Załącznik do Zarządzenia Dyrektora Miejskiego Ośrodka
Pomocy Rodzinie w Opolu Nr 44/2016 z dnia 7 listopada 2016 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI
W MIEJSKIM OŚRODKU POMOCY RODZINIE W OPOLU

I. WSTĘP

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich przetwarzania.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja zbiorów osobowych, miejsc ich przetwarzania.

Polityka Bezpieczeństwa została opracowana przez Administratora Danych, Miejski Ośrodek Pomocy Rodzinie w Opolu, zwany dalej również MOPR, w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa. Polityka Bezpieczeństwa wraz z Instrukcją Zarządzania Systemem Informatycznym oraz dokumentami w nich wskazanymi stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 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. Nr 100, poz. 1024). Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą. Każda osoba mającą dostęp do danych osobowych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby, o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

1. Informacje ogólne.

Podstawowym celem przygotowania i wdrożenia dokumentu Polityki Bezpieczeństwa jest zapewnienie zgodności działania Miejskiego Ośrodka Pomocy Rodzinie w Opolu z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Polityka Bezpieczeństwa w szczególności opisuje sposoby przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

2. Cel i zakres polityki bezpieczeństwa.

Polityka bezpieczeństwa rozumiana jest, jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz MOPR. Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych (w odniesieniu, do których w przypadku szczegółowych regulacji występuje odesłanie do zasad i procedur wskazanych w rozdziale IX. Na Politykę Bezpieczeństwa składają się następujące informacje:

- Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- Sposób przepływu danych pomiędzy poszczególnymi systemami,
- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa. Rygorowi Polityki Bezpieczeństwa podlegają także dane powierzone Miejskiemu Ośrodkowi Pomocy Rodzinie w Opolu do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych.

II. PODSTAWY PRAWNE

Poniżej opisano aktualne przepisy prawne w zakresie ochrony danych osobowych oraz wybrane, najważniejsze definicje i terminy.

1. Ustawa oraz akty wykonawcze.

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych. Pełną listę aktów prawnych stanowią:

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j. Dz. U. z 2016 r., poz. 922), dalej zwaną również u.o.d.o.,
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 225, poz. 1350 z późn. zm.) – art. 13 ust. 3 u.o.d.o.,
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 94, poz. 923 z późn. zm.) – art. 22a u.o.d.o.,
- Rozporządzenie 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) – art. 39a u.o.d.o.,

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536) – art. 46a u.o.d.o.,
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. z 2014 r. poz. 1934) art. 46f u.o.d.o.,
- Rozporządzenie Ministra Administracji I Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 20015 r., poz. 745) – art. 36a ust. 9 pkt 1 u.o.d.o.,
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych (Dz. U. z 2015 r., poz. 719) – art. 36a, ust. 9 pkt 2 u.o.d.o.

Niniejszy dokument powstał w oparciu o art. 36. ust. 2. oraz art. 39a ustawy o ochronie danych osobowych, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych. Szczegółowy zakres dokumentu określa Rozporządzenie 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 wydane do art. 39a u.o.d.o.

2. Definicje i objaśnienie terminów.

W dokumencie przyjmuje się następującą terminologię:

Generalny Inspektor Ochrony Danych Osobowych-organ do spraw ochrony danych osobowych.

Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Administrator danych (ADO)-organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Funkcję ADO w Miejskim Ośrodku Pomocy Rodzinie w Opolu pełni Dyrektor.

Administrator bezpieczeństwa informacji (ABI)-osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. ABI jest powoływany przez ADO.

Dane osobowe-wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe-dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Zbiór danych-każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Informatyk -osoba zatrudniona na stanowisku informatyka, upoważniona przez ADO do zarządzania systemem informatycznym.

Osoba Zarządzająca Zbiorem Danych Osobowych-osoba, która odpowiada za bieżące zarządzanie poszczególnymi zbiorami danych osobowych przetwarzanymi w strukturze Administratora Danych. Kierownicy komórek organizacyjnych MOPR lub osoby upoważnione do zastępowania kierownika pod jego nieobecność. Inne osoby z komórek organizacyjnych MOPR. Osoby takie są wyznaczane pisemnie przez ADO.

Przetwarzanie danych-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.

System informatyczny-zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym-wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą-oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie.

Identyfikator użytkownika-ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło-ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie-działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozliczalność-właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność danych-właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Poufność danych-właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

Dokumentacja przetwarzania danych-dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Sprawdzenie-czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem".

Sprawozdanie-dokument opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia, którego celem jest zweryfikowanie zgodności przetwarzania danych

Odbiorca danych-rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- Osoby, której dane dotyczą.
- Osoby upoważnionej do przetwarzania danych.
- Przedstawiciela podmiotu mającego siedzibę lub miejsce zamieszkania w państwie trzecim.
- Podmiotu, któremu administrator danych powierzył w drodze umowy przetwarzanie danych.
- Organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Polityka Bezpieczeństwa-dokument określający szczegółowe zasady ochrony danych osobowych stosowane w MOPR, zwaną „Polityką".

Pracownik-osoba zatrudniona w MOPR na podstawie umowy o pracę, umowy zlecenia, umowy o dzieło oraz osoba będąca stażystą, praktykantem, wolontariuszem. Osoba fizyczna, podmiot lub inna instytucja wykonująca usługi na rzecz MOPR mająca dostęp i/lub przetwarzająca dane osobowe.

Raport-przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.

Rozporządzenie-Rozporządzenie 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), zwane dalej „Rozporządzeniem".

Sieć publiczna-sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych**.**

Sieć telekomunikacyjna- systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju;

Teletransmisja-przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

Usuwanie danych-zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Państwo trzecie-państwo nienależące do Europejskiego Obszaru Gospodarczego.

III. ZASADY I ELEMENTY POLITYKI BEZPIECZEŃSTWA

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje całkowitej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych, pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych. W tym celu tworzy się:

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

Na podstawie § 4 pkt 2 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 tworzy się wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych służących do ich przetwarzania stanowiący załącznik nr 1 do niniejszej dokumentacji.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.

Na podstawie § 4 pkt 1 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 tworzy się wykaz budynków i pomieszczeń, tworzących obszar przetwarzania danych osobowych. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 2 do niniejszej dokumentacji.

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Na podstawie § 4 pkt 3 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 wprowadza się do załącznika nr 1 opis struktury poszczególnych zbiorów osobowych.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Na podstawie §4 pkt 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, dla zbiorów przetwarzanych w systemach teleinformatycznych, w przypadku przepływu danych pomiędzy systemami, wprowadza się opis sposobu przepływu danych pomiędzy poszczególnymi systemami. Sposób przepływu danych został opisany szczegółowo w rozdziale IX Polityki.

5. Ewidencja osób upoważnionych.

Wprowadza się ewidencję osób upoważnionych do przetwarzania danych. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku, kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu. Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych. Szczegółowy opis dotyczący Upoważnień do przetwarzania danych osobowych znajduję się w rozdziale VI Polityki bezpieczeństwa.

6. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, w MOPR w Opolu wprowadzono określa się środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przewarzanych danych. Szczegółowy opis zastosowanych rozwiązań został opisany w rozdziale VIII Polityki.

7. Charakterystyka możliwych zagrożeń.

W rozdziale scharakteryzowano możliwe do wystąpienia zagrożenia bezpieczeństwa.

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.
- **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych lub naruszenia ich poufności.

- **Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych. Zagrożenia te możemy podzielić na: nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione).

8. Potencjalne zagrożenia przetwarzania danych.

Poniżej przedstawiono listy potencjalnych zagrożeń bezpieczeństwa danych z podziałem na zagrożenia miejsc przetwarzania oraz rodzajów danych, tj. zbiorów przetwarzanych tradycyjnie (papierowo) oraz z wykorzystaniem systemów informatycznych. W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić Administratora danych.

Zagrożenia miejsc przetwarzania danych.

- Włamania od strony okien – wybite szyby, niedomknięte skrzydła.
- Włamania od strony drzwi – uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach.
- Oddziaływanie czynników zewnętrznych – wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana.
- Pozostawienie niezamkniętych drzwi lub okien, jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych.
- Pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach.

Zagrożenia związane z przetwarzaniem danych w zbiorach papierowych.

- Pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy.
- Pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze.
- Pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe.
- Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
- Przetwarzanie danych przez osoby nieuprawione.
- Nieuzasadnione sporządzanie kserokopii danych.

Zagrożenia związane z przetwarzaniem danych elektronicznych.

- Dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych.
- Dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią.
- Sporządzanie kopii danych w sytuacjach nie przewidzianych procedurą.
- Utrata kontroli nad kopią danych osobowych.
- Podmiana nośników z danymi osobowymi.
- Pozostawienie zapisanego hasła dostępu.
- Samodzielne instalowanie jakiegokolwiek oprogramowania.
- Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
- Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.
- Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych.
- Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
- Awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich.

- Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
- Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
- Próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej.
- Dopuszczanie, aby osoby inne niż Informatyk lub inne osoby uprawnione, podłączały jakikolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji.
- Ślady manipulacji przy układach sieci komputerowej lub komputerach.
- Obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.
- Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

9. Postępowanie z kluczami.

Klucze główne oraz alarm.

- Do otwierania i zamykania głównych drzwi wejściowych oraz do rozkodowywania i kodowania systemu alarmowego przed rozpoczęciem i po zakończeniu pracy uprawnione są osoby wyznaczone przez ADO.
- Osoby otrzymują kod do systemu alarmowego.
- Osoby, którym zostały powierzone klucze do głównych drzwi oraz kod systemu alarmowego są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim.

Klucze dostępowe do kaset lub szaf z kluczami do pomieszczeń

- Klucze do poszczególnych pomieszczeń znajdują się w zamykanych kasetach lub szafkach na klucze, do których dostęp mają wyznaczone przez ADO osoby.
- Osoby, które uzyskały dostęp do kaset lub szaf z kluczami są zobowiązane do zabezpieczania kluczy dostępowych do tych kaset lub szaf i wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim.

Klucze do pomieszczeń.

- Klucze do pomieszczeń, znajdujące się w kasetach lub szafach na klucze, wydawane są poszczególnym pracownikom, w tym personelowi obsługi, zgodnie z ich potrzebami wynikającymi z zakresu czynności lub niezbędnymi do wykonywania zadań służbowych.
- Osoby, które otrzymały klucze do pomieszczeń zobowiązane są do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim, a także do ich zabezpieczania w indywidualny, właściwy dla każdej sytuacji sposób, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.

Klucze do biurek stanowiskowych i szaf.

- Osoby mające dostęp do kluczy od biurek stanowiskowych, szaf biurowych, kas pancernych oraz sejfów, zobowiązane są do ich zabezpieczania w indywidualny, właściwy dla każdej sytuacji sposób, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.
- Osoby, mające dostęp do kluczy od biurek stanowiskowych, szaf biurowych, kas pancernych oraz sejfów są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim.

Duplikaty kluczy.

- Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń są przechowywane w wyznaczonym przez ADO miejscu.

- ADO wyznacza osobę odpowiedzialną za należyte przechowywanie, zabezpieczanie oraz udostępnianie kluczy zapasowych.
- Osoba wyznaczona ma obowiązek wydawać klucze zapasowe tylko w uzasadnionych sytuacjach.
- Klucze zapasowe po ich wykorzystaniu powinny być niezwłocznie zwrócone.

IV. ODPOWIEDZIALNOŚĆ ZA OCHRONĘ DANYCH OSOBOWYCH.

Miejski Ośrodek Pomocy Rodzinie w Opolu jest jednostką organizacyjną Gminy Miasta Opola i wykonuje zadania własne i zlecone z zakresu polityki społecznej. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki oraz Instrukcji odpowiadają w Miejskim Ośrodku Pomocy Rodzinie w Opolu: Administrator Danych Osobowych, Administrator Bezpieczeństwa Informacji, Osoby Zarządzające Zbiorami Danych, Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz MOPR, która uzyskała upoważnienie do przetwarzania danych osobowych.

1. Administrator Danych Osobowych.

Obowiązki ADO określone w Ustawie i Rozporządzeniu pełni Dyrektor Miejskiego Ośrodka Pomocy Rodzinie w Opolu. Każdorazowo ADO zgodnie z wewnętrznie obowiązującymi procedurami wyraża zgodę oraz akceptację na wszystkie działania ABI, w które zaangażowane są podmioty trzecie.

2. Administrator Bezpieczeństwa Informacji.

Administratorem Bezpieczeństwa Informacji w MOPR jest osoba powołana przez ADO. Do zadań Administratora Bezpieczeństwa Informacji należy w szczególności:

- Zapewnienie przestrzegania przepisów o ochronie danych o ochronie danych osobowych i innymi przepisami prawa.
- Sprawdzanie zgodności przetwarzania danych osobowych z przepisani u.o.d.o. oraz opracowanie w tym zakresie sprawozdania dla ADO.
- Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, zgodnie z wymogami określonymi w Ustawie.
- Udostępnianie rejestru, o którym mowa powyżej, na stronie internetowej ADO, przy czym na stronie głównej MOPR umieszczone jest odwołanie umożliwiające bezpośredni dostęp do rejestru.
- Udostępnienie, w siedzibie ADO, do wglądu każdemu zainteresowanemu rejestru w postaci papierowej.
- Opracowanie planu sprawdzeń określających przedmiot poszczególnych sprawdzeń, zakres czynności, które będą podjęte w toku sprawdzenia oraz termin przeprowadzenia sprawdzenia.
- Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych osobowych.
- Zgłaszanie zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zgłaszanie wniosków o wykreślenie zbioru z rejestru zbiorów danych prowadzonego przez ww. organ, jeśli zachodzi konieczność dokonania takich czynności w odniesieniu do danego zbioru danych osobowych,
- Stały nadzór nad treścią Polityki, Instrukcji oraz innych dokumentów związanych z ochroną danych osobowych stosowanych w MOPR oraz aktualizacja i modyfikacja ww. dokumentów,

- Udzielanie odpowiedzi na zapytania kierowane do MOPR przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
- Prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach,
- Nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
- Monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych,
- Opiniowanie w sprawie możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru lub przetwarzania danych w innym celu niż ten, dla którego dane zostały zebrane,
- Opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych,
- Przygotowywanie lub opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych lub decyzji w kwestii udostępnienia danych osobowych ze zbiorów,
- Wydawanie pisemnych zaleceń wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z Ustawą, Rozporządzeniem, Polityką oraz Instrukcją,
- Kontrola przetwarzania i stanu zabezpieczenia danych osobowych przetwarzanych w MOPR,
- Inicjatywa i nadzór nad wdrażaniem w MOPR nowych rozwiązań w zakresie zabezpieczenia danych osobowych,
- Przechowywanie papierowej wersji dokumentacji z zakresu przetwarzania i ochrony danych osobowych,
- Przygotowywanie upoważnień do przetwarzania danych osobowych, wydawanych przez ADO.

3. Informatyk.

Do uprawnień i obowiązków Informatyka należą w szczególności:

- Administrowanie systemem informatycznym,
- Nadawanie uprawnień do przetwarzania danych osobowych w systemach informatycznych, w tym nadawanie identyfikatorów użytkownika i haseł dostępu,
- Nadawanie identyfikatorów użytkownikom przetwarzającym dane w systemach informatycznych,
- Informowanie ABI o nadaniu identyfikatora użytkownikom systemów informatycznych, w celu nadania stosownych upoważnień do przetwarzania danych osobowych,
- Stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej,
- Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
- Kontrola systemu antywirusowego,
- Kontrola awaryjnego zasilania komputerów,
- Kontrola i wykonywanie kopii awaryjnych,
- Konserwacja oraz uaktualnienia systemów informatycznych,
- Nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

- Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
- Identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
- Sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji,
- Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
- Podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w Instrukcji,
- Informowanie ABI o konieczności wprowadzenia zmian w Instrukcji (z powodu np. zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych),
- Informatyk pozostaje w stałym kontakcie z ABI i jest przez niego na bieżąco informowany o zmianach procedur związanych z ochroną danych osobowych w MOPR oraz zmianach przepisów prawnych związanych z ochroną danych osobowych.
- Informowanie na bieżąco ABI o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego,
- Przedstawianie ADO ewentualnych potrzeb w zakresie zabezpieczeń danych osobowych w systemie informatycznym.

4. Osoby zarządzające zbiorem danych osobowych.

1. Zarządzającymi Zbiorami Danych Osobowych są osoby, które odpowiadają za bieżące zarządzanie poszczególnymi zbiorami danych osobowych przetwarzanymi w strukturze Administratora Danych. Osoby takie są wyznaczane pisemnie przez ADO.
2. Zarządzający Zbiorem Danych Osobowych jest instruowany przez ABI. W ramach szkolenia jest on zapoznawany z ogólnymi zagadnieniami związanymi z ochroną danych osobowych oraz szczegółowymi procedurami związanymi z ochroną danych osobowych w MOPR, a w szczególności związanymi z zarządzanymi zbiorami danych osobowych.
3. Dla każdego zbioru danych musi zostać wyznaczona jedna osoba pełniąca obowiązki Zarządzającego Zbiorem Danych Osobowych, przy czym możliwe jest pełnienie przez jedną osobę funkcji Zarządzającego Zbiorem Danych Osobowych w stosunku do kilku zbiorów danych osobowych.
4. Zarządzający Zbiorem Danych Osobowych jest zobowiązany do ścisłej współpracy z ABI w zakresie przetwarzania danych osobowych w zarządzanym przez niego zbiorze danych, a w szczególności zobowiązany jest do wykonywania zaleceń w dziedzinie bezpieczeństwa przetwarzania danych.
5. Do uprawnień i obowiązków Zarządzającego Zbiorem Danych Osobowych należą w szczególności:
   - Zgłaszanie do ABI zamiaru zbierania danych osobowych i utworzenia zbioru, bądź jego nowego elementu oraz konsultowanie kwestii zamiaru wprowadzenia w zbiorze zmian w zakresie: sposobu zbierania oraz udostępniania danych, celu i zakresu przetwarzania danych, miejsca przetwarzania danych, zmiany formy przetwarzania danych, zaprzestania przetwarzania, usunięcia danych ze zbioru lub zniszczenia zbioru danych oraz zastosowanych zabezpieczeń związanych z jego przetwarzaniem,

- Udzielanie ABI oraz innym pracownikom upoważnionym do przetwarzania danych osobowych wyjaśnień w sprawie zarządzanych przez niego zbiorów oraz konsultowanie z nimi odpowiedzi na wszelkie zapytania w tej kwestii kierowane przez podmioty zewnętrzne,
- Występowanie z wnioskiem do ADO o nadanie upoważnień osobom przetwarzającym dane osobowe w nadzorowanych przez nich zbiorach, zgodnie z procedurą obowiązującą w MOPR,
- Nadzór nad wdrożeniem i stosowaniem fizycznych środków zabezpieczenia obszarów, w których przetwarzane są dane osobowe zawarte w zbiorze, którym zarządza,
- Udział w wewnętrznym postępowaniu kontrolnym oraz w postępowaniu kontrolnym prowadzonym przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych w odniesieniu do zarządzanego przez niego zbioru,

4. Pracownicy MOPR posiadający dostęp do danych osobowych.

1. Każdy pracownik MOPR, który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia i Polityki.
2. Dostęp do określonego zbioru danych osobowych pracownik MOPR uzyskuje na podstawie pisemnego upoważnienia.
3. Pracownicy zatrudnieni - na podstawie umowy o pracę, bądź świadczący usługi na podstawie umów cywilnoprawnych (w tym także stażyści oraz praktykanci MOPR) - przy przetwarzaniu danych osobowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera oświadczenie o znajomości zasad bezpieczeństwa przetwarzania danych.
4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi naruszenie obowiązków pracowniczych.

V. OBOWIĄZKI INFORMACYJNE PRZY PRZETWARZANIU DANYCH OSOBOWYCH.

1. Zbieranie danych osobowych od osób, których dane dotyczą.

W przypadku zbierania danych osobowych od osoby, której te dane dotyczą ADO jest zobowiązany poinformować tę osobę o:

- Adresie swojej siedziby i pełnej nazwie,
- Celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- Prawie dostępu do treści swoich danych oraz ich poprawiania,
- Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

2. Zbieranie danych osobowych nie od osób, których dane dotyczą.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

- Adresie swojej siedziby i pełnej nazwie,
- Celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
- Źródle danych,
- Prawie dostępu do treści swoich danych oraz ich poprawiania,
- Prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
- Prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad nie stosuje się, jeżeli:

- Przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- Dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,
- Osoba, której dane dotyczą, posiada informacje, o których mowa powyżej.

3. Przetwarzanie danych.

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwie, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
- Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
- Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
- Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Przetwarzanie danych jest zabronione w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także

innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Przetwarzanie tych danych jest jednak dopuszczalne, jeżeli:

- Osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba, że chodzi o usunięcie dotyczących jej danych,
- Przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- Przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
- Jest to niezbędne do wykonania **s**tatutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych, niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
- Przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
- Przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
- Przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- Przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
- Jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,
- Przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

4. Zgłaszanie przetwarzanych danych.

Powołany przez Dyrektora MOPR ABI, został zgłoszony do rejestru GIODO. W takim przypadku, zgodnie zapisami ustawy, zgłoszeniu nie podlegają zbiory tworzone w MOPR, które nie zawierają danych wrażliwych. Wszystkie inne zbiory podlegają zgłoszeniu do rejestru.

5. Powierzanie przetwarzania danych.

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla MOPR, ADO może powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- Umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,
- Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,
- Podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych określone w Ustawie. W

zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych,

- Odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy Ustawy.

6. Prawa osób, których dane dotyczą.

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych MOPR, a zwłaszcza prawo do:

- Uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy.
- Uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze.
- Uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych.
- Uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba, że ADO jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej.
- Uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.
- Żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
- Wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację.
- Wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy ADO przetwarza dane niezgodnie z przeznaczeniem.

Jeżeli, dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, ADO może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.

Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić informacji, odnośnie do jej danych osobowych. Na wniosek osoby, której dane dotyczą, informacji udziela się na piśmie.

ADO odmawia osobie, której dane dotyczą, udzielenia informacji, jeżeli spowodowałoby to:

- Ujawnienie wiadomości zawierających informacje niejawne,
- Zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- Zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
- Istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

7. Przekazywanie danych do państwa trzeciego.

Przekazanie danych osobowych do państwa trzeciego (poza Europejski Obszar Gospodarczy) może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych, za wyjątkiem sytuacji wynikających z obowiązku nałożonego na ADO przepisami

prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych. ADO może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

- Osoba, której dane dotyczą, udzieliła na to zgody na piśmie.
- Przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie.
- Przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem.
- Przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych.
- Przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
- Dane są ogólnie dostępne.

W pozostałych przypadkach przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody GIODO, wydanej w drodze decyzji administracyjnej, pod warunkiem, że ADO zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

8. Dokumentowanie.

MOPR w Opolu stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną. Zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Ponadto:

- Prowadzona jest dokumentacja opisująca sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych,
- Prowadzona jest kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
- Prowadzona jest ewidencja osób upoważnionych do ich przetwarzania, zawierająca: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
- Wyznaczony jest ABI, nadzorujący przestrzeganie zasad ochrony danych osobowych.

9. Sankcje karne.

- Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo, do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn ten dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca

działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

- Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Kto inspektorowi GIODO udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
- Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako naruszenie obowiązków pracowniczych.
- Orzeczona kara dyscyplinarna nie wyklucza odpowiedzialności karnej osoby winnej zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

VI. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO. Upoważnienia nadawane są indywidualnie, odrębnie do każdego zbioru danych osobowych, przed rozpoczęciem przez pracownika przetwarzania danych osobowych w danym zbiorze.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy w tym także stażyści, wolontariusze, praktykanci, a także inne osoby, współpracujące z MOPR, które uzyskują dostęp do danych osobowych w związku ze świadczeniem na rzecz MOPR usług na podstawie umów cywilnoprawnych.
3. Procedura zarządzania upoważnieniami do przetwarzania danych osobowych w zbiorach danych osobowych dla osób niebędących pracownikami MOPR, wskazana jest w przedmiotowych umowach o powierzeniu przetwarzania danych osobowych.
4. Upoważnienia do przetwarzania danych osobowych nadawane są przez ADO.
5. Osoby Zarządzające Zbiorami Danych występują do ADO, za pośrednictwem ABI, o nadanie uprawnień do przetwarzania danych osobowych dla wszystkich podległych pracowników komórki organizacyjnej, zgodnie z załącznikiem nr 3.
6. Przed nadaniem upoważnienia, w razie wątpliwości, co do zakresu upoważnienia, Osoby Zarządzające Zbiorem Danych, konsultują się z ABI, który podejmuje decyzję o akceptacji bądź odmowie akceptacji przyznania upoważnienia do przetwarzania danych osobowych dla

pracownika. W sytuacjach niebudzących zastrzeżeń Osoby Zarządzające Zbiorem Danych wnioskują o nadanie upoważnienia.

7. Osoby Zarządzające Zbiorem Danych ponoszą odpowiedzialność za przyznanie (utrzymywanie) zbyt szerokich uprawnień, w stosunku do realizowanych przez pracownika zadań, zwłaszcza, jeżeli w związku z tym doszło do naruszenia bezpieczeństwa przetwarzania danych osobowych.
8. Przed nadaniem upoważnienia pracownik, któremu ma być ono nadane jest informowany o przepisach z zakresu przetwarzania i ochrony danych osobowych. Osobą odpowiedzialną za zapoznanie pracowników MOPR z przepisami o ochronie danych osobowych jest ABI.
9. Po odbyciu szkolenia wprowadzającego, osobom biorącym udział w procesach przetwarzania danych osobowych, nadawane jest upoważnienie do przetwarzania danych osobowych, wydawane jest ono w dwóch egzemplarzach. Jednocześnie osoba, której nadawane jest upoważnienie do przetwarzania danych osobowych zostaje zobowiązana do stosowania obowiązujących w MOPR zasad ochrony danych osobowych, poprzez złożenie własnoręcznego podpisu na oświadczeniu znajomości zasad bezpieczeństwa przetwarzania danych.
10. Jeden egzemplarz upoważnienia jest przechowywany, jako część dokumentacji MOPR, drugi jest wydawany pracownikowi, któremu nadano upoważnienie. Przechowywaniem dokumentacji MOPR zajmuje się ABI.
11. Zarządzający Zbiorami Danych osobowych pozostaje w stałym kontakcie z ABI i jest na bieżąco informowany o: zmianach procedur związanych z ochroną danych osobowych w MOPR oraz zmianach przepisów prawnych związanych z ochroną danych osobowych.
12. Pracownicy, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych przechodzą szkolenie informacyjne. W ramach szkolenia są oni zapoznawani z podstawowymi pojęciami z zakresu ochrony danych osobowych (dane osobowe, przetwarzanie danych osobowych, dane wrażliwe, zbiór danych osobowych), odpowiedzialnością prawną ciążącą na osobach przetwarzających dane osobowe, procedurami działania w przypadku wykrycia nieuprawnionego dostępu do danych osobowych, procedurami kontaktu z ABI, ADO, Informatykiem oraz sposobem postępowa.
13. Wydanie każdego upoważnienia jest odnotowywane przez ABI w prowadzonej przez niego ewidencji upoważnień.
14. Zakres nadanych pracownikowi uprawnień może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym czasie. W takim przypadku tryb wskazany do nadawania uprawnień określony w niniejszym Rozdziale jest właściwy również w razie aktualizacji zakresu przyznanych uprawnień dla pracownika w związku z jego dostępem do określonego zbioru danych osobowych.
15. Obligatoryjna utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:
    - Zmiany stanowiska pracy w MOPR, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,
    - Umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie,
    - Rozwiązania stosunku pracy.

16. W przypadkach określonych w punkcie powyżej, Osoby Zarządzające Zbiorem Danych Osobowych, zobowiązane są niezwłocznie do powiadomienia ADO o konieczności dokonania zmian w prowadzonej ewidencji osób dopuszczonych do przetwarzania danych. Powiadomienie dokonywane jest zgodnie z załącznikiem nr 3.
17. W przypadku zaistnienia nadzwyczajnych okoliczności, wpływających na konieczność poszerzenia wiedzy pracowników MOPR przetwarzających dane osobowe, ADO przeprowadza szkolenie uzupełniające.
18. Uszczegółowienie trybu nadania, zmiany, utraty uprawnień logicznego dostępu do danych osobowych przetwarzanych w systemach informatycznych zawarte jest w rozdziale IX.

VII. KONTROLA PRZETWARZANIA I STAN ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w strukturze Administratora Danych Osobowych sprawuje ABI.
2. Czynności kontrolne przeprowadzane są w ciągu całego roku. Kontrolą, o której mowa w ust. 1, mogą zostać objęte zarówno komórki organizacyjne MOPR, w których przetwarzane są w zbiorach dane osobowe, jak i pojedyncze stanowiska pracy wyodrębnione w strukturze Administratora Danych w celu ustalenia, czy w ich obszarze funkcjonowania nie znajdują się dane osobowe, które powinny zostać poddane zasadom ochrony przewidzianym w Ustawie, Rozporządzeniu oraz dokumentacji przetwarzania danych.
3. Z czynności sprawdzających sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i czynności przeprowadzonych w jej trakcie. We wnioskach protokołu dokonuje się całościowej oceny stanu ochrony danych przetwarzanych w kontrolowanej komórce organizacyjnej Administratora Danych oraz wskazuje występujące w tym zakresie uchybienia wraz ze sposobami i terminem ich usunięcia.
4. Sporządzany protokół jest podpisywany przez ABI oraz obowiązkowo przez kierownika lub pracownika kontrolowanej komórki organizacyjnej lub stanowiska. Jeden egzemplarz protokołu otrzymuje kierownik lub pracownik kontrolowanej komórki organizacyjnej. Drugi po zapoznaniu przez ADO, przechowywany jest przez ABI.
5. ABI przysługuje prawo do wykonania czynności sprawdzających w zakresie weryfikacji usunięcia przez komórkę uchybień i wykonania innych zaleceń wskazanych w protokole z przeprowadzonej kontroli. Z czynności tych spisywany jest protokół. W przypadku nie wykonania zaleceń pokontrolnych ABI informuje pisemnie o tym fakcie ADO wnioskując o podjęcie działań dyscyplinujących.
6. ABI ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.

VIII. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE POUFNOŚĆ, INTEGRALNOŚĆ I ROZLICZALNOŚĆ PRZETWARZANYCH DANYCH OSOBOWYCH.

1. Środki organizacyjne.

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się określone poniżej rozwiązania w tym zakresie stosowane w MOPR w Opolu.

- Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez ADO. Podpisany dokument jest przetrzymywany w prowadzonym rejestrze upoważnień.
- Przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania powierzonych zadań. Zakres uprawnień do przetwarzania danych wynika z zakresu tych zadań.
- Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
- Wyznaczono Administratora Bezpieczeństwa Informacji (ABI).
- Opracowano i wdrożono Politykę Bezpieczeństwa, o której mowa w ustawie o ochronnie danych osobowych.
- Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej dokumentacji.
- Osoby, które przetwarzają dane osobowe zostały zapoznane z przepisami z zakresu ochrony danych osobowych. Nowo przyjęty pracownik, przed przystąpieniem do przetwarzania danych, jest zapoznawany z przepisami przez ABI.
- Podmioty realizujące zadania na zlecenia MOPR, które przetwarzają dane osobowe, zostały poinformowane o sposobach zabezpieczenia danych osobowych. Z podmiotami tymi została podpisana umowa o powierzeniu przetwarzania danych osobowych.
- Ponadto każdy pracownik, upoważniony do przetwarzania danych osobowych, potwierdza pisemnie fakt zapoznania się Polityką bezpieczeństwa i zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument jest przechowywany przez ABI.
- Osoby zatrudnione przy przetwarzaniu danych osobowych w systemie elektronicznym zostały zapoznane w zakresie zabezpieczeń systemu informatycznego.
- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Przebywanie osób, nieuprawnionych w ww. obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
- Przebywanie w pomieszczeniach, w których przetwarzane są dane w postaci elektronicznej osób nieposiadających upoważnienia jest dopuszczalne za zgodą Administratora danych.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

- Nie należy dopuszczać osób niemających uprawnień do danych osobowych do treści tych danych, np. pokazywanie dokumentów.
- Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach, zgodnie z prowadzoną ewidencją. Jeżeli posiadane druki lub zestawienia są niezbędne należy je zanonimizować (usunąć dane osobowe, np. adres, pesel, pozostawiając imiona).
- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.
- Każdorazowe zbieranie danych o osobach, bez względu na źródło tych danych, rodzi na ADO obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszar przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- W celu zapewnienia ochrony danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego oraz bezpośrednio do programów przetwarzających dane.
- Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie opisane zostały w rozdziale IX niniejszej dokumentacji.

2. Środki techniczne – ochrona fizyczna.

W poniższej tabeli zestawiono sumarycznie dla wszystkich pomieszczeń zastosowane środki ochrony fizycznej. Szczegółowe fizyczne zabezpieczenia zbiorów w poszczególnych pomieszczeniach znajdują się w załączniku nr 2.

L.p.	Środki ochrony fizycznej
1.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi)
2.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
3.	Pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
	Pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system zabezpieczeń, uniemożliwiający dostęp osobom nieupoważnionym.
4.	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
5.	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
6.	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę jest nadzorowany przez służbę ochrony.
	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych objęty jest systemem kontroli dostępu.
7.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.
8.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.
	Zbiór danych osobowych w formie papierowej przechowywany jest w szafie zamykanej na klucz.
9.	Kopie zapasowe/archiwalne zbioru danych przechowywane są w zamkniętej niemetalowej szafie.

	Kopie zapasowe/archiwalne zbioru danych przechowywane są w zamkniętym pomieszczeniu zabezpieczonym systemem alarmowym.
10	Kopie zapasowe/archiwalne zbioru danych przechowywane są w zamykanym na klucz pokoju.
11.	Pomieszczenie, w których przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
12.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

3. Środki techniczne – infrastruktura informatyczna, programy i bazy danych

W poniższej tabeli zestawiono, sumaryczne dla wszystkich komputerów i baz danych, stosowane środki ochrony infrastruktury informatycznej, telekomunikacyjnej, narzędzi programowych i baz danych.

L.p.	Ochrona infrastruktury, narzędzi programowych i baz danych
1.	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych
2.	Zastosowano środki uniemożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3.	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4.	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5.	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
6.	Zastosowano kryptograficzne środki ochrony danych osobowych.
7.	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8.	Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

IX. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Na podstawie § 3 ust. 1 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 opracowano Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1. Charakterystyka systemu.

1) Sieć informatyczną, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecne i przyszłe serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2) Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3) System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

1. Ogólne zasady pracy w systemie informatycznym.

1) ABI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2) Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez Informatyka do eksploatacji licencjonowane oprogramowanie.
3) Informatyk prowadzi ewidencję oprogramowania.
4) Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   - Mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
   - Mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   - Mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   - Urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   - Mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
   - Mechanizmy zarządzania zmianami.
5) Użytkownikom zabrania się:
   - Korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody ADO,
   - Udostępniania stanowisk roboczych osobom nieuprawnionym,
   - Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez ADO,
   - Samowolnego instalowania i używania programów komputerowych,
   - Korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   - Umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym,
   - Używania komputera bez zainstalowanego oprogramowania antywirusowego.

2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności opisana została w załączniku nr 3.

3. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła, jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2) Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać osobne hasła i login do systemu operacyjnego oraz aplikacji.
3) Hasło składa się, z co najmniej ośmiu znaków, zawiera, co najmniej jedną wielką literę, co najmniej jedną cyfrę lub/i co najmniej jeden znak specjalny.

4) W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
5) Zmianę hasła należy dokonywać nie rzadziej, niż co 30 dni.
6) Hasła użytkowników generuje Informatyk i przekazuje wraz z loginem użytkownikowi.
7) Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do zmiany hasła dostępu.
8) Hasło nie może być zapisywane i przechowywane.
9) Użytkownik nie może udostępniać loginu i hasła.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1) Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.
2) Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem lub wyłączenia monitora.
3) Zakończenie pracy w systemie następuje poprzez prawidłowe wylogowanie się z aplikacji oraz systemu operacyjnego i pozostawienie komputera włączonego, celem wykonania kopii zapasowej
4) Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.
5) Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.
6) Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, określa Regulamin Pracy.
7) Konieczność pracy w aplikacjach sieciowych w godzinach innych, niż określone w Regulaminie Pracy, powinna być zgłoszona Informatykowi.
8) Informatyk monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1) Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2) Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
3) Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfiguracyjnych systemu odpowiedzialny jest Informatyk. Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.

4) Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
5) Kopie baz danych gromadzonych na serwerach wykonywane są przez Informatyka w dniach roboczych po zakończeniu pracy przez użytkowników i zapisywane na dysku sieciowym. Kopia z ostatniego dnia miesiąca zapisywana jest dodatkowo na nośniku optycznym i przechowywana w zamkniętym pokoju i zamkniętej szafie przez 5 lat.
6) Kopie zbiorów danych osobowych zlokalizowanych na komputerach lokalnych wykonywane są w dniach roboczych po zakończeniu pracy przez użytkownika. Kopie zapisywane są na dyskach sieciowych i przechowywane przez 5 dni.
7) Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.
8) Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, których obowiązkiem jest pozostawienie komputera w stanie umożliwiającym wykonanie automatycznej kopii bezpieczeństwa.
9) Informatyk zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
10) Zewnętrzne nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.
11) Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.
12) Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych.

1) Nośniki danych oraz programy służące do przetwarzania danych osobowych, a także dane konfiguracyjne systemu informatycznego, przechowuje Informatyk w odpowiednio zabezpieczonym pomieszczeniu.
2) Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z Informatykiem.
3) Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.
4) Mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

7. Sposób zabezpieczenia systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.

Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1) Informatyk zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.

2) System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.
3) System antywirusowy musi mieć aktywną funkcję automatycznej aktualizacji wzorców wirusów.
4) W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie Informatyka.
5) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Informatyk podejmuje działania zmierzające do usunięcia zagrożenia.
6) Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać. Zewnętrze elektroniczne nośniki informacji muszą być dopuszczone do użycia przez Informatyka.

8. Informacje o odbiorcach danych.

Informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

1) Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące informacje:
   - Dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się, jako dane jawne,
   - Sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celu przekazania jej danych innemu administratorowi.
2) Zapis pkt 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji tekstu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.
3) Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1.
4) W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w pkt 1, prowadzi się odrębny „rejestr udostępniania", w oparciu o własne rozwiązania organizacyjne.
5) Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.

9. Przysyłanie danych poza obszar przetwarzania.

1) Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2) W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptograficzną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (tel., faks, bezpośrednia rozmowa).
3) Zabrania się przekazywania danych przez aplikacje internetowe niewykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https").

10. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   - Likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   - Przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   - Naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem Informatyka.
2) Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonuje Informatyk lub pracownicy firm przez niego wskazanych.
3) Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO lub posiadające umowy na powierzenie przetwarzania danych w zakresie konserwacji i napraw.
4) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez Informatyka.
5) Informatyk wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

11. Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi.

1) System Kadry-Płace. Dotyczy danych wprowadzanych w systemie Kadry, automatycznie przenoszonych do systemu Płace.

Pola: identyfikator pracownika, imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu/mieszkania, pesel, konto bankowe, nazwa banku, informacje o nieobecnościach w pracy, dział, wydział, oddział, komórka, stanowisko, ilość dzieci, kalendarze pracy, identyfikator kodu tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia, data wyrejestrowania z ubezpieczenia, kod tytułu ubezpieczenia(dla wyrejestrowania).

2) System Kadry - Program Płatnik. Dotyczy danych wprowadzanych w systemie Kadry, które automatycznie przenoszone są do systemu Płace, a następnie przenoszone są do systemu Płatnik.

Pola: identyfikator pracownika, imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu/mieszkania, pesel, identyfikator kodu tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia, data wyrejestrowania z ubezpieczenia, kod tytułu ubezpieczenia(dla wyrejestrowania).

3) System Płace – Program Płatnik. Dotyczy to danych wprowadzonych w systemie Płace, a następnie przenoszone są do systemu Płatnik.

Pola: identyfikator pracownika, imię, nazwisko, składki ubezpieczeniowe, kod tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia.

4) System Pomost Std – Program Millenet. Dotyczy danych z systemu „Pomost Std" firmy Sygnity, przenoszonych do systemu Millenet za pomocą importu oraz przekazywanych do banku transmisją elektroniczną.

Pola: Identyfikator klienta lub instytucji, imię, nazwisko, nawa banku, nr konta, kwota wypłaty.

5) System Kadry Płace – Program Millenet. Dane dotyczące systemu „Kadry – Płace" firmy UNIT4TETA, przenoszonych do systemu MIllenet za pomocą importu oraz przekazywanych dom banku transmisją elektroniczną.

Pola: Imię, nazwisko, nazwa banku, numer rachunku osobistego, kwota wypłaty.

12. Systemy informatyczne stosowane w MOPR, w których przetwarzane są zbiory danych osobowych.

1) System informatyczny „Pomost Std" firmy Sygnity Kraków.
   - Moduł obsługa klienta;
   - Moduł rodziny zastępcze;
   - Moduł piecza zastępcza;
2) System informatyczny „Kadry – Płace" firmy UNIT4TETA Wrocław.
   - Moduł kadry;
   - Moduł płace;
   - Moduł fundusz bezosobowy;
   - Moduł komunikacja z bankami;
   - Moduł archiwum;
3) System informatyczny „Płatnik" firmy Asecco Warszawa.
4) Program „Finanse" firmy Progman.
5) Program „Wyposażenie" firmy Progman.
6) Program „Kasa" firmy Progman.
7) Program „Stołówka" firmy Progman.
8) Program „PFRON".

X. ZAŁĄCZNIKI

Załącznik nr 1 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.

Załącznik nr 3 – Procedura nadawania uprawnień do przetwarzania danych osobowych w MOPR w Opolu.