdzenia czytelności nośników kopii zapasowych

1. Wydobycie nośnika zawierającego kopie bezpieczeństwa (jeśli kopia tworzona jest na nośniku zewnętrznym)
2. Sprawdzenie możliwości odczytu danych zawartych w kopii bezpieczeństwa.
3. Odtworzenie plików i innych danych zawartych w kopii bezpieczeństwa.
4. Sprawdzenie poprawności i integralności danych zawartych w kopii bezpieczeństwa.
5. Ponowne złożenie danych w miejscu przechowywania kopii bezpieczeństwa.
6. Sporządzenie notatki służbowej.

Zał. nr 15

Zasady korzystania przez pracowników Miejskiego Ośrodka Pomocy Społecznej w Brzezinach ze sprzętu komputerowego i oprogramowania

1. Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe zainstalowane godnie z odpowiednimi regulaminami i wymogami prawnymi. Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.
2. Pracownik korzysta z Oprogramowania oraz z zasobów informatycznych tylko i wyłącznie w związku z wykonywaniem obowiązków pracowniczych.
3. Pracownik zobowiązuje się do nie ingerowania w system operacyjny bez wiedzy i pisemnej zgody Pracodawcy. Ingerencja w system informatyczny bez pisemnej zgody Pracodawcy będzie traktowana jako ciężkie naruszenie obowiązków pracowniczych wraz z konsekwencjami prawnymi z tego wynikającymi.
4. Do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
5. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny (t.j. Dz.U.2018r.poz.1600 ze zm.) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j.Dz.U.2018 poz.1191 ze zm.) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.
6. Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę łączącej Pracodawcę z Pracownikiem lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j.Dz.U.2018r. poz.917 ze zm.).

Zał. Nr 16

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia .....2018 roku w Brzezinach pomiędzy:

Miejskim Ośrodkiem Pomocy Społecznej w Brzezinach zwanym dalej „Administratorem" reprezentowanym przez Kierownika Teresę Kwiecień

a

zwanym w dalszej części umowy „Podmiotem przetwarzającym"

§ 1

Powierzenie przetwarzania danych osobowych

1.Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady UE 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 (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2.Podmiot przetwarzający 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.

3.Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1.Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane :

2.Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy z dnia .....

§3

Obowiązki podmiotu przetwarzającego

1.Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, 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.Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3.Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

4.Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5.Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie zgromadzone w celu wykonania umowy dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6.Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7.Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin liczonych od chwili stwierdzenia naruszenia.

§4

Prawo kontroli

1.Administrator zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2.Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.

3.Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 10 dni .

4.Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1.Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2.Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

3.Podwykonawca, o którym mowa w ust. 1 winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

4.Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1.Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2.Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§7

Czas obowiązywania umowy

1.Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania umowy na wykonywanie przez Podmiot przetwarzający obowiązków określonych w §2 ust.2 .

2.Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem okresu wypowiedzenia ustalonego w umowie na wykonywanie przez Podmiot przetwarzający czynności w §2 ust.2.

§8

Rozwiązanie umowy

1.Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b) przetwarza dane osobowe w sposób niezgodny z umową;

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1.Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").

2.Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1.Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

2.W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

3.Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych .

Administrator danych	Podmiot przetwarzający