Załącznik do Zarządzenia nr 24/15
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Toruniu
z dnia 31 grudnia 2015 r. w sprawie zmiany
Polityki Bezpieczeństwa Danych Osobowych
w MOPR w Toruniu

Cele, strategia i polityka zabezpieczania systemów informatycznych, w których są przetwarzane dane osobowe w Miejskim Ośrodku Pomocy Rodzinie w Toruniu

1. Cel i przeznaczenie dokumentu

Niniejszy dokument ma zapewnić właściwe zarządzanie zabezpieczeniami systemów informatycznych oraz prawidłową ochronę danych osobowych w nich przetwarzanych.

W dokumencie tym przedstawione zostaną:
1. cele, strategia i polityka zabezpieczeń systemów informatycznych;
2. zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych;
3. potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych;
4. zabezpieczenia adekwatne do zagrożeń i ryzyka;
5. sposoby kontroli przetwarzania danych osobowych.

Dokument przeznaczony jest dla użytkowników systemów informatycznych przetwarzających dane podlegające pod ustawę o ochronie danych osobowych.

2. Cele i polityka zabezpieczania systemów informatycznych, w których przetwarzane są dane osobowe

Celem zabezpieczania systemów informatycznych przetwarzających dane osobowe jest realizacja art.47 i art.51 Konstytucji Rzeczypospolitej Polskiej oraz Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tj. Dz.U. z 2015 r. poz.2135).

W świetle ww. ustawy przetwarzane dane osobowe winny być chronione przed:
1. ich udostępnianiem podmiotom nieupoważnionym;
2. zbieraniem przez podmioty nieuprawnione;
3. upowszechnianiem;
4. nielegalnym pozyskiwaniem;
5. uszkodzeniem, zniszczeniem lub nieuprawnioną modyfikacją danych.

W celu realizacji ochrony danych osobowych należy zabezpieczyć systemy informatyczne przetwarzające te dane. Zabezpieczenie takie winno być realizowane na różnych płaszczyznach, w szczególności zaś:
1. infrastruktury technicznej (sprzętowej i oprogramowania);
2. użytkowania systemów informatycznych;
3. pozyskiwania i likwidacji informacji;

4. wykrywania i właściwego reagowania na przypadki naruszenia bezpieczeństwa danych osobowych.

5. Za bezpieczeństwo danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu odpowiedzialny jest Dyrektor Ośrodka jako administrator danych. Politykę ochrony danych osobowych realizuje przy pomocy wyznaczonego przez siebie administratora bezpieczeństwa informacji.

2.1. Zadania administratora bezpieczeństwa informacji

1.Celem działania Administratora Bezpieczeństwa Informacji – zwanym dalej ABI - jest zapewnienie przestrzegania przepisów o ochronie danych osobowych przetwarzanych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu.
2. Do zakresu zadań ABI należą zadania, o których mowa w art.36a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych oraz rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji a w szczególności:
a) sprawowanie zgodności danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Dyrektora, będącego Administratorem Danych Osobowych;
b) nadzorowanie i aktualizacja dokumentacji, o której mowa w art. 36 ust.2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych oraz przestrzegania zasad w niej określonych;
c) prowadzenie rejestru zbioru danych przetwarzanych przez pracowników, zgodnie z obowiązującymi przepisami prawa, a w szczególności rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych;
d) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych (pracowników i Zleceniobiorców);
e) nadzorowanie i kontrolowanie przestrzegania stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania , zmieniania, udostępniania i ich usuwania;
f)nadzorowanie i kontrolowanie przestrzegania zasad ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń;
g) przygotowywanie i składanie wniosków o zgłoszenie zbiorów do rejestru zbiorów danych osobowych ABI lub w Biurze Generalnego inspektora Ochrony Danych osobowych oraz aktualizacji ich zgłoszeń;
h) tworzenie projektów zarządzeń, instrukcji i wytycznych w zakresie ochrony danych osobowych;
i) wyjaśnienie i dokumentowanie przypadków naruszenia zasad przetwarzania i ochrony danych osobowych;
j) wykonywanie kopii awaryjnych baz danych;
k)bezzwłoczne podejmowanie działań w przypadku otrzymania informacji o nieprawidłowej pracy systemu przetwarzającego dane osobowe, naruszeniu zabezpieczeń systemu, wystąpieniu sytuacji wskazującej na możliwość naruszenia bezpieczeństwa danych.
l) występowanie do Dyrektora z wnioskiem o ukaranie osób, które naruszyły bezpieczeństwo danych osobowych.
4. Wykonując swoje czynności ABI posiada uprawnienia oraz upoważnienia do:

a) kontrolowania realizacji umów dotyczących udostępnienia lub powierzenia danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania zapisów bezpieczeństwa i ochrony danych osobowych;
b) decydowania o pozbawieniu lub ograniczeniu zakresu przetwarzania danych osobowych i uprawnień w systemach informatycznych dla użytkowników którzy powodują zagrożenie bezpieczeństwa i ochrony danych osobowych;
c) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych sprawdzeń (kontroli lub audytów) i dostosowania ochrony danych do stanu zgodnego z przepisami;
d) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących okoliczności powstania zagrożeń dla bezpieczeństwa i ochrony danych osobowych;
e) wydawania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji wydanych upoważnień;
f) organizowanie szkoleń dla pracowników Miejskiego Ośrodka Pomocy Rodzinie w Toruniu z zakresu przetwarzania i ochrony danych osobowych;
g) rozpatrywanie skarg i wniosków w zakresie przetwarzania i ochrony danych osobowych;
h) kontrolowania pracowników w zakresie zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzenie sprawdzenia (kontrole i audyty).

2.2. Polityka zabezpieczania danych osobowych

W celu właściwej realizacji zadań związanych z bezpieczeństwem danych osobowych należy wziąć pod uwagę następujące zagrożenia:
1. fizyczne – związane z zabezpieczeniem pomieszczeń;
2. wynikające ze zdarzeń losowych;
3. wynikające z nieprawidłowej pracy systemów informatycznych;
4. wynikające z dostępu do informacji osób nieuprawnionych;
5. wynikające z działania użytkowników.

Należy również uwzględnić możliwości organizacyjne, finansowe i techniczne w realizacji ochrony danych osobowych, w szczególności:
1. posiadane „zasoby ludzkie” – ilość oraz fachowość kadry;
2. stosunek nakładów finansowych do jakości i ważkości gromadzonej informacji;
3. stosunek nakładów finansowych do kosztów pozyskania informacji oraz do kosztów związanych z ewentualną utratą informacji;
4. uwarunkowania architektoniczne zezwalające na odpowiednią realizację ustawy o ochronie danych osobowych.

3. Identyfikacja i analiza zagrożeń

Zagrożenia dla bezpieczeństwa danych przetwarzanych w systemach informatycznych mają charakter:
1. fizycznych – kradzież i/lub zniszczenie sprzętu komputerowego, nośników lub wydruków zawierających dane osobowe; do tej grupy zagrożeń należy zaliczyć również te, które wynikają z niszczenia zabezpieczeń fizycznych pomieszczeń (np. włamania), jak i te wynikające z nieuprawnionego dostępu do systemu informatycznego (dot.to włamań do sieci komputerowych i systemów przesyłania informacji);

2. losowy – wyładowania elektryczne, pożar, zalanie wodą pomieszczeń, w których odbywa się przetwarzanie danych i/lub są przechowywane nośniki informacji oraz wydruki komputerowe, awarie zasilania, zakłócenia w sieci energetycznej;
3. wadliwej pracy systemów informatycznych – uszkodzenia i awarie sprzętu komputerowego, nieprawidłowa praca systemów operacyjnych i/lub oprogramowania użytkowego, wirusy komputerowe, awarie w sieciach komputerowych;
4. dostęp osób nieuprawnionych – brak nadzoru nad pomieszczeniami, podgląd informacji na ekranie, zła organizacja formatek ekranu (na jednym ekranie mogą być informacje dotyczące tylko jednej osoby), zły obieg dokumentów, brak nadzoru nad naprawami i konserwacją sprzętu i oprogramowania, włamania do systemów informatycznych (np. przez internet), nieprzestrzeganie zasad eksploatacji systemów komputerowych, niewłaściwy nadzór nad niszczeniem dokumentów lub kasowaniem informacji;
5. działania użytkowników – pomyłki w trakcie przetwarzania danych, kradzież i/lub nielegalne kopiowanie danych, wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem.

Podczas analizowania ryzyka związanego z niebezpieczeństwem utraty informacji, zagrożeniami dla bezpieczeństwa danych lub wejścia w ich posiadanie przez podmioty nieupoważnione należy wziąć pod uwagę następujące czynniki:
1. wartość sprzętu komputerowego;
2. wartość oprogramowania użytkowego - w szczególności jest to związane z „wirusami" komputerowymi niszczącymi oprogramowanie;
3. wartość zgromadzonej informacji – zarówno w aspekcie ważności dla celów w jakich jest gromadzona, jak i w aspekcie kosztów jej pozyskania lub ewentualnego odtworzenia;
4. koszty utraty informacji lub niewłaściwe jej wykorzystanie – wiązać to się może np. z kosztami ewentualnych procesów sądowych i odszkodowań;
5. fachowość i odpowiedzialność osób obsługujących systemy informatyczne.

Mając na uwadze powyższe należy podjąć odpowiednie kroki w celu wyeliminowania oraz minimalizacji zagrożeń dla bezpieczeństwa danych osobowych.

4. Potrzeby w zakresie zabezpieczenia danych osobowych i systemów informatycznych

W celu zapewnienia właściwego zabezpieczenia systemów informatycznych oraz ochrony danych osobowych istnieją następujące potrzeby:

1. W zakresie zagrożeń fizycznych:
   1) pomieszczenia, w których odbywa się przetwarzanie danych osobowych muszą być wyposażone w zamki patentowe uniemożliwiające dostęp osób nieuprawnionych i należy je zamykać na czas nieobecności osób zatrudnionych;
   2) nośniki danych z kopiami archiwalnymi musza być przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   3) wydruki komputerowe z danymi osobowymi muszą być przechowywane w szafach zamykanych na zamek uniemożliwiający dostęp do nich osób postronnych, w pomieszczeniach zamykanych na zamek patentowy;
   4) w przypadku instalowania komputerowych systemów sieciowych, okablowanie sieciowe należy układać w osłonach ochronnych tak, aby odcinek łączący komputery był jak najkrótszy;

5) sprzątanie pokoi musi odbywać się pod nadzorem osób uprawnionych do przetwarzania danych osobowych;

2. W zakresie zagrożeń wynikających ze zdarzeń losowych:
   1) budynki, w których odbywa się przetwarzanie danych osobowych muszą być wyposażone w instalację odgromową, która jest okresowo przeglądana i konserwowana;
   2) wszystkie urządzenia komputerowe muszą być podłączone do odrębnej sieci elektrycznej;
   3) muszą być opracowane instrukcje zawierające sposób postępowania ze sprzętem komputerowym służącym do przetwarzania danych osobowych, z instrukcjami tymi muszą się zapoznać osoby pracujące przy przetwarzaniu danych osobowych.
3. W zakresie zagrożeń wynikających z nieprawidłowej pracy systemów informatycznych:
   1) dane przetwarzane w systemach informatycznych powinny być archiwizowane w sposób określony w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu";
   2) przegląd i testowanie oprogramowania użytkowego i baz danych odbywać się powinien w sposób określony w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu";
   3) na użytkowanych komputerach musi być zainstalowane automatycznie się uruchamiające oprogramowanie antywirusowe;
   4) użytkownicy systemów komputerowych, na których odbywa się przetwarzanie danych osobowych są zobowiązani do sprawdzania programem antywirusowym używanych przenośnych nośników informacji (m.in.dyskietki, płyty CD oraz DVD, przenośne pendriv'y) przed ich użyciem;
   5) użytkownicy systemów są zobowiązani niezwłocznie informować administratora bezpieczeństwa informacji o wszelkich objawach niewłaściwej pracy systemu informatycznego.
4. W zakresie zagrożeń wynikających z dostępu do danych przez osoby nieupoważnione:
   1) do obsługi systemów informatycznych, w których odbywa się przetwarzanie danych osobowych mogą być dopuszczeni wyłącznie upoważnieni pracownicy i Zleceniobiorcy. W Miejskim Ośrodku Pomocy Rodzinie prowadzony jest i na bieżąco aktualizowany rejestr tych pracowników i Zleceniobiorców;
   2) we wszystkich systemach informatycznych, w których odbywa się przetwarzanie danych osobowych muszą być stosowane systemy autoryzacji dostępu;
   3) stosowana musi być okresowa zmiana haseł w sposób opisany w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu";
   4) wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji muszą być zniszczone w niszczarce;
   5) nośniki informacji zawierające dane osobowe, a przeznaczone do: likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych są pozbawiane zapisu w sposób uniemożliwiający jego odtworzenie;
   6) przekazywanie danych na zewnątrz Ośrodka odbywa się wyłącznie na zasadach określonych w Ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997r.
5. W zakresie zagrożeń wynikających z działań użytkowników:

1) wszyscy pracownicy i Zleceniobiorcy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do zachowania tajemnicy przetwarzanych danych osobowych, również po ustaniu zatrudnienia;
2) wszyscy pracownicy i Zleceniobiorcy zatrudnieni przy przetwarzaniu danych osobowych muszą zostać przeszkoleni w zakresie przepisów dotyczących ochrony danych osobowych;
3) dla poszczególnych pracowników i Zleceniobiorców zatrudnionych przy przetwarzaniu danych osobowych, o ile będzie to technicznie i organizacyjnie możliwe, musza zostać ustalone indywidualne prawa dostępu do danych osobowych;
4) indywidualne zakresy czynności pracowników zatrudnionych przy przetwarzaniu danych osobowych określają uprawnienia pracowników do przetwarzania danych osobowych;
5) zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowanie oprogramowania innego niż niezbędne do realizacji przetwarzania danych osobowych i/lub realizacji zadań służbowych;
6) zabronione jest wykonywanie kopii baz danych w celach innych niż archiwizacja i/lub przekazania danych podmiotowi uprawnionemu;
7) zabronione jest wykonywanie wydruków z baz danych w celach innych niż wynika to z zasad przetwarzania, archiwizacji i/lub przekazania danych podmiotowi uprawnionemu.