Załącznik do Zarządzenia Kierownika
Ośrodka Pomocy Społecznej Nr 14/2022
z dnia 28 grudnia 2022 r.

Instrukcja Zarządzania Systemem Informatycznym w Ośrodku Pomocy Społecznej w Starym Sączu

§ 1

1. Instrukcja Zarządzania Systemami Informatycznymi, zwana dalej „Instrukcją” jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury używania, zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych, wykorzystywanymi w Ośrodku Pomocy Społecznej w Starym Sączu, zwanym dalej „Ośrodkiem”.

2. W podmiocie o nazwie: Ośrodek Pomocy Społecznej w Starym Sączu, za przestrzeganie zapisów „instrukcji” odpowiedzialny są: Administrator Danych Osobowych, zwany dalej „ADO”, Inspektor Ochrony Danych, zwany dalej „IOD” oraz Administrator Systemów Informatycznych zwany dalej „ASI”.

3. Instrukcja obejmuje swoim zakresem wszystkie osoby zatrudnione w Ośrodku, które biorą udział w procesie przetwarzania danych osobowych w systemach informatycznych.
4. Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą ADO lub IOD.

5. Poziom bezpieczeństwa systemów informatycznych przetwarzających dane osobowe określono jako wysoki. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Na bezpieczeństwo procesu przetwarzania danych osobowych składają się: rozliczalność, poufność i integralność przetwarzanych danych.

6. Administrator Danych Osobowych monitoruje wdrożenie zabezpieczenia systemu informatycznego, stosując na poziomie wysokim środki bezpieczeństwa.

7. Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może skutkować odpowiedzialnością dyscyplinarną określonej przepisami Kodeksu Pracy. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami Kodeksu Karnego. Jeżeli skutkiem działania użytkownika jest szkoda materialna, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

§ 2

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych Osobowych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. **Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne.** Hasło w żaden sposób nie powinno kojarzyć się bezpośrednio z użytkownikiem. Hasło przy wpisywaniu nie może w sposób jawny wyświetlać się na ekranie.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

§ 3

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

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

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na miesiąc. Kopie muszą być tworzone na specjalnie przeznaczonym do tego celu nośnikach, które zostaną w należyty sposób zabezpieczone przed dostępem osób nieuprawnionych. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 4

Zabrania się osobom użytkującym komputer przenośny zawierający dane osobowe jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarza się dane osobowe.

§ 5

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.

§ 6

1. Administrator Danych Osobowych celem zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informatycznych powołuje Administratora Systemów Informatycznych.

2. Do głównych zadań Administratora Systemów Informatycznych zwanego dalej ASI należy:
a) Rejestracja uprawnionych użytkowników w danym systemie informatycznym,
b) Nadzorowanie pracy serwerów,
c) Kasowanie/dezaktywowanie kont użytkowników, którzy nie mogą już pracować w systemach informatycznych Ośrodka,
d) Monitorowanie funkcjonowania zabezpieczeń nadzór nad czynnościami związanymi z prowadzeniem systemu sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,
e) Konfiguracja komputerów w sposób zgodny z wymogami bezpieczeństwa informacji,
f) Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany,
g) podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszeń,
h) nadzór nad wykonywaniem i przechowywaniem kopii zapasowych,

i) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych.

§ 7

Rejestracji użytkowników w danym systemie dokonuje Administrator Systemów Informatycznych. Użytkownik po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami, loguje się na nie w celu sprawdzenia poprawności otrzymanych informacji i uprawnień.

§ 8

Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych lub rozwiązanie stosunku pracy lub umowy o innym charakterze obliguje ASI do odebrania temu użytkownikowi możliwości dostępu do danych osobowych przetwarzanych w systemach informatycznych.

§ 9

Podczas rozpoczęcia pracy w komputerze użytkownik jest autoryzowany poprzez podanie swojego hasła. Dopiero po pomyślnej autoryzacji w sieci komputerowej użytkownik może uzyskać możliwość uruchomienia programu służącego do przetwarzania danych osobowych, dokonując osobnej autoryzacji w tym programie.

§ 10

Przy każdorazowym opuszczeniu stanowiska komputerowego, użytkownik jest zobowiązany dopilnować, aby na ekranie nie były wyświetlane informacje lub dane osobom nieuprawnionym, poprzez:

a) zablokowanie komputera odpowiednią kombinacją klawiszy, lub
b) stosowanie wygaszacza ekranu zabezpieczonego hasłem, lub
c) wylogowanie się z sieci komputerowej.

§ 11

Podczas kończenia pracy na danej stacji roboczej należy:
a) wylogować się z systemu informatycznego,
b) wylogować się z sieci komputerowej, zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
c) sprawdzić czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

§ 12

W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie IOD lub ASI.

§ 13

W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Ośrodka, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach Ośrodka w oparciu o architekturę klient-serwer. Wynika stąd praktyka przetwarzania danych w bazach znajdujących się na dedykowanych dla poszczególnych programów serwerach. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Ośrodka, stanowią jedynie „końcówki" klienckie systemu.

§ 14

Wszelkie informacje (w tym dane osobowe), przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach systemów informatycznych, są zapisywane bezpośrednio na serwerach.

§ 15

Każdorazowo przed wykonaniem aktualizacji w systemach informatycznych i bazodanowych a także przed wykonywaniem prac konserwacyjnych systemów wykonywane są ich kopie zapasowe.

§ 16

W obszarze przetwarzania danych na komputerach stacjonarnych, laptopach, tabletach Ośrodka zabrania się stosowania własnych, będących własnością użytkowników pamięci przenośnych, dysków twardych, płyt CD-DVD i innych urządzeń, na których można zapisywać dane osobowe.

§ 17

Każdy zespół/sekcja w Ośrodku posiada własny, przypisany tylko temu zespołowi/sekcji adres poczty elektronicznej. Preferowaną formą przekazywania materiałów/ plików elektronicznych pomiędzy pracownikami Ośrodka jest poczta elektroniczna.

§ 18

Przekazywanie i niszczenie elektronicznych nośników informacji:
a) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez IOD,
b) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),
c) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,
d) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ADO lub IOD.

§ 19

Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.

§ 20

Użytkownik ma obowiązek niezwłocznie powiadomić IOD o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.

§ 21

W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia podejrzenia możliwości uszkodzenia informacji ASI w porozumieniu z IOD jest zobowiązany do:
a) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
b) sprawdzenia spójności i integralności informacji przetwarzanych w systemie informatycznym,
c) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej,
d) w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej.

§ 22

Instrukcja zarządzania systemem informatycznym stanowi uzupełnienie do Polityki Ochrony Danych w Ośrodku Pomocy Społecznej w Starym Sączu i jest dokumentem obowiązującym w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.

§ 23

Instrukcja zarządzania systemem informatycznym jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności podmiotu.

§ 24

Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Ośrodka ma obowiązek zapoznania się z niniejszą Instrukcją Zarządzania Systemem Informatycznym.

§ 25

Naruszenie zasad wynikających z Polityki Bezpieczeństwa Danych Osobowych oraz z Instrukcji zarządzania systemem informatycznym może stanowić:
a) Podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
b)Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem informatycznym nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.

Stary Sącz, grudzień 2023 r.

Franciszek Tudaj
Kierownik Ośrodka Pomocy Społecznej
w Starym Sączu