ZARZĄDZENIE NR 61/2015
WÓJTA GMINY JEDWABNO
z dnia 30 czerwca 2015

w sprawie wprowadzenia „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno".

Na podstawie art. 36 ust. 1, 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182) oraz § 3, 4 i 5 Rozporządzenia 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. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1

Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Gminy Jedwabno do przestrzegania zasad i realizacji zadań określonych w załączniku, o których mowa w § 1.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

§ 4

Traci moc zarządzenie Nr 82/2011 Wójta Gminy Jedwabno z dnia 31 sierpnia 2011 roku w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Jedwabnie.

Wójt

SŁAWOMIR AMBROZIAK

Załącznik do zarządzenia Nr 61/2015
Wójta Gminy Jedwabno
z dnia 30.06.2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W Urzędzie Gminy Jedwabno

(Jedwabno, 2015)

ROZDZIAŁ I

Podstawowe pojęcia oraz zakres przedmiotowy instrukcji

§ 1

Stosownie do postanowień §3 i §5 rozporządzenia 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. Nr 100, poz. 1024), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Jedwabno.

§ 2

Ilekroć w instrukcji jest mowa o:

systemie informatycznym - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

zabezpieczeniu systemu informatycznego - należy przez to rozumieć zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.

zbiorze danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

przetwarzaniu danych - 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 systemach informatycznych;

usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Administratorze Danych Osobowych - dalej jako Administrator danych; - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem danych w Urzędzie Gminy Jedwabno jest Wójt Gminy Jedwabno;

Administratorze Bezpieczeństwa Informacji - rozumie się przez to osobę wyznaczoną przez Administratora danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

użytkowniku - rozumie się przez to upoważnionego przez Administratora danych (w przypadku powołania Administratora Bezpieczeństwa Informacji również przez ABI), wyznaczonego do przetwarzania danych osobowych pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.

§ 3

1. Instrukcja ta określa:
   a) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności;
   b) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności;
   c) procedury rozpoczęcia, zawieszenia i zakończenia pracy;
   d) metody i częstotliwość tworzenia kopii awaryjnych;
   e) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;
   f) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
   g) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
   h) sposób postępowania w zakresie komunikacji w sieci komputerowej.
2. Działaniem instrukcji objęci są:
   a) Administrator Danych;
   b) Administrator Bezpieczeństwa Informacji;
   c) osoby zatrudnione w Urzędzie Gminy Jedwabno przy przetwarzaniu danych osobowych;
   d) osoby, które przetwarzają dane osobowe znajdujące się w posiadaniu Urzędzie Gminy Jedwabno.

ROZDZIAŁ II

Administracja i organizacja bezpieczeństwa

§4

1. Instrukcja ma zastosowanie na obszarze wskazanym w Polityce Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Jedwabno (dalej Polityka Bezpieczeństwa), w którym przetwarzane są dane osobowe w systemie informatycznym.
2. Przebywanie wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych osobowych.

§ 5

Administrator Bezpieczeństwa Informacji sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień instrukcji, a w szczególności:

1) sam lub za pomocą wyznaczonej przez siebie osoby sporządza kopie bezpieczeństwa baz danych;
2) pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub - gdy nie jest to możliwe - uszkadza je trwale w sposób uniemożliwiający odczytanie danych;
3) nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;
4) zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w Polityce Bezpieczeństwa;
5) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
6) sam lub za pomocą wyznaczonej osoby sprawuje nadzór nad czynnościami związanymi z ochroną antywirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;
7) nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane osobowe;
8) podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

ROZDZIAŁ III

Obowiązki osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

§ 6

1. Dostęp do sytemu informatycznego należącego do Administratora danych posiadają jedynie osoby upoważnione.
2. Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:
   a) niepowołanym dostępem;
   b) nieuzasadnioną modyfikacją lub zniszczeniem;
   c) nielegalnym ujawnieniem;
   d) pozyskaniem w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
3. Przed dopuszczeniem do przetwarzania danych osobowych, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.
4. Bezpośredni dostęp do sprzętu i aplikacji służących do przetwarzania danych osobowych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
5. Jeżeli istnieje taka możliwość, system, na którym możliwy jest dostęp do danych osobowych, powinny automatycznie wylogować/zablokować użytkownika po upływie ustalonego czasu nieaktywności.
6. Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

ROZDZIAŁ IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

§ 7

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
   a) zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym - hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
   b) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
   c) w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji,

d) w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.

2. Przerywając przetwarzanie danych w ciągu godzin pracy, użytkownik powinien co najmniej: wylogować się z systemu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Niemniej jednak zalecane jest w takich przypadkach:

a) skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu);
b) zakończenie pracy w systemie informatycznym - wylogowanie się z systemu.

3. Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:

a) zakończenia pracy w systemie informatycznym;
b) wylogowania się z systemu informatycznego;
c) wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe;
d) zamknięcia i opuszczenia pomieszczeń biurowych;

4. Korzystanie z pomieszczeń biurowych oraz ich wyposażenia w celach niezwiązanych z przetwarzaniem danych osobowych wynikających z uzyskanego upoważnienia może następować tylko za zgodą Administratora danych lub Administratora Bezpieczeństwa Informacji i nie może być związane z przetwarzaniem danych znajdujących się w zbiorach danych Administratora danych.

5. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

ROZDZIAŁ V

Procedury rejestracji użytkowników

§ 8

1. Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.

2. Rejestr użytkowników systemu prowadzi Administrator Danych bądź Administrator Bezpieczeństwa Informacji.

3. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem i hasłem dostępu.
4. Nadawanie identyfikatorów i przydzielanie haseł;
   a) w celu jednoznacznego określenia użytkowników zaleca się następującą metodologię nadawania nazw kont:
   b) pierwsza litera imienia + nazwisko (nie używając polskich znaków i wielkich liter);
   c) hasło składa się z co najmniej 8 znaków; zalecane jest, aby zawierało małe i wielkie litery oraz cyfry i znaki specjalne;
   d) zmiana hasła powinna być wykonywana nie rzadziej niż co 30 dni. W systemie informatycznym zapewnia się automatyczne wymuszanie zmiany hasła,
   e) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie;
   f) identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzaniu danych osobowych;
   g) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie;
   h) obowiązek ten rozciąga się także na okres po upływie ważności hasła;
   i) hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika;
   j) utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.

ROZDZIAŁ VI

Kopie bezpieczeństwa

§ 9

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

§ 10

1. Kopie bezpieczeństwa baz danych powinny być wykonywane codziennie (od poniedziałku do piątku).

2. W Urzędzie Gminy Jedwabno do tworzenia kopii bezpieczeństwa wykorzystuje się dedykowane skrypty oraz przestrzeń dyskową na komputerze ABI oraz lub inne dostępne na rynku urządzenia przeznaczone do tworzenia kopii zapasowych.
3. Tworzenie kopii bezpieczeństwa odbywa się poprzez automatyczne wykonanie kopii na serwerze oraz ręczne przekopiowanie na dysk komputera ABI.
4. Osobą odpowiedzialną za tworzenie kopii zapasowych oraz weryfikację zgodnie z pkt 9 jest Administrator Bezpieczeństwa Informacji.
5. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
6. Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
7. Ewentualne dodatkowe kopie bezpieczeństwa należy przechowywać w innym miejscu niż kopie pierwotne.
8. Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz.
9. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
10. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
11. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

ROZDZIAŁ VII

Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

§ 11

1. Wydruki komputerowe z systemu, zawierające dane osobowe są sporządzane jedynie dla celów operacyjnych.

2. Wydruk komputerowy z systemu, zawierający dane osobowe, po odpowiednim opisaniu i oznaczeniu, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.
3. Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych, (operacyjnych) przechowywane są w zamykanych szafach.
4. Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w odpowiednich, przeznaczonych do tego zamykanych szafach.
5. Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
6. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.

ROZDZIAŁ VIII

Ochrona antywirusowa

§ 12

1. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie Administratora Bezpieczeństwa Informacji.
3. System informatyczny podlega regularnej, (co najmniej raz w tygodniu) kontroli pod kątem obecności wirusów komputerowych.
4. Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
5. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
6. Osobą odpowiedzialną za powyższe działania jest Administrator Bezpieczeństwa Informacji.

ROZDZIAŁ IX

Konserwacja i naprawa systemu przetwarzającego dane osobowe

§ 13

1. Prace bieżące w dziedzinie konserwacji i naprawy systemu przetwarzającego dane osobowe prowadzi osoba odpowiedzialna za te czynności lub w wypadku konieczności zaangażowania do w/w czynności przedsiębiorcy zajmującego się zawodowo ich wykonywaniem, są one wykonywane pod bezpośrednim nadzorem Administratora danych lub Administratora Bezpieczeństwa Informacji.
2. Administrator danych lub Administrator Bezpieczeństwa Informacji mogą upoważniać pracowników Biura do nadzorowania bieżących napraw w dziedzinie konserwacji i napraw.
3. Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.
4. Czynności serwisowe mogą być wykonywane jedynie pod nadzorem Administratora Bezpieczeństwa Informacji lub osoby wyznaczonej.

ROZDZIAŁ X

Sposoby postępowania w zakresie komunikacji w sieci komputerowej

§ 14

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem które będzie dostarczone innym kanałem informacyjnym np. SMS/telefon.
2. W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym.
3. Nieuzasadnione kopiowanie danych z serwera na stacje robocze bądź na nośniki informatyczne jest zabronione.

ROZDZIAŁ XI

Zasady korzystania z komputerów przenośnych

§ 15

1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w Polityce Bezpieczeństwa.

2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:

   a) zabezpieczyć dostęp do komputera hasłem (w przypadku systemu operacyjnego Windows - w sposób który umożliwia to oprogramowanie);

   b) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;

   c) zabezpieczyć aplikacje przetwarzające dane osobowe hasłem.

ROZDZIAŁ XII

Postępowanie w sytuacji stwierdzenia naruszenia ochrony danych osobowych

§16

Naruszeniem zabezpieczeń systemu informatycznego są w szczególności:

1) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych - przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych;
2) naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę);
3) celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania;
4) nieautoryzowane logowanie do systemu;
5) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
6) istnienie nieautoryzowanych kont dostępu do danych osobowych;
7) włamanie lub jego usiłowanie z zewnątrz sieci;
8) nieautoryzowane zmiany danych w systemie;
9) nie zablokowanie dostępu do systemu przez osobę uprawnioną do przetwarzania danych osobowych w czasie jej nieobecności;
10) ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
11) brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;
12) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
13) kradzież nośników, na których zapisane są dane osobowe;

14) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
15) niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
16) niewłaściwe bądź nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe.

§ 17

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym Administratora Danych oraz Administratora Bezpieczeństwa Informacji.

§ 18

W przypadkach, o których mowa w § 16 i § 17, należy podjąć czynności zmierzające do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów przestępstwa i minimalizacji zaistniałych szkód, w tym w szczególności:

1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności:
   a) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   b) dane osoby zgłaszającej,
   c) opis miejsca zdarzenia,
   d) opis przedstawiający stan techniczny sprzętu służącego do przetwarzania lub przechowywania danych osobowych,
   e) wszelkie ustalone okoliczności zdarzenia;
2) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem;
3) dokonać identyfikacji zaistniałego zdarzenia, poprzez ustalenie w szczególności:
   rozmiaru zniszczeń,
   a) sposobu, w jaki osoba niepowołana uzyskała dostęp do danych osobowych,
   b) rodzaju danych, których dotyczyło naruszenie;
   c) wyeliminować czynniki bezpośredniego zagrożenia utraty danych osobowych;

d) sporządzić protokół z wyżej wymienionych czynności;

e) poinformować właściwe organy ścigania w przypadku podejrzenia popełnienia przestępstwa.

§ 19

Administrator danych bądź Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, przy udziale osoby, o której mowa w § 17, obowiązani są do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:

a) zmianę hasła dla administratora i użytkowników;

b) fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;

c) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

§ 20

Po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych, osoby odpowiedzialne za bezpieczeństwo danych osobowych obowiązane są podjąć wszelkie inne działania mające na celu wyeliminowanie podobnych naruszeń w przyszłości oraz zmniejszenie ryzyka występowania ich negatywnych skutków. W szczególności, jeżeli przyczyną naruszenia są:

1) błąd osoby upoważnionej do przetwarzania danych osobowych związany z przetwarzaniem danych osobowych - należy przeprowadzić dodatkowe szkolenie, indywidualne lub grupowe;

2) uaktywnienie wirusa komputerowego - należy ustalić źródło jego pochodzenia oraz wykonać test zabezpieczenia antywirusowego;

3) zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych - należy wyciągnąć konsekwencje zgodnie z przepisami z zakresu prawa pracy o odpowiedzialności pracowników;

4) włamanie - należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających;

5) zły stan urządzenia lub sposób działania programu lub inne niedoskonałości informatycznego systemu przetwarzania danych osobowych - należy niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

§ 21

1. Wykonanie czynności, o których mowa w §19 i §20, ma na celu przywrócenie prawidłowego działania systemu.
2. W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych, lub ich zniekształcenia, odtwarza się bazy danych osobowych z ostatniej kopii bezpieczeństwa.

§ 22

1. Administrator Bezpieczeństwa Informacji obowiązany jest sporządzić raport ze zdarzenia naruszającego zabezpieczenia systemu informatycznego, obejmujący wnioski dotyczące całokształtu procesu teleinformatycznego przetwarzania danych osobowych, a w szczególności:
   a) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych;
   b) zawartości zbioru danych osobowych;
   c) prawidłowości działania systemu informatycznego i teleinformatycznego, w którym przetwarzane są dane osobowe z uwzględnieniem skuteczności stosowanych do chwili wystąpienia naruszenia, środków zabezpieczających przed dostępem osób niepowołanych;
   d) jakości działania sieci informatycznej;
   e) wykluczenia obecności wirusów komputerowych;
   f) ustalenia przyczyny i przebiegu zdarzenia;
   g) wyciągnięcia wniosków co do uniknięcia podobnych naruszeń w przyszłości.
2. Raport, o którym mowa w ust. 1, jest przekazywany Administratorowi danych w terminie 30 dni od dnia potwierdzenia zdarzenia naruszenia zabezpieczenia systemu informatycznego.

ROZDZIAŁ XIII
Postanowienia końcowe

§ 23

1. Instrukcja niniejsza nie narusza postanowień powszechnie obowiązującego prawa.
2. W sprawach nieunormowanych stosuje się przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182) oraz przepisy rozporządzenia 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. Nr 100, poz. 1024).

Wójt
Sławomir Ambroziak