POLITYKA BEZPIECZEŃSTWA

w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Miastku

Rozdział I

(Postanowienia ogólne, definicje)

§ 1

Postanowienia ogólne

1. Polityka bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych administrowanych przez Miejsko-Gminny Ośrodek Pomocy Społecznej w Miastku.
2. Podstawą do opracowania i wdrożenia dokumentu są:
   a) Rozporządzenie 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych [dalej: RODO];
   b) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000) [dalej: Ustawa].
3. Polityka bezpieczeństwa ma zastosowanie do ochrony danych osobowych przetwarzanych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Miastku, w celu ich bezpiecznego wykorzystania, oraz określa zasady korzystania z systemów informatycznych.
4. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) Poufność danych – rozumianą jako właściwość, że dane nie są udostępniane osobom nieupoważnionym.
   b) Integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
   c) Rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
   d) Integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 2

Definicje

Określenia i skróty użyte w Polityce bezpieczeństwa oznaczają:

1. Podmiot – Miejsko-Gminny Ośrodek Pomocy Społecznej w Miastku;
2. Administrator Danych Osobowych – Miejsko-Gminny Ośrodek Pomocy Społecznej w Miastku, zwany dalej „ADO"; decydujący o celach i środkach przetwarzania danych, reprezentowany przez Kierownik Magdalenę Stankowiak;
3. Inspektor Ochrony Danych – osobę powołaną przez ADO, odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Miastku, zwaną dalej „IOD";
4. Administrator Systemów Informatycznych – osobę wyznaczoną przez ADO, zwaną dalej „ASI";
5. System informatyczny – zespół środków technicznych (urządzenia komputerowe, drukujące, łączności, oprogramowanie), zespół zabezpieczeń środków technicznych, sieć informatyczna i udostępniane przez nią zasoby, narzędzia zastosowane w celu przetwarzania danych;
6. Bezpieczeństwo systemu informatycznego – wdrożenie środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów RODO oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem danych;
7. Zbiór danych osobowych – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji;
8. Przetwarzanie danych osobowych – wykonywanie operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie, niezależnie od formy, w jakiej wykonywane są te czynności;
9. Osoba upoważniona lub użytkownik systemu – osobę posiadającą upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem";
10. 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;
11. Dane osobowe (dane) – wszelkie dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Rozdział II

(Obszary przetwarzania danych osobowych)

§ 3

Obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Podmiocie obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Obszar przetwarzania danych osobowych określony jest w „**Wykazie pomieszczeń, w których przetwarzane są dane osobowe**", stanowiącym załącznik nr 1 do Polityki bezpieczeństwa. Wykaz ten prowadzony jest przez ADO i zawiera następujące informacje:
    a) lokalizację budynku,
    b) numer pomieszczenia i jego przeznaczenie,
    c) wskazanie piętra budynku,
    d) określenie pracownika/działu w Podmiocie użytkującego dane pomieszczenie,
    e) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
    f) określenie zabezpieczenia pomieszczenia.
3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki bezpieczeństwa „**Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe**".

§ 4

Sposób przepływu danych pomiędzy poszczególnymi systemami

1. W ramach procesów przetwarzania danych dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „**Wykazie systemów przetwarzania danych osobowych**", będącym załącznikiem nr 3 do Polityki bezpieczeństwa.

§ 5

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Miastku.

Rozdział III

(Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem)

§ 6

Zadania administratora danych osobowych

1. Zadania administratora danych osobowych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Miastku w rozumieniu RODO wykonuje Kierownik Magdalena Stankowiak.
2. Przetwarzanie danych przez ADO następuje zgodnie z zasadami wskazanymi w art. 5 RODO.
3. ADO powołuje IOD.
4. ADO powołuje zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
5. ADO powołuje ASI.

§ 7

Zadania IOD

1. Do zakresu obowiązków IOD należy w szczególności:
    a) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
        - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych osobowych,
        - nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych i środki zapewniające ochronę przetwarzanych danych osobowych oraz przestrzegania zasad w niej określonych,
        - zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

§ 8

Uprawnienia IOD

W celu realizacji powierzonych zadań IOD w Podmiocie, ma on prawo:

a) kontrolować komórki organizacyjne Podmiotu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
b) wydawać polecenia kierownikom komórek organizacyjnych Podmiotu w zakresie bezpieczeństwa danych osobowych;
c) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
d) żądać od wszystkich pracowników Podmiotu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych;

e) wstępu do pomieszczeń, w których przetwarzane są dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych, w celu oceny zgodności przetwarzania z prawem.

§ 9

Zadania właścicieli zasobów danych osobowych

1. ADO wyznacza właścicieli zasobów danych osobowych.
2. Rolę właścicieli zasobów danych osobowych odgrywają kierownicy działów odpowiedzialni za dany zasób danych osobowych.
3. Do obowiązków właścicieli zasobów danych osobowych należy w szczególności:
   a) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez kierowane działy;
   b) występowanie z wnioskiem do ADO o nadanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom;
   c) zgłaszanie do IOD zamiaru wprowadzenia zmian w zakresie i sposobach przetwarzania danych w kierowanym dziale;
   d) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
   e) przestrzeganie obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń;
   f) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w kierowanym dziale, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych i przekazywanie IOD aktualnej ewidencji tych osób;
   g) sprawowanie w kierowanym dziale nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny;
   h) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 10

Obowiązki ASI

1. ASI odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Podmiocie.
2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:
   a) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Podmiocie;
   b) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;

c) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;

d) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Podmiocie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;

e) nadzór nad przesyłaniem danych osobowych drogą teletransmisji;

f) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;

g) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

h) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;

i) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

j) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

Rozdział IV

(Gromadzenie danych osobowych)

§ 11

Uzyskiwanie danych osobowych

Dane osobowe przetwarzane w Podmiocie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 12

Wykorzystanie danych osobowych

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 13

Obowiązek uzupełniania danych osobowych

W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem RODO albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział V

(Obowiązek informacyjny)

§ 14

Odpowiedzialność osób na stanowiskach kierowniczych

1. Kierownicy komórek organizacyjnych Podmiotu, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:
    a) adresie siedziby Podmiotu, pod którym dane są zbierane i przetwarzane oraz danych kontaktowych;
    b) gdy ma to zastosowanie – danych kontaktowych Inspektora Ochrony Danych
    c) celu zbierania danych;
    d) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
    e) odbiorcach danych, jeżeli istnieją
    f) jeśli ma to zastosowanie – zamiarze przekazania danych osobowych do państwa trzeciego
    g) prawach osoby, której dane dotyczą (art. 12 – 23 RODO);
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 14 RODO.
3. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i 2, stanowi załącznik nr 4 do Polityki bezpieczeństwa.

§ 15

Zgoda na przetwarzanie danych osobowych

1. Kandydaci do pracy w Podmiocie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
2. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.
3. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 2, stanowi załącznik 5 do Polityki bezpieczeństwa.

Rozdział VI

(Udostępnianie danych osobowych)

§ 16

Osoby uprawnione do wglądu do danych osobowych

1. ADO udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
    a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
    b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
    c) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 6 do Polityki bezpieczeństwa.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu ADO i informuje o tym IOD.
7. ADO podejmuje decyzję o udostępnieniu i przekazuje ją do właściciela zasobów danych osobowych.
8. Właściciel zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 17

Odmowa udostępnienia danych osobowych

Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

Rozdział VII

(Ochrona przetwarzania danych osobowych)

§ 18

Obowiązek posiadania upoważnienia

1. Do przetwarzania danych mogą być dopuszczeni pracownicy Podmiotu posiadający upoważnienie nadane przez ADO. Wzór upoważnienia określa załącznik nr 7 do Polityki bezpieczeństwa.
2. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 8 do Polityki bezpieczeństwa.

§ 19

Przechowywanie imiennych upoważnień do przetwarzania danych osobowych

1. ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:
   a) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych; wzór formularza oświadczenia stanowi załącznik nr 10 do Polityki bezpieczeństwa;
   b) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi załącznik nr 10 do Polityki bezpieczeństwa;
   c) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej; wzór formularza porozumienia stanowi załącznik nr 9 do Polityki bezpieczeństwa.

§ 20

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 i 29 RODO, na podstawie umowy zawartej na piśmie pomiędzy ADO, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2. Właściciel zasobów danych osobowych informuje IOD o zamiarze powierzenia danych osobowych do przetwarzania.
3. IOD przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
4. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
5. Każda osoba delegowana do wykonywania zadań na rzecz Podmiotu, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie

o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

6. Projekt umowy parafują:
   a) właściciel zasobów danych osobowych,
   b) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym.
7. Zaparafowany projekt umowy jest przedkładany przez IOD do akceptacji i podpisu ADO. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 11 do Polityki bezpieczeństwa.

§ 21

Obowiązki podmiotu przetwarzającego dane osobowe

1. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających dane przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
2. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
3. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.

Rozdział VIII

(Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

§ 22

Zabezpieczenia organizacyjne

1. Został wyznaczony IOD nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. Została opracowana i wdrożona Polityka Bezpieczeństwa.
3. Została opracowana i wdrożona Instrukcja Zarządzania Systemem Informatycznym.
4. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez ADO.
5. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
6. Osoby zatrudnione przy przetwarzaniu danych, w tym danych szczególnych kategorii zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego, oraz przeszkolone.
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

8. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
10. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

§ 23

Zabezpieczenia ochrony fizycznej danych osobowych

Zasady ochrony fizycznej opisane są w załączniku nr 2 do Polityki bezpieczeństwa „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe."

§ 24

Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji Zarządzania Systemem Informatycznym.

§ 25

Zabezpieczenia narzędzi programowych i baz danych

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

Rozdział IX

(Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych. Instrukcja alarmowa)

§ 26

Określenie sytuacji naruszenia bezpieczeństwa danych osobowych

Przepisy niniejszego rozdziału stosuje się w przypadku:

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

§ 27

Określenie osób zobowiązanych

Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 28

Określenie naruszenia zabezpieczenia systemu informatycznego

Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

a) nieautoryzowany dostęp do danych;
b) nieautoryzowane modyfikacje lub zniszczenie danych;
c) udostępnienie danych nieautoryzowanym podmiotom;
d) nielegalne ujawnienie danych;
e) pozyskiwanie danych z nielegalnych źródeł.

§ 29

Działania pracowników

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub IOD (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.
2. Katalog przykładowych incydentów i form naruszeń oraz sposobów postępowania przy ich wystąpieniu prezentuje załącznik nr 12 do Polityki bezpieczeństwa.
3. W przypadku kiedy IOD stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
    a) źródło powstania incydentu lub zagrożenia
    b) zakres działań korygujących lub naprawczych
    c) termin realizacji
    d) osobę odpowiedzialną
4. IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wykonywanych działań. Po ich zakończeniu dokonuje oceny efektywności. Powyższe czynności IOD zamieszcza w rejestrze incydentów stanowiącym załącznik nr 13 do Polityki bezpieczeństwa.

§ 30

Działania IOD

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

§ 31

Podporządkowanie się poleceniom IOD

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

§ 32

Raport końcowy

IOD po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi załącznik nr 14 do Polityki bezpieczeństwa.

Rozdział X

(Odpowiedzialność służbowa i karna)

§ 33

Odpowiedzialność służbowa

1. Pracownik, który:
    a) przetwarza dane osobowe:
        - do których przetwarzania nie jest upoważniony,
        - których przetwarzanie jest zabronione,
        - niezgodne z celem;
    b) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
    c) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
    d) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw

– podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjom określonym w Kodeksie pracy.

2. Naruszenie zasad ochrony danych osobowych obowiązujących w Podmiocie może również zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną określoną w przepisach odrębnych.

§ 34

Przepisy karne

Naruszenie przepisów o ochronie danych osobowych stanowi podstawę do dochodzenia roszczeń cywilno – prawnych przez osoby, której dane osobowe przetwarzane są niezgodnie z przepisami RODO ustawy, jak również może stanowić nałożenie pieniężnych kar administracyjnych na ADO, a nawet odpowiedzialność karną zgodnie z art. 107 lub 108 ustawy.

Art. 107. [Nielegalne przetwarzanie danych osobowych]
1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 108. [Udaremnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych]
Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

KIEROWNIK
MIEJSKO-GMINNEGO
OŚRODKA POMOCY SPOŁECZNEJ
W MIASTKU
Magdalena Stankowiak