Załącznik Nr 2
do zarządzenia Nr 51
Mazowieckiego Kuratora Oświaty
z dnia 14 czerwca 2012 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W KURATORIUM OŚWIATY W WARSZAWIE

Spis treści

Stosowane definicje

Administrator danych osobowych, zwany dalej „ADO" – organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. W Kuratorium Oświaty w Warszawie zadania Administratora danych osobowych wykonuje Mazowiecki Kurator Oświaty.

Administrator bezpieczeństwa informacji, zwany dalej „ABI" – osoba wyznaczona przez ADO, pełniąca obowiązki wskazane w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926, z późn. zm.), zwanej dalej „ustawą" i odpowiedzialna za nadzór nad zapewnieniem bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Kuratorium Oświaty w Warszawie**.**

Administrator systemu informatycznego, zwany dalej „ASI" – osoba wyznaczona przez ADO, odpowiedzialna za nadzór nad zapewnieniem poprawnego i bezpiecznego przetwarzania informacji w systemie informatycznym Kuratorium Oświaty w Warszawie oraz za sprawność, konserwację i wdrażanie technicznych zabezpieczeń tego systemu przez lokalnych administratorów systemu.

Lokalni administratorzy systemu, zwani dalej „LAS" – osoby podlegające ASI, odpowiedzialne w Kuratorium i w delegaturach za praktyczną realizację zadań dotyczących zapewnienia poprawnego i bezpiecznego przetwarzania informacji w systemie informatycznym oraz za sprawność, konserwację i wdrażanie technicznych zabezpieczeń tego systemu.

Osoba upoważniona do przetwarzania danych osobowych, zwana dalej „osobą upoważnioną" – osoba, której ADO nadał uprawnienia w formie pisemnego upoważnienia do przetwarzania danych osobowych w określonym czasie i zakresie i dla której upoważnienie to nie zostało całkowicie wycofane.

Przetwarzanie danych osobowych, rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym**.**

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

Użytkownik systemu informatycznego, zwany dalej „użytkownikiem" – pracownik korzystający z systemu informatycznego Kuratorium Oświaty w Warszawie przy wykonywaniu powierzonych obowiązków służbowych.

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

Stacja robocza, stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

Dokumentacja przetwarzania danych osobowych, zgodnie z rozporządzeniem 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. z 2004 r. Nr 100, poz. 1024).

1. Procedura nadawania uprawnień do przetwarzania danych i ich rejestrowania w systemie informatycznym Kuratorium Oświaty w Warszawie

1) ADO jest uprawniony do nadawania uprawnień do dostępu do danych osobowych i ich przetwarzania. Nadawanie uprawnień odbywa się poprzez wystawienie i wydanie w formie pisemnej stosownego upoważnienia do dostępu do danych osobowych i ich przetwarzania. Powyższe zagadnienie jest szczegółowo opisane w **„Procedurze nadawania uprawnień do przetwarzania danych osobowych i rejestrowania ich w systemie informatycznym w Kuratorium Oświaty w Warszawie" –** stanowiącej załącznik nr 1 do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie.
2) W procesie nadawania uprawnień do przetwarzania danych osobowych, należy korzystać z dokumentów opracowanych według wzorów formularzy, określonych w załącznikach od nr 2 do nr 6 do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1) Zasady stosowania haseł w ramach użytkowania systemu informatycznego:
   a) użytkownicy systemu informatycznego i aplikacji przetwarzających dane osobowe korzystają w procesie uwierzytelnienia z identyfikatorów i haseł;
   b) identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie;
   c) nowe hasło jest przekazywane użytkownikowi przez LAS;
   d) po zalogowaniu do systemu informatycznego z wykorzystaniem hasła otrzymanego od LAS, użytkownik jest zobowiązany do dokonania natychmiastowej zmiany hasła;
   e) hasła dostępu do systemu informatycznego oraz aplikacji przetwarzających dane osobowe musi spełniać poniższe warunki:
      - nie być krótsze niż osiem znaków,
      - zawierać małe i duże litery oraz cyfry lub znaki specjalne,
      - zmieniane przez użytkownika nie rzadziej niż 30 dni oraz powinno różnić się od pięciu ostatnio używanych haseł;
   f) oprogramowanie systemowe oraz aplikacje powinny być skonfigurowane w taki sposób, o ile ich funkcjonalność na to pozwala, aby wymuszać stosowanie powyżej opisanych zasad. Brak powyższych mechanizmów funkcjonalnych w programie nie zwalnia użytkowników systemu informatycznego z obowiązku ich przestrzegania;
   g) użytkownik zobowiązany jest do:
      - nieujawniania hasła innym osobom,
      - zachowania hasła w tajemnicy, również po jego wygaśnięciu,
      - niezapisywania hasła w sposób ogólnie dostępny,
      - przestrzegania zasad dotyczących jakości i częstotliwości zmiany hasła,

- wprowadzania hasła do systemu w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie;

h) w przypadku utraty hasła do systemu informatycznego użytkownik występuje niezwłocznie do LAS z wnioskiem o udostępnienie nowego hasła. Po otrzymaniu wniosku LAS generuje nowe hasło i przekazuje je użytkownikowi.

2) Postępowanie w zakresie haseł administracyjnych:

a) administracja systemem informatycznym powinna odbywać się z wykorzystaniem kont przypisanych poszczególnym osobom administrującym systemem. Dopuszczalne jest stosowanie jednego identyfikatora dla upoważnionych osób, o ile jest to uwarunkowane względami technicznymi;

b) hasła administracyjne podlegają wymaganiom wskazanym w pkt 2 ppkt 1 lit. e „Zasad stosowania haseł w ramach użytkowania systemu informatycznego"*;*

c) hasła do wspólnych kont administracyjnych deponowane są w sejfie ABI, znajdującym się w pomieszczeniu nr 306. Dostęp do sejfu mają ABI ASI i ADO;

d) za nadzór nad zmianą haseł do wspólnych kont administracyjnych i przekazanie ich ABI odpowiedzialny jest ASI; technicznie zmianę haseł wykonuje LAS, który przekazuje je w zapieczętowanej kopercie ABI, a w razie jego nieobecności ASI;

e) za bezpieczeństwo zdeponowanych nowych haseł i zniszczenie starych odpowiedzialny jest ABI;

f) zniszczenie starych haseł powinno być przeprowadzone w sposób nieodwracalny, po dostarczeniu do zdeponowania nowych haseł.

3) Metody i środki uwierzytelnienia:

a) każdy użytkownik posiada swoje konto na stacji roboczej. Dostęp do systemu informatycznego możliwy jest po zalogowaniu się użytkownika na swoje konto;

b) kolejny etap uwierzytelniania realizowany jest na poziomie poszczególnych programów. Wykorzystywany jest w tym celu mechanizm identyfikatorów i haseł. Miejsce uwierzytelnienia jest uzależnione od rodzaju programu;

c) programy i systemy operacyjne w miarę możliwości technicznych, powinny być skonfigurowane w taki sposób, aby pięciokrotne, następujące po sobie, wprowadzenie błędnego hasła powodowało zablokowanie konta użytkownika co najmniej na godzinę. Na wniosek użytkownika, LAS może odblokować je wcześniej.

4) Zasady rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów informatycznych:

a) rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik wprowadza niezbędny do pracy identyfikator i hasło. Hasło jest wprowadzane w sposób minimalizujący ryzyko podejrzenia go przez osoby trzecie;

b) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, użytkownik kontaktuje się z LAS;

c) w przypadku niestandardowego zachowania programu przetwarzającego dane osobowe, użytkownik natychmiast kontaktuje się z LAS. W szczególności dotyczy to sytuacji, gdy:
   - wygląd programu odbiega od stanu normalnego,
   - pewne opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też pewne opcje niedostępne użytkownikowi w normalnej sytuacji zostały udostępnione,
   - sposób działania programu odbiega od stanu normalnego,
   - nastąpiło znaczące spowolnienie działania systemu informatycznego,
   - zakres danych lub sposób ich przedstawiania przez program odbiega od stanu normalnego;

d) zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy) użytkownik blokuje stację roboczą, korzystając z klawiszy Ctrl-Alt-Delete. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej, poprzez ponowne wciśnięcie klawiszy Ctrl-Alt-Delete oraz wprowadzenie hasła, w sposób gwarantujący brak możliwości jego podejrzenia przez osoby trzecie. W przypadku stacji roboczych z systemami operacyjnymi nieposiadającymi mechanizmu blokowania, użytkownik zobowiązany jest do zamknięcia programu i wyłączenia stacji roboczej;

e) kończąc pracę w systemie informatycznym użytkownik wylogowuje się ze wszystkich programów, z których korzystał oraz zamyka system operacyjny i wyłącza stację roboczą. W przypadku, gdy użytkownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, włącza alarm, o ile pomieszczenie wyposażone jest w system alarmowy oraz deponuje klucz, zgodnie z obowiązującymi zasadami jego przechowywania.

5) Procedury przetwarzania danych osobowych na komputerach przenośnych:
Przechowywanie i przetwarzanie danych osobowych na komputerach przenośnych realizowane może być wyłącznie na zasadach opisanych w rozdziale 7 Polityki bezpieczeństwa.

6) Procedury wykonywania kopii zapasowych:

a) kopie zapasowe serwerów wykonywane są przez LAS. Kopie te wykonuje się w celu zapobieżenia utraty serwera na skutek nieprzewidzianych zdarzeń losowych. Za nadzór nad wykonywaniem kopii zapasowych serwerów przez LAS odpowiada ASI;

b) na pisemny, zaakceptowany przez przełożonego, wniosek osoby upoważnionej do przetwarzania zbiorów danych osobowych, LAS za zgodą ASI wykonuje dodatkowe kopie zapasowe zbiorów przechowywanych na serwerach;

c) za wykonywanie kopii zapasowych zbiorów danych osobowych odpowiadają pracownicy, których upoważniono do ich gromadzenia i przetwarzania. Jeśli wykonanie takiej kopii nie jest możliwe z przyczyn technicznych, pracownik

informuje o tym LAS, który opracowuje i wdraża odpowiedni dla danego przypadku system tworzenia kopii, o ile środki techniczne i rodzaj oprogramowania to umożliwiają;

d) kopie zapasowe serwerów wykonuje się raz na dobę w godzinach nocnych, zaś pracownicy upoważnienie do przetwarzania danych osobowych wykonują kopie do końca dnia, w którym wprowadzono zmiany w zbiorze;

e) kopie zapasowe serwerów wykonuje się na dysku niezależnego komputera, znajdującego się w pomieszczeniu innym niż serwery, należycie chronionym lub na nośnikach wymiennych (dysk twardy przenośny, płyta CD/DVD, pamięć przenośna USB);

f) pracownicy upoważnieni do przetwarzania zbiorów danych osobowych wykonują kopie zapasowe na nośnikach wymiennych (np. płyta CD/DVD, pamięć przenośna USB), które przechowują w zamkniętej na klucz szafie/biurku;

g) opisy kopii zapasowych powinny wskazywać jednoznacznie nazwę zbioru danych osobowych lub zasobu, którego kopia dotyczy oraz datę jej wykonania;

h) niszczenia kopi zapasowych zbiorów danych osobowych dokonuje się po wygaśnięciu podstaw do jego przetwarzania i wycofaniu zbioru z ewidencji GIODO na zaakceptowany przez przełożonego wniosek użytkownika złożony do ABI;

i) ASI jest odpowiedzialny za koordynację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego. Działania odtworzeniowe realizowane są w oparciu o istniejące kopie zapasowe. Po odtworzeniu systemu informatycznego ASI jest zobowiązany do przeprowadzenia testów poprawności jego działania przed oddaniem systemu do użytkowania;

j) ASI na wniosek ABI jest odpowiedzialny za okresowe testowanie możliwości odtworzenia danych zapisanych na kopiach zapasowych, a w przypadku negatywnych wyników testów za podjęcie właściwych działań korygujących.

3. Przechowywanie nośników informacji

1) Ogólne zasady postępowania z nośnikami informacji:
   a) przy przekazywaniu danych osobowych drogą elektroniczną poza teren Kuratorium wymagane jest zastosowanie procedury opisanej w Polityce bezpieczeństwa;
   b) wydruki z danymi osobowymi podlegają ewidencjonowaniu zgodnie z obowiązującymi zasadami opisanymi w Instrukcji kancelaryjnej;
   c) papierowe i elektroniczne nośniki danych zawierające dane osobowe przechowywane są w sposób minimalizujący ryzyko dostępu do nich osób nieupoważnionych. W szczególności powinny być one przechowywane w zamkniętych szafkach na terenie obszaru, w którym przetwarzane są dane osobowe;
   d) dane osobowe w systemie informatycznym przechowywane są przez czas wymagany spełnieniem celu, dla którego są one przetwarzane, a po jego upływie podlegają zniszczeniu;

e) w przypadku zmiany przeznaczenia sprzętu komputerowego dane osobowe na nim zapisane podlegają usunięciu;
f) w przypadku likwidacji sprzętu komputerowego, znajdujące się w nim nośniki danych np. dysk twardy, podlegają fizycznemu zniszczeniu. Za techniczne zniszczenie nośnika danych odpowiedzialny jest LAS po poinformowaniu ASI. Prawidłowość wykonania czynności potwierdza ABI.

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

1) Obowiązki użytkowników:

a) w celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

- korzystania z wszelkich nośników stwarzających zagrożenie dla systemu informatycznego,
- otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi. W przypadkach wątpliwych należy skonsultować się z bezpośrednim przełożonym,
- dostępu do stron internetowych nie związanych z pełnionymi obowiązkami służbowymi, a w szczególności dostępu do stron nie należących do wiarygodnych organizacji lub podmiotów;

b) w przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić LAS. Do powyższych objawów można zaliczyć:
- istotne spowolnienie działania systemu informatycznego,
- nietypowe działanie programu,
- nietypowe komunikaty,
- utrata danych lub modyfikacja danych.

2) Stosowane zabezpieczenia przed niebezpiecznym oprogramowaniem:
a) system informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
- ograniczenie uprawnień użytkowników na większości stacji roboczych,
- zabezpieczenie komputerów użytkowników oprogramowaniem antywirusowym, automatycznie aktualizującym sygnatury wirusów,
- zapory sieciowe zainstalowane na stacjach roboczych,
- automatyczna aktualizacja oprogramowania systemów operacyjnych komputerów,
- okresowe badanie bezpieczeństwa sieci.

5. Zasady wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1) Przegląd i konserwacja sprzętu informatycznego oraz nośników informacji wbudowanych w sprzęt stacjonarny są realizowane przez wyznaczonych przez ASI pracowników.

2) W przypadku, gdy prace muszą być przeprowadzone poza Kuratorium, w szczególności, jeżeli dotyczą one serwisu sprzętu objętego gwarancją, przed dostarczeniem sprzętu do naprawy, należy wyjąć nośnik danych (dysk twardy HDD), a jeżeli nie jest to możliwe to usunąć dane osobowe i program służący do ich przetwarzania przy użyciu oprogramowania do bezpiecznego usuwania danych, uprzednio sporządzając kopię zapasową zbiorów danych osobowych i programu na nośnik przenośny.

6. Postępowanie użytkowników w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji

1) Każdy użytkownik jest zobowiązany do powiadomienia o zauważonym incydencie ABI. W przypadkach, gdy nie jest możliwe powiadomienie ABI, użytkownik powiadamia ASI.

2) O naruszeniu bezpieczeństwa danych osobowych mogą świadczyć:
   a) zagubienie lub kradzież nośnika z danymi osobowymi;
   b) kradzież sprzętu informatycznego, w którym przechowywane są dane;
   c) brak możliwości uruchomienia przez użytkownika programu pozwalającego na dostęp do danych osobowych;
   d) brak możliwości zalogowania się do tego programu;
   e) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w programie, w tym brak możliwości wykonania pewnych operacji dostępnych użytkownikowi lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
   f) niestandardowy wygląd programu;
   g) poszerzony lub zawężony zakres danych dostępnych użytkownikowi;
   h) znaczne spowolnienie działania systemu informatycznego;
   i) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny;
   j) ślady włamania lub prób włamania do pomieszczeń na terenie obszaru przetwarzania danych osobowych;
   k) włamanie lub próby włamania do szafek, w których przechowywane są w formie papierowej lub elektronicznej nośniki danych osobowych;
   l) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami;
   m) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej;
   n) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3) ABI wraz z ASI i właściwymi merytorycznie pracownikami Kuratorium podejmują działania zmierzające do:
   a) potwierdzenia wystąpienia incydentu;
   b) ustalenia przyczyn wystąpienia incydentu i zabezpieczenia ewentualnych dowodów;
   c) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się incydentu;
   d) usunięcia skutków incydentu;

e) monitorowania działania odtworzonego systemu, celem potwierdzenia usunięcia zagrożenia;
f) analizy podatności, które przyczyniły się do wystąpienia incydentu i określenia wymaganych działań korekcyjnych.

4) W przypadku incydentów spowodowanych celowym działaniem, ABI powiadamia ADO o zaistniałym fakcie. ADO może powiadomić organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

5) ABI prowadzi ewidencję wykrytych incydentów, uwzględniającą:
   a) imię i nazwisko osoby zgłaszającej incydent;
   b) datę zgłoszenia incydentu;
   c) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu;
   d) wyniki przeprowadzonych działań;
   e) podjęte działania naprawcze.
6) ABI co najmniej raz w roku dokonuje przeglądu ewidencji incydentów, celem określenia ewentualnych działań korekcyjnych w zakresie zabezpieczenia przetwarzania danych osobowych i obsługi incydentów. W trakcie powyższych prac analitycznych ABI może zobowiązać osoby, od których zgłoszenia incydentów były przyjmowane, do udzielenia dodatkowych wyjaśnień.