INSTRUKCJA ZRZĄDZANIA SYSTEMEM INFORMATYCZNYM

Zarząd Stowarzyszenia Lokalna Grupa Działania "EUROGLICJA" z siedzibą w Sokołowie Małopolskim, będąc jednocześnie administratorem danych osobowych przetwarzanych w systemie informatycznym wprowadza niniejszą instrukcję zarządzania systemem informatycznym. Celem instrukcji jest zapewnienie efektywnego zarządzania systemem informatycznym oraz zapewnienie należytej ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami.

I. Postanowienia ogólne

1. Definicje

Ilekroć w instrukcji jest mowa o:

1) ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) rozporządzeniu - rozumie się przez to rozporządzenie 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),
3) administratorze danych - rozumie się przez to Stowarzyszenie LGD Eurogalicja,
4) administratorze bezpieczeństwa informacji - rozumie się przez to osobę wyznaczoną przez administratora danych,
5) administratorze systemu – rozumie się przed to osobę wyznaczoną przez administratora danych,
6) osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która została upoważniona na piśmie przez administratora danych do przetwarzania danych osobowych,
7) użytkowniku - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
8) odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
a. osoby, której dane dotyczą,
b. osoby upoważnionej do przetwarzania danych,
c. przedstawiciela, o którym mowa w art. 31a ustawy,
d. podmiotu, o którym mowa w art. 31 ustawy,
e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
2) identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
12) uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
13) serwisancie - rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.

W związku z tym, iż kilka urządzeń systemu informatycznego administratora danych jest połączonych z siecią publiczną, administrator danych stosuje środki bezpieczeństwa o których mowa w rozporządzeniu na poziomie wysokim.

II. Postanowienia szczegółowe

Instrukcja zarządzania systemem informatycznym zawiera następujące informacje:
1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy 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, o których mowa w pkt 4,
2) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
3) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
4) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Ad. 1

System informatyczny administratora danych obejmuje trzy komputery stacjonarne oraz jeden komputery przenośne – wszystkie połączone siecią za pomocą protokołu internetowego TCP/IP. Do systemu informatycznego administratora danych mają dostęp wyłącznie osoby upoważnione przez administratora danych do przetwarzania danych osobowych. Administrator systemu niezwłocznie po uzyskaniu upoważnienia rejestruje osobę upoważnioną w ewidencji osób upoważnionych do przetwarzania danych osobowych oraz nadaje jej identyfikator i hasło. Administrator danych w czasie nieobecności administratora systemu upoważnia inną osobę do wprowadzania do rejestru osób, którym nadano upoważnienia do przetwarzania danych osobowych oraz do nadawania im identyfikatora i hasła.

Ad. 2

Uwierzytelnienie użytkownika systemu odbywa się poprzez wprowadzenie do systemu informatycznego identyfikatora oraz hasła.

Identyfikator użytkownika składa się z imienia i nazwiska osoby upoważnionej do przetwarzania danych osobowych pisanego łącznie, z małych liter, bez znaków interpunkcyjnych.

Hasło zgodnie z rozporządzeniem składa się z co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.

Użytkownik jest zobowiązany do zmiany hasła, nie rzadziej jednak niż co 30 dni.

Użytkownik systemu jest zobowiązany do zachowania w tajemnicy hasła dostępu i nie może go udostępniać osobom nieuprawnionym.

Administrator systemu sprawuje kontrolę nad procesem pierwszego uwierzytelnienia użytkownika oraz wykreśla użytkownika z systemu. Wykreślenie użytkownika z systemu następuje na skutek pozbawienia go przez administratora danych upoważnienia do przetwarzania danych osobowych. Przyczyną pozbawienia upoważnienia może być w szczególności: udostępnienie hasła osobie

nieupoważnionej; kradzież danych osobowych zawartych w zbiorach; wykluczenie ze Stowarzyszenia LGD "EUROGALICJA".

Ad. 3

Użytkownik systemu w celu rozpoczęcia pracy jest zobowiązany do:

1) włączenia napięcia na listwie sieciowej,
2) włączenia komputera,
3) wprowadzenia identyfikatora użytkownika,
4) wprowadzenia hasła użytkownika.

Użytkownik systemu powinien dołożyć szczególnej staranności w celu uniemożliwienia dostępu do przetwarzanych danych osobom trzecim. W tym celu w pomieszczeniu, w którym przetwarzane są dane osobowe mogą się znajdować wyłącznie osoby posiadające upoważnienie do przetwarzania danych lub osoby trzecie przy obecności w/w osób upoważnionych do przetwarzania danych.

Użytkownik systemu na czas swojej nieobecności w pomieszczeniu ma obowiązek wylogować się z profilu użytkownika. Do jego obowiązków należy również niedopuszczenie do sytuacji, w której ze względu na nieodpowiednie ustawienie monitora dostęp do przetwarzanych danych będą miały osoby nieupoważnione. W tym celu administrator systemu wprowadzi automatyczne uruchamianie „wygaszacza ekranu" po upływie 5 minut od zaprzestania pracy w systemie informatycznym. Ponowne uruchomienie systemu nastąpi po wprowadzeniu hasła, które jest udostępniane wszystkim użytkownikom systemu.

Po zakończeniu pracy użytkownik jest zobowiązany wylogować się z systemu, a następnie wyłączyć komputer i listwę sieciową.

Ad. 4

Administrator danych przetwarza dane osobowe za pomocą edytora tekstu *„Microsoft Word"* oraz *„Microsoft Excel"* w formie plików komputerowych. Dane, o których mowa w zbiorze zawierającym dokumentację księgową i pracowniczą administratora danych są przetwarzane ręcznie, w formie papierowej, jak również w systemie informatycznym za pomocą edytora tekstu *„Microsoft Word"* i *„Microsoft Excel"* oraz System PŁATNIK, System finansowo-księgowy Comarch Optima. Zbiór danych zawierający dane udostępnione na stronie internetowej www.eurogalicja.org jest przetwarzany w systemie informatycznym administratora danych za pomocą systemu CMS WordPress oraz Joomla .

Kopie zapasowe plików zawartych w poszczególnych zbiorach danych są sporządzane każdorazowo po ich sporządzeniu.

Kopie robocze plików tworzy i przechowuje się na pamięci USB (pendrive) lub płycie CD/DVD, stanowiącej własność administratora danych.

Ad. 5

Administrator danych przechowuje przetwarzane dane osobowe na pamięci USB lub płycie CD/DVD stanowiącej własność administratora danych.

Administrator danych zgodnie z wymogami rozporządzenia:
a) przechowuje kopie robocze w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
b) usuwa je niezwłocznie po ustaniu ich użyteczności.

Administrator danych przechowuje pamięci USB i płyty CD/DVD zawierające kopie robocze plików tworzących poszczególne zbiory danych w zamykanej na klucz szafie.

Ad. 6

Zabezpieczenie systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego następuje poprzez zastosowanie przez administratora danych zapory sieciowej (firewall) oraz programu antywirusowego posiadającego funkcję ochrony antywirusowej i ochrony systemu.

Program antywirusowy zapewnia stałą ochronę przed wirusami i innymi zagrożeniami np.: trojanami, robakami. Aktualizacja programu antywirusowego jest dokonywana w częstotliwości zalecanej przez wytwórcę programu.

Kontrolę nad regularną aktualizacją programu antywirusowego sprawuje administrator systemu.

Użytkownicy systemu korzystający z zewnętrznych nośników danych są zobowiązani każdorazowo sprawdzić za pomocą programu antywirusowego, czy nośnik nie jest zainfekowany.

W przypadku zidentyfikowania przez użytkownika systemu jakichkolwiek nieprawidłowości w jego funkcjonowaniu, wskazujących w szczególności na obecność wirusa lub innego zagrożenia, zobowiązany jest on niezwłocznie powiadomić o tym fakcie administratora danych.

Ad. 7

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym administratora danych system ten zapewnia odnotowanie informacji o odbiorcach danych w rozumieniu art. 7 pkt 6 ustawy. Zakres udzielonych informacji obejmuje: dane odbiorcy, datę wydania oraz zakres udostępnionych danych.

Ad. 8

Osobą odpowiedzialną za przeprowadzenie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych jest administrator systemu. Przeglądy są dokonywane w miarę potrzeb.

W przypadku konieczności dokonania naprawy, której nie jest w stanie wykonać administrator systemu, naprawę zleca się serwisantom. Zgodnie z wymogami rozporządzenia urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

III. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomość jej treści.