POLITYKA OCHRONY DANYCH OSOBOWYCH

W SYSTEMACH TELEINFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

W FUNDACJI RAZEM-CS

Spis treści

WSTĘP

Wdrożenie niniejszej „Polityki ochrony danych osobowych w systemach teleinformatycznych służących do przetwarzania danych osobowych w Fundacji RAZEM-CS" zwanej dalej Polityką, ma na celu zabezpieczenie danych osobowych przetwarzanych w systemach teleinformatycznych.

Polityka jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych w Fundacji RAZEM-CS oraz instrukcje zarządzania systemami teleinformatycznymi powinny być zgodne z niniejszym dokumentem.

ROZDZIAŁ I. POSTANOWIENIA OGÓLNE

1. Cel wydania dokumentu.
    1) Celem wydania dokumentu jest realizacja postanowień art.24 ust.1 i ust.2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 (Ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE L 119 z 04.05.2016 r. str. 47), zwanego dalej Rozporządzeniem;
    2) Opracowanie i wdrożenie niniejszego dokumentu ma na celu podniesienie standardów przetwarzania danych osobowych w systemach teleinformatycznych w Fundacji RAZEM-CS w Zamościu.
2. Streszczenie dokumentu:

    Niniejsza polityka określa:

    1) Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień oraz wskazania osoby odpowiedzialnej za te czynności;
    2) Stosowane metody i środki uwierzytelnienia w systemie orz procedury związane z ich urządzaniem i użytkowaniem;
    3) Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie przeznaczone dla użytkowników systemu;
    4) Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
    5) Sposób, miejsce i okres przechowywania:
        a) Elektronicznych nośników informacji zawierających dane osobowe,
        b) Kopii zapasowych;
    6) Sposób zabezpieczenia systemu teleinformatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu;
    7) Procedury wykonywania przeglądów i konserwacji systemów oraz elektronicznych nośników informacji służących do przetwarzania danych osobowych.
3. Zakres stosowania dokumentu:

1) Niniejszy dokument dotyczy danych osobowych przetwarzanych w systemach teleinformatycznych.
2) Wszyscy pracownicy Fundacji RAZEM-CS w Zamościu przetwarzający dane osobowe w systemach teleinformatycznych powinni stosownie do swoich obowiązków służbowych zapoznać się z Polityką i przestrzegać regulacji oraz zasad określonym w niniejszym dokumencie. Powyższemu obowiązkowi podlegają również stażyści, aplikanci, praktykanci przetwarzający dane osobowe w systemach teleinformatycznych.

4. Definicje pojęć:
   1) W niniejszej polityce stosuje się terminologię opisana w słowniku pojęć z zakresu ochrony danych osobowych stanowiącym załącznik nr 1 do Polityki Danych Osobowych w Fundacji RAZEM-CS w Zamościu.
5. Przeglądy Polityki Danych Osobowych w Fundacji RAZEM-CS w Zamościu. Wszelkie propozycje zmian Polityki należy zgłaszać Administratorowi Danych wyznaczonemu przez Zarząd lub Radę Fundacji RAZEM-CS. AD w porozumieniu z informatykiem raz na kwartał dokonuje przeglądu i aktualizacji Polityki (lub każdorazowo w przypadku konieczności dokonania istotnych zmian).

ROZDZIAŁ II. PROCEDURY NADAWANIA, MODYFIKACJI I REJESTROWANIA UPRAWNIEŃ W SYSTEMIE TELEINFORMATYCZNYM.

1. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych w celu zabezpieczenia przed nieuprawnionym dostępem do zasobów systemowych. Wspomniana kontrola realizowana jest m.in. poprzez zarządzenie uprawnieniami dostępu do systemu oraz wprowadzenie procedury rejestracji użytkownika w systemie – dotyczy systemów SL2014 oraz SIO, Empatia i nnych.
2. Każda osoba przed przystąpieniem do przetwarzania danych osobowych w systemach informatycznych zobligowana jest do zapoznania się z:
   1) Rozporządzeniem
   2) Polityką Ochrony Danych Osobowych w Fundacji RAZEM-CS w Zamościu
   3) Polityką Ochrony Danych Osobowych w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych Fundacji RAZEM-CS
   4) Niniejszą Polityką
3. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych może uzyskać wyłącznie osoba uprawniona, która posiada imienne upoważnienie do przetwarzania danych osobowych.
4. Nadanie i jakiekolwiek zmiany uprawnień do użytkowania systemu informatycznego, w którym przetwarzane są dane osobowe następują wyłącznie na wniosek bezpośredniego przełożonego użytkownika.
5. Wniosek dotyczący systemu, w którym przetwarza się dane osobowe wymaga akceptacji Administratora Danych.
6. Bezpośredni przełożony występuje z wnioskiem o nadanie/modyfikacje/odbiór uprawnień dla pracownika w następujących sytuacjach:

1) Pracownik nowoprzyjęty
2) Pracownik zmieniający stanowisko pracy lub miejsce zatrudnienia w ramach Fundacji RAZEM-CS
3) Pracownik, dla którego w ramach jego obowiązków służbowych zaistniała konieczność modyfikacji nadanych wcześniej uprawnień
4) Pracownik, dla którego w ramach jego obowiązków zaistniała konieczność nadania uprawnień.

7. Wszystkie nadane/ modyfikowane/ wycofane uprawnienia, inaczej zwane upoważnieniami rejestrowane są w rejestrze nadanych upoważnień RODO. Niniejszy Rejestr znajduje się w dokumentacji Fundacji RAZEM-CS, prowadzonej przez wyznaczonego Administratora.

ROZDZIAŁ III. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA W SYSTEMIE ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. Identyfikacja i uwierzytelnianie użytkownika
    1) W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli do tych danych
    2) Stosowanie mechanizmów uwierzytelniania i zarzadzanie hasłami użytkownika w systemach informatycznych ma na celu ochronę danych przed nieuprawnionym dostępem, utratą i modyfikacją danych osobowych. Ponadto realizacja zasad uwierzytelniania użytkownika w systemie pozwala na zapewnienie dostępności, autentyczności, rozliczalności, integralności i poufności danych.
    3) Użytkownik uzyskuje dostęp do urządzeń teleinformatycznych, z których ma dostęp do systemów informatycznych wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przy pomocy hasła.
    4) Użytkownik uzyskuje dostęp do systemu, w którym są przetwarzane dane osobowe po wprowadzeniu loginu i hasła oraz dodatkowo po dokonaniu uwierzytelnienia za pomocą profilu zaufanego.
    5) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych w systemie teleinformatycznym, nie może być przydzielony innej osobie.
2. Zarządzanie i zasady posługiwania się hasłami
    1) Przekazywaniem haseł zajmuje się Osoba zarządzająca sprzętem komputerowym wspólnie z Administratorem Danych Fundacji RAZEM-CS
    2) Użytkownik jest odpowiedzialny za wszystkie operacje dokonywane przy użyciu jego identyfikatora oraz zachowanie poufności swojego hasła. Hasło należy utrzymywać w tajemnicy również po upływie jego ważności.
    3) Oprogramowanie systemowe nie może pozwalać na wyświetlanie hasła jawnym tekstem na monitorze komputera, jak również na przechowywanie i zapisywanie hasła w postaci jawnego tekstu.
    4) Użytkownikowi zabrania się przekazywania hasła innym osobom oraz zapisywania i umieszczania haseł w miejscach, w których mogłoby zostać ujawnione.

5) Hasła dostępu z uprawnieniami Administratora powinny być przechowywane w bezpiecznym miejscu, w sposób zapewniający utrzymanie ich w tajemnicy.
6) Wymagania dotyczące haseł:
    b) Musi składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne
    c) Musi być zmieniane co kwartał
    d) Musi być inne niż 5 ostatnio używanych haseł

ROZDZIAŁ IV. PROCEDURY, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU I URZADZEŃ TELEINFORMATYCZNYCH

1. Procedura rozpoczęcia pracy:
    1) Przed rozpoczęciem pracy, użytkownik powinien sprawdzić, czy na stacji roboczej lub innym sprzęcie informatycznym nie znajdują się ślady uszkodzeń lub ingerencji osób trzecich (w przypadku podejrzenia naruszenia zabezpieczeń systemu teleinformatycznego służącego do przetwarzania danych osobowych należy niezwłocznie powiadomić Osobę zarządzającą sprzętem komputerowym i Administratora Danych).
    2) należy uruchomić komputer oraz zalogować się do systemu za pomocą loginu i hasła, a w przypadku systemów, w których są przetwarzane dane osobowe, uwierzytelnić profilem zaufanym. Hasło należy wprowadzać w sposób zapewniający jego poufność tj. uniemożliwiający jego podejrzenie.
    3) Monitory urządzeń komputerowych musza być ustawione w sposób uniemożliwiający osobie nieuprawnionej wgląd w wyświetlane na monitorze dane osobowe.
2. Procedura zawieszenia pracy w systemie:
    1) Użytkownik systemu powinien przestrzegać zasady czystego ekranu, która polega na zabezpieczeniu komputera pozostawionego bez nadzoru przed jego nieuprawnionym użyciem. Użytkownik przy każdorazowym opuszczeniu stanowiska komputerowego powinien zadbać, aby na ekranie nie były wyświetlane dane osobowe. W sytuacji pozostawienia bez nadzoru komputera lub innego sprzętu zabezpieczanego hasłem oraz w momencie opuszczania pomieszczenia biurowego, w którym to urządzenie się znajduje, użytkownik zobowiązany jest do zablokowania urządzenia (blokowanie komputera z zainstalowanym systemem operacyjnym Microsoft Windows dokonuje się poprzez naciśnięcie klawiszy „Windows flaga +L” lub „CTRL+ALT+Delete”, a następnie ENTER.)
    2) Na stacjach roboczych wymaga się stosowania wygaszacza ekranu chronionego hasłem w przypadku braku aktywności użytkownika w systemie.
3. Procedura zakończenia pracy w systemie:
    1) Zamknąć uruchomiony program/aplikacje służącą do przetwarzania danych osobowych.
    2) Wylogować się z systemu

3) Wyłączyć urządzenie komputerowe (niedopuszczalne jest wyłączenie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

ROZDZIAŁ V. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. W Fundacji RAZEM-CS w Zamościu dane osobowe przetwarzane w systemie teleinformatycznym zabezpiecza się poprzez wykonywanie kopii zapasowych zbiorów danych i programów służących do przetwarzania danych. Kopie zapasowe tworzy się w celu zapewnienia optymalnego poziomu ochrony danych osobowych przetwarzanych w Fundacji RAZEM-CS.
2. Za wskazanie zbiorów do zabezpieczenia kopią zapasową odpowiada Administrator Danych Fundacji RAZEM-CS w Zamościu.
3. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem ma obowiązek okresowo przeprowadzać operacje testowego odzyskiwania danych z wykonanych kopii zapasowych w celu weryfikacji procesu odtworzenia kopii. Odtworzenie może być sprawdzane wyłącznie w środowisku testowym.
4. Użytkownik ma następujące możliwości zabezpieczenia danych (plików):
    1) Sporządzenie kopii zapasowych na wymiennym nośniku
    2) Przechowywanie danych (plików) zapisanych na nośnikach informacji

ROZDZIAŁ VI. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.

1. W Fundacji RAZEM-CS istnieje obowiązek przechowywania wydruków, elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych w miejscach zabezpieczających dane przed nieuprawnionym dostępem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
2. Z uwagi na specyfikę pracy Fundacji RAZEM-CS związaną z realizacją projektów współfinansowanych ze środków Unii Europejskiej, każdy pracownik upoważniony do obsługi projektów posiada własny elektroniczny nośnik danych, za który osobiście odpowiada.
3. Wydruki informacji zawierające dane osobowe przechowywane są w zabezpieczonym pomieszczeniu biura Fundacji RAZEM-CS w metalowej szafie zamykanej na klucz, stanowiącym główny obszar przetwarzania danych osobowych określonych w załączniku do Polityki Ochrony Danych Osobowych w Fundacji RAZEM-CS w Zamościu.
4. Kierownik biura ponosi odpowiedzialność za zabezpieczenie kluczy do szafy, w której przechowywane są dane osobowe.

5. Wydruki zawierające dane osobowe, należy zniszczyć w niszczarce niezwłocznie po ich wykorzystaniu, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.

ROZDZIAŁ VII. ZABEZPIECZENIE I OCHRONA SYSTEMU

1. Za integralność i utrzymanie prawidłowego działania systemów informatycznych służących do przetwarzania danych osobowych odpowiada Osoba zarządzająca sprzętem komputerowym i oprogramowaniem.
2. Bezpieczeństwo funkcjonowania sieci komputerowej zapewnia się poprzez zabezpieczenia sprzętowe, oprogramowanie i procedury oraz serwisowanie sprzętu komputerowego.
3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed:
    a. Utratą danych osobowych spowodowaną awarią lub zakłóceniami zasilania
    b. Zagrożeniami pochodzącymi z sieci publicznej poprzez stosowanie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem do danych
    c. Działaniem szkodliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.
4. Połączenie sieci wewnętrznej z Internetem jest realizowane za pośrednictwem urządzeń zapewniających ochronę zasobów komputerowych znajdujących się w sieci wewnętrznej.
5. Dostęp do sieci Internet związany jest m.in. z następującymi zagrożeniami: utrata kontroli nad zasobami systemu informatycznego, przechwycenie informacji na temat zasobów sieci wewnętrznej, atak na zasoby sieci, dostęp do zasobów systemu, w którym przetwarzane są dane osobowe.
6. Ochrona przed wyżej wymienionymi zagrożeniami odbywa się poprzez wprowadzenie i przestrzeganie określonych procedur, instrukcji zasad i mechanizmów technicznych na etapie wdrożenia oraz eksploatacji systemu teleinformatycznego polegających w szczególności na:
    a. Stosowaniu sprzętowych i programowych zabezpieczeń na styku z siecią Internet
    b. Zarządzaniu dostępem do sieci Internet
    c. Stosowaniu ograniczeń w dostępie do usług internetowych
    d. Stosowaniu odpowiednich zabezpieczeń stanowisk komputerowych mających dostęp do sieci Internet
    e. Kontrolowaniu dostępu użytkowników do usług i zasobów sieci Internet zgodnie z przyznanymi uprawnieniami
    f. Konieczności użytkowania bezpiecznych, ogólnie znanych stron www
    g. Blokowaniu niektórych stron internetowych
7. Szkodliwym oprogramowaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu i zniszczenia w systemie są:
    a. Wirusy, konie trojańskie, robaki internetowe

b. Programy mające na celu nieautoryzowane zdobycie, modyfikacje lub destrukcje danych
c. Programy umożliwiające zdobycie lub podniesienie uprawnień w systemach informatycznych służących do przetwarzania danych
d. Programy które mogą wpłynąć niekorzystnie na pracę systemów informatycznych poprzez utrudnienie lub sparaliżowanie ich pracy
e. Inne, które mogą spowodować destabilizacje działania i fałszowanie danych

8. W przypadku nastąpienia naruszeń ochrony danych osobowych w systemie teleinformatycznym należy podjąć działania zgodnie z Polityką Ochrony Danych Osobowych w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych w Fundacji RAZEM-CS w Zamościu.
9. W Fundacji RAZEM-CS każdy komputer jest objęty ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego.
10. Za instalacje i właściwe skonfigurowanie oprogramowania antywirusowego na stanowiskach roboczych i komputerach przenośnych odpowiada Osoba zarządzająca sprzętem komputerowym i oprogramowaniem.
11. Aktualizacja baz wirusów odbywa się automatycznie. Po każdej naprawie i konserwacji urządzenia, a przed ponownym włączeniem do systemu informatycznego zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania.

ROZDZIAŁ VIII. ZASADY DLA UŻYTKOWNIKÓW SYSTEMU TELEINFORMATYCZNEGO

1. Użytkownik systemu teleinformatycznego jest zobowiązany do:
    1) Przestrzegania prawa oraz wewnętrznych regulacji w zakresie prawidłowego i bezpiecznego przetwarzania danych osobowych w systemie informatycznym
    2) Prawidłowego korzystania z urządzeń i systemów informatycznych zgodnie z powierzonymi obowiązkami służbowymi
    3) Ochrony powierzonego sprzętu komputerowego oraz wszystkich zasobów systemu teleinformatycznego, z których korzysta podczas przetwarzania danych osobowych w ramach wykonywania swoich obowiązków służbowych
    4) Ochrony danych osobowych przed ich udostępnianiem osobom nieupoważnionym, nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem stosując dostępne środki techniczne oraz zasady opisane w niniejszej Polityce oraz Polityce Ochrony Danych Osobowych w Fundacji RAZEM-CS
    5) Zachowania szczególnej staranności przy przetwarzaniu danych osobowych, a zwłaszcza do zapewnienia, aby dane były:
        a) Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą
        b) Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych

nie jest uznawane w myśl art. 89 ust. 1 Rozporządzenia za niezgodne z pierwotnymi celami (ograniczenie celu)

c) Adekwatne, stosowne oraz ograniczone do niezbędnego minimum do celów w których są przetwarzane (minimalizacja danych)

d) Prawidłowe i w razie potrzeby uaktualniane, należy podjąć niezbędne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (prawidłowość)

e) Przechowywane w formie umożliwiającej identyfikację osób, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w którym dane są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub celów statystycznych na mocy art. 89 ust.1 Rozporządzenia, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy Rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą

f) Przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2. Użytkownikom nie wolno:
   1) Wykorzystywać identyfikator innych użytkowników i uruchamiać aplikacji deszyfrujących (łamiących) hasła
   2) Ujawniać innym osobom przetwarzanych danych osobowych oraz informacji o sposobach zabezpieczenia danych osobowych w systemach teleinformatycznych
   3) Używania modemów GSM będących na wyposażeniu sprzętu przenośnego podczas korzystania z sieci LAN. Urządzenia te powinny być wtedy wyłączone lub zablokowane
   4) Przechowywania na dostępnych zasobach informatycznych, tj. komputer, nośniki wymienne, dyski sieciowe itp. wszystkiego rodzaju utworów np. muzyka, filmy, programy naruszające prawo do własności intelektualnej zgodnie z ustawą o prawie autorskim i prawach pokrewnych
   5) Korzystania z oprogramowania innego niż zakupione na podstawie odpowiednich umów zawartych przez Fundację RAZEM-CS lub stworzone samodzielnie, zatwierdzone i udostępnione do użytku przez osobę zarządzającą sprzętem komputerowym i oprogramowaniem
   6) Samodzielnej instalacji lub deinstalacji jakiegokolwiek oprogramowania
   7) Samodzielnej instalacji wymiany i usuwania jakichkolwiek komponentów oraz wyposażenia urządzenia komputerowego bez zgody Osoby zarządzającej sprzętem komputerowym i oprogramowaniem w Fundacji RAZEM-CS

8) Samodzielnego uruchamiania urządzenia komputerowego z nośników zewnętrznych
9) Wynoszenia komputerów stacjonarnych lub jakichkolwiek elementów komputerów z siedziby Biura Fundacji RAZEM-CS
10) Przechowywania danych służbowych na prywatnych komputerach
11) Wykonywania kopii i dystrybucji oprogramowania i jego dokumentacji, których właścicielem jest Fundacja RAZEM-CS
12) Modyfikowania logów i plików systemowych
13) Dokonania prób obejścia zabezpieczeń narzucanych przez systemy informatyczne.