Załącznik nr 1 do Zarządzenia nr 20/12/2013 Prezydenta Miasta Lublin z dnia 13 grudnia 2013 r.
w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Lublin

Polityka bezpieczeństwa danych osobowych

Rozdział I
Główne zasady bezpiecznego przetwarzania danych osobowych

§ 1

1. Osoba upoważniona do przetwarzania danych osobowych:
   1) zapewnia ochronę danych osobowych przed:
      a) udostępnieniem osobie nieupoważnionej,
      b) zabraniem przez osobę nieuprawnioną,
      c) przetwarzaniem z naruszeniem ustawy,
      d) zmianą,
      e) utratą,
      f) uszkodzeniem,
      g) zniszczeniem;
   2) przetwarza dane osobowe wyłącznie w zakresie czynności, do których została upoważniona i tylko w celu wykonania obowiązków służbowych;
   3) zobowiązuje się do zachowania poufności danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie, jak i po zakończeniu pracy, praktyki, stażu, lub innego stosunku prawnego.
2. Dyrektor IT, współpracując z zarządzającym zbiorem, wdraża taki system informatyczny służący do przetwarzania danych osobowych, który gwarantuje:
   1) rozliczalność;
   2) integralność;
   3) uwierzytelnianie.

Rozdział II
Organizacja procedury nadawania i odbierania uprawnień dostępu do danych osobowych oraz systemów informatycznych

§ 2

1. Zarządzający zbiorem danych osobowych:
   1) prowadzi w systemie EZD dokumentację:
      a) ewidencję upoważnień,
      b) upoważnienia do przetwarzania i cofnięcia upoważnień o symbolu klasyfikacyjnym 1334, haśle klasyfikacyjnym „Ustalanie uprawnień dostępu do danych i systemów” i kategorii archiwalnej B10 lub wyznacza pracownika do prowadzenia tej dokumentacji;
   2) ustala z dyrektorem IT, kto będzie administratorem systemu lub wyznacza go spośród sobie podległych osób upoważnionych, jak również może

powierzyć przetwarzanie danych w tym zakresie podmiotowi zewnętrznemu.
2. Zarządzający zbiorem dopuszcza do przetwarzania danych osobowych wyłącznie osoby upoważnione do przetwarzania.
3. Formularze „Upoważnienie do przetwarzania” i „Cofnięcie upoważnienia” są sporządzane elektronicznie w systemie EZD zgodnie ze wzorami określonymi w załącznikach nr 1 i 2 do Polityki, dla każdej osoby wyznaczonej do przetwarzania danych osobowych w zbiorze, bez określenia czasu ważności upoważnienia (aktualne szablony formularzy w systemie Mdok: Dane osobowe_Upoważnienie do przetwarzania oraz Dane osobowe_Cofnięcie upoważnienia).
4. W przypadku niedostępności systemu EZD, w sytuacji konieczności nadania lub cofnięcia upoważnienia, mogą być stosowane papierowe postaci formularzy "Upoważnienie do przetwarzania" i "Cofnięcie upoważnienia", które niezwłocznie po uruchomieniu systemu, muszą zostać odwzorowane cyfrowo i w postaci elektronicznej dołączone do akt sprawy. Postać papierową dokumentów przechowuje się w sposób przyjęty w Urzędzie Miasta Lublin dla dokumentów wewnętrznych odwzorowanych cyfrowo.

§ 3

1. Zarządzający zbiorem, chcąc uzyskać dla pracownika sobie podległego upoważnienie do przetwarzania w zbiorze danych, którym sam zarządza, przydziela mu jedną z czynności takich jak: przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych i określa jego uprawnienia w systemie informatycznym.
2. Zarządzający zbiorem wypełnia elektronicznie w systemie EZD część „A” formularza „Upoważnienie do przetwarzania”, podając następujące dane:
   1) wnioskujący;
   2) imię i nazwisko osoby wyznaczonej do przetwarzania danych, symbol stanowiska ze struktury organizacyjnej;
   3) nazwa zbioru danych osobowych (nazwa zbioru zgodna z wnioskiem zgłoszeniowym do GIODO);
   4) obszar przetwarzania danych osobowych (nazwa ulicy i nr budynku i lokalu);
   5) czynności w zbiorze danych (przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych);
   6) uprawnienia w systemie informatycznym, konkretne czynności charakterystyczne dla danego systemu informatycznego lub czynności zdefiniowane w systemie dla konkretnego stanowiska pracy (w przypadku zbiorów prowadzonych na nośniku papierowym, podaje dane od pkt 1 do pkt 5).
3. Zarządzający zbiorem podpisuje elektronicznie w systemie EZD formularz „Upoważnienie do przetwarzania” w części „A” w polach:
   1) „Podpis wnioskującego” - operacją podpisu „Podpisz”;
   2) „Podpis zarządzającego zbiorem” - operacją podpisu „Akceptuj”;

   i przekazuje go elektronicznie administratorowi systemu funkcją „przekaż dalej” bez zaznaczania opcji „do wglądu” (w przypadku zbiorów prowadzonych na nośniku papierowym przekazuje administratorowi bezpieczeństwa informacji).
4. Administrator systemu, po sprawdzeniu podpisu zarządzającego zbiorem,

generuje w systemie informatycznym konto dla nowego użytkownika, wypełnia elektronicznie w systemie EZD część „B" formularza „Upoważnienie do przetwarzania", wpisując identyfikator (ewentualnie nazwę aplikacji).
5. Administrator systemu podpisuje elektronicznie w systemie EZD w części „B" w polu oznaczonym „Podpis administratora systemu" formularz „Upoważnienie do przetwarzania" i przekazuje go elektronicznie administratorowi bezpieczeństwa informacji funkcją „przekaż dalej" bez zaznaczania opcji „do wglądu".
6. Administrator bezpieczeństwa informacji wypełnia elektronicznie w systemie EZD część „C" formularza „Upoważnienie do przetwarzania" wpisując kolejny nr upoważnienia z ewidencji osób upoważnionych, imię i nazwisko osoby oraz nazwę zbioru danych osobowych.
7. Administrator bezpieczeństwa informacji podpisuje elektronicznie w systemie EZD w części „C" w polu oznaczonym „Podpis administratora bezpieczeństwa informacji" formularz „Upoważnienie do przetwarzania", a następnie przekazuje elektronicznie formularz funkcją „odpowiedz" administratorowi systemu (w przypadku zbiorów prowadzonych na nośniku papierowym – przekazuje zarządzającemu zbiorem).
8. Administrator systemu, po sprawdzeniu podpisu administratora bezpieczeństwa informacji, przekazuje elektronicznie w systemie EZD funkcją „przekaż dalej" z zaznaczeniem opcji „do wglądu" formularz „Upoważnienie do przetwarzania" osobie upoważnionej oraz udostępnia jej identyfikator i hasło.
9. Osoba upoważniona podpisuje elektronicznie w systemie EZD w części „D" w polu oznaczonym „Podpis osoby upoważnionej" formularz „Upoważnienie do przetwarzania", potwierdzając tym samym, że:
   1) zapoznała się przed przystąpieniem do przetwarzania z zarządzeniem oraz ustawą i rozporządzeniem do niej;
   2) zobowiązuje się do przetwarzania danych osobowych wyłącznie w zakresie upoważnienia i nadanych uprawnień;
   3) zachowa w tajemnicy treści danych osobowych oraz informacje o sposobach ich zabezpieczenia.

§ 4

1. Wnioskujący, będący kierownikiem komórki organizacyjnej lub zatrudniony na stanowisku pracy w departamencie, chcąc uzyskać dla pracownika sobie podległego upoważnienie do przetwarzania danych osobowych, w zbiorze danych, którym sam nie zarządza, uzgadnia z zarządzającym zbiorem możliwe do zaakceptowania przez zarządzającego czynności w zbiorze, takie jak: przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych i możliwe do zaakceptowania uprawnienia w systemie informatycznym.
2. Wnioskujący, o którym mowa w ust. 1, wypełnia elektronicznie w systemie EZD część „A" formularza „Upoważnienie do przetwarzania", podając następujące dane:
   1) wnioskujący;
   2) imię i nazwisko osoby wyznaczonej do przetwarzania danych, symbol stanowiska ze struktury organizacyjnej;
   3) nazwa zbioru danych osobowych (nazwa zbioru zgodna z wnioskiem

zgłoszeniowym do GIODO);
4) obszar przetwarzania danych osobowych (nazwa ulicy i nr budynku);
5) czynności w zbiorze danych (przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych);
6) uprawnienia w systemie informatycznym, konkretne czynności charakterystyczne dla danego systemu informatycznego lub czynności zdefiniowane w systemie dla konkretnego stanowiska pracy (w przypadku zbiorów prowadzonych na nośniku papierowym, podaje dane od pkt 1 do pkt 5).

3. Wnioskujący podpisuje elektronicznie w systemie EZD formularz „Upoważnienie do przetwarzania" w części „A" w polu „Podpis wnioskującego" - operacją podpisu „Podpisz" i przekazuje go elektronicznie do zarządzającego zbiorem, funkcją „przekaż dalej" bez zaznaczania opcji „do wglądu". Zarządzający zbiorem, administrator systemu, administrator bezpieczeństwa informacji oraz osoba upoważniona stosują odpowiednio § 3 ust. 3 pkt 2 do ust. 9.
4. Zarządzający zbiorem, może odmówić wnioskującemu, będącemu kierownikiem komórki organizacyjnej lub zatrudnionemu na stanowisku pracy w departamencie przyznania uprawnień do przetwarzania danych osobowych w zbiorze jeżeli:
1) system informatyczny służący do przetwarzania danych osobowych w zbiorze nie posiada możliwości zwiększenia liczby użytkowników;
2) analiza ryzyka przetwarzania danych osobowych przez osoby wyznaczone do przetwarzania nie daje gwarancji zabezpieczenia danych.

§ 5

1. Wnioskujący, będący kierownikiem jednostki organizacyjnej Miasta Lublin, chcąc uzyskać dla pracownika sobie podległego upoważnienie do przetwarzania danych osobowych, w zbiorze danych, którym sam nie zarządza, uzgadnia z zarządzającym zbiorem możliwe do zaakceptowania przez zarządzającego czynności w zbiorze, takie jak: przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych i możliwe do zaakceptowania uprawnienia w systemie informatycznym.
2. Wnioskujący, o którym mowa w ust. 1, przesyła zarządzającemu zbiorem dane określone w § 3 ust. 2 jednym z podanych niżej sposobów:
1) elektronicznie:
a) jeżeli posiada podpis kwalifikowany:
- elektroniczną platformą usług administracyjnych ePUAP,
- pocztą elektroniczną,
b) jeżeli posiada profil zaufany na ePUAP i jest upoważniony do reprezentowania podmiotu, w imieniu którego działa - platformą usług administracyjnych ePUAP;
2) w postaci papierowej z podpisem odręcznym. Punkt podawczy Urzędu Miasta Lublin rejestruje w systemie EZD wniosek w postaci papierowej, jako dokument przychodzący z pełnym odwzorowaniem cyfrowym, a jego postać papierową odkłada do właściwego składu chronologicznego. Zarządzający zbiorem włącza do akt sprawy postać elektroniczną formularza.
3. Zarządzający zbiorem, po otrzymaniu wniosku, w oparciu o otrzymane dane, wypełnia elektronicznie w systemie EZD część „A" formularza „Upoważnienie

do przetwarzania", zgodnie z § 3 ust. 2. Zarządzający zbiorem, administrator systemu, administrator bezpieczeństwa informacji stosują odpowiednio § 3 ust. 3 pkt 2 do ust. 7.

4. Administrator systemu, po sprawdzeniu w systemie EZD podpisu administratora bezpieczeństwa informacji drukuje formularz „Upoważnienie do przetwarzania", potwierdza zgodność kopii w postaci papierowej z dokumentem elektronicznym w częściach A – C.
5. Osoba upoważniona składa odręczny podpis na kopii upoważnienia w części „D", potwierdzając tym samym, że:
   1) zapoznała się przed przystąpieniem do przetwarzania z zarządzeniem oraz ustawą i rozporządzeniem do niej;
   2) zobowiązuje się do przetwarzania danych osobowych wyłącznie w zakresie upoważnienia i nadanych uprawnień;
   3) zachowa w tajemnicy treści danych osobowych oraz informacje o sposobach ich zabezpieczenia.
6. Administrator systemu wydaje osobie upoważnionej identyfikator i hasło, wykonuje odwzorowanie cyfrowe wydrukowanego formularza z podpisem osoby upoważnionej, które dodaje jako załącznik do formularza już istniejącego w systemie EZD, funkcją „dodaj załącznik". Postać papierową upoważnienia wydaje osobie upoważnionej.
7. Zarządzający zbiorem może odmówić wnioskującemu, będącemu kierownikiem jednostki organizacyjnej Miasta Lublin, przyznania uprawnień do przetwarzania danych osobowych w zbiorze jeżeli:
   1) system informatyczny służący do przetwarzania danych osobowych w zbiorze nie posiada możliwości zwiększenia liczby użytkowników;
   2) analiza ryzyka przetwarzania danych osobowych przez osoby wyznaczone do przetwarzania nie daje gwarancji zabezpieczenia danych.

§ 6

1. Zarządzający zbiorem, chcąc cofnąć upoważnienie do przetwarzania dla pracownika sobie podległego, w zbiorze danych, którym sam zarządza, wypełnia elektronicznie w systemie EZD w części „A" formularz „Cofnięcie upoważnienia".
2. Zarządzający zbiorem podpisuje elektronicznie w systemie EZD w części „A" w polu oznaczonym „Podpis zarządzającego zbiorem" formularz „Cofnięcie upoważnienia" i przekazuje go elektronicznie do administratora systemu funkcją „przekaż dalej" bez zaznaczania opcji „do wglądu" (w przypadku zbiorów prowadzonych na nośniku papierowym, przesyła administratorowi bezpieczeństwa informacji).
3. Administrator systemu odbiera osobie upoważnionej uprawnienia w systemie oraz podpisuje elektronicznie w systemie EZD w części „B" w polu oznaczonym „Podpis administratora systemu" formularz „Cofnięcie upoważnienia",a następnie przekazuje go elektronicznie do administratora bezpieczeństwa informacji funkcją „przekaż dalej" bez zaznaczania opcji „do wglądu".
4. Administrator bezpieczeństwa informacji wypełnia elektronicznie w systemie EZD formularz „Cofnięcie upoważnienia" w części „C", podpisuje w polu oznaczonym „Podpis administratora bezpieczeństwa informacji", odnotowuje ten fakt w ewidencji a następnie przekazuje elektronicznie formularz funkcją „przekaż

dalej” z zaznaczeniem opcji „do wglądu” zarządzającemu zbiorem.

§ 7

1. Wnioskujący, będący kierownikiem komórki organizacyjnej lub zatrudniony na stanowisku pracy w departamencie, chcąc cofnąć dla pracownika sobie podległego upoważnienie do przetwarzania w zbiorze danych, którym sam nie zarządza, wypełnia elektronicznie w systemie EZD w części „A” formularz „Cofnięcie upoważnienia”.
2. Wnioskujący podpisuje elektronicznie w systemie EZD formularz „Cofnięcie upoważnienia” funkcją „podpisz” z menu „operacje” i przekazuje elektronicznie formularz do zarządzającego zbiorem funkcją „przekaż dalej”, bez zaznaczania opcji „do wglądu”. Zarządzający zbiorem, administrator systemu i administrator bezpieczeństwa informacji stosują odpowiednio zapisy § 6 ust. 2 do ust. 4.

§ 8

1. Wnioskujący, będący kierownikiem jednostki organizacyjnej Miasta Lublin, chcąc uzyskać dla pracownika sobie podległego cofnięcie upoważnienia do przetwarzania danych osobowych w zbiorze danych, którym sam nie zarządza, przesyła zarządzającemu zbiorem dane określone w części „A” w załączniku nr 2 do Polityki, w trybie wskazanym w § 5 ust. 2.
2. Zarządzający zbiorem, po otrzymaniu wniosku wypełnia elektronicznie w systemie EZD w części „A” formularz „Cofnięcie upoważnienia”. Zarządzający zbiorem, administrator systemu, administrator bezpieczeństwa informacji stosują odpowiednio zapisy § 6 ust. 2 do ust. 4.

§ 9

1. Zarządzający zbiorem wnioskuje o cofnięcie upoważnienia do zbioru po uzyskaniu informacji o tym, że osoba upoważniona:
   1) działa na szkodę administratora danych;
   2) nie zachowuje w tajemnicy hasła, treści danych osobowych oraz informacji o sposobach ich zabezpieczenia;
   3) zmieniła komórkę organizacyjną lub stanowisko pracy w departamencie lub jednostkę organizacyjną Miasta Lublin, zakończyła zatrudnienie, pracę, staż, praktykę lub inny stosunek prawny;
   4) zmieniła imię i nazwisko;
   5) zmieniła, decyzją przełożonego, czynności w zbiorze danych (przeglądanie danych lub modyfikowanie danych, lub administrowanie systemem, lub administrowanie serwerem, bazą danych);
   6) zmieniła, decyzją przełożonego, uprawnienia w systemie, konkretne czynności charakterystyczne dla danego systemu informatycznego lub zdefiniowane w systemie dla konkretnego stanowiska pracy;
   7) zaprzestała, decyzją przełożonego, przetwarzania w zbiorze danych.
2. Informacje o zdarzeniach wymienionych w § 9 ust. 1 pkt 3 – 7, dotyczące podległych pracowników, wnioskujący jest zobowiązany każdorazowo przekazać zarządzającemu zbiorem wypełniając formularze „Cofnięcie upoważnienia”.
3. Wnioskujący oraz administrator systemu po powzięciu informacji o ryzyku dalszego przetwarzania danych osobowych przez osobę upoważnioną,

wymienionym w § 9 ust. 1 pkt 1 – 2, natychmiast powiadamia o tym zarządzającego zbiorem.

4. Zarządzający zbiorem po uzyskaniu informacji o ryzyku dalszego przetwarzania danych osobowych przez osobę upoważnioną, zleca telefonicznie oraz drogą elektroniczną administratorowi systemu, natychmiastowe odebranie w systemie informatycznym uprawnień tej osobie do czasu przeprowadzenia postępowania wyjaśniającego przez administratora bezpieczeństwa informacji (w przypadku zbiorów prowadzonych tylko na nośniku papierowym, czynności pozbawienia dostępu do zbioru danych osobowych wykonuje zarządzający zbiorem). Zarządzający zbiorem lub wnioskujący przygotowuje wniosek o cofnięcie upoważnień, stosując odpowiednio § 6 lub § 7, lub § 8.

Rozdział III
Organizacja pozostałych czynności związanych z zabezpieczeniem przetwarzania danych osobowych

§ 10

1. Administrator bezpieczeństwa informacji :
   1) sporządza elektronicznie i aktualizuje wykaz zbiorów danych osobowych, zgodnie ze wzorem określonym w załączniku nr 3 do Polityki;
   2) sporządza elektronicznie i aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie ze wzorem określonym w załączniku nr 4 do Polityki;
   3) sporządza elektronicznie i aktualizuje wykaz budynków tworzących obszary przetwarzania danych osobowych, zgodnie ze wzorem określonym w załączniku nr 5 do Polityki;
   4) sporządza elektronicznie i aktualizuje opis struktury zbioru danych osobowych, zgodnie ze wzorem określonym w załączniku nr 6 do Polityki;
   5) sporządza elektronicznie i aktualizuje opis przepływu danych osobowych, zgodnie ze wzorem określonym w załączniku nr 7 do Polityki.
2. Zarządzający zbiorem we współpracy z administratorem bezpieczeństwa informacji oraz administratorem systemu:
   1) rejestruje zbiór danych osobowych w rejestrze GIODO, wysyłając za pomocą platformy elektronicznej e-Giodo, wypełniony i podpisany wspólnie z administratorem danych wniosek zgłoszeniowy (zgodnie z art. 41 oraz art. 46 ustawy, chyba że administrator danych jest zwolniony z obowiązku rejestracji zbioru zgodnie z art. 43 ustawy);
   2) aktualizuje wniosek zgłoszeniowy w terminie do 30 dni od dokonania zmian w zbiorze danych osobowych, stosując przepisy art. 41 ustawy;
   3) wyrejestrowuje zbiór danych osobowych stosując przepisy art. 44a ustawy.
3. Zarządzający zbiorem dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, stosując zapisy art. 26 ustawy, a w szczególności zapewnia aby dane te były:
   1) przetwarzane zgodnie z art. 23 – 31a ustawy odnośnie zasad przetwarzania danych;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane

dalszemu przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów przetwarzania;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to niezbędne do osiągnięcia celu przetwarzania;
5) przekazywane do państwa trzeciego, zgodnie z art. 47 – 48 ustawy.

Rozdział IV
Powierzenie przetwarzania danych osobowych innemu podmiotowi

§ 11

1. Powierzenie przetwarzania następuje w formie umowy na piśmie zawartej pomiędzy Gminą Lublin a podmiotem zewnętrznym. Umowa powierzenia, musi mieć jasno sprecyzowany cel i zakres przetwarzania oraz określać sposób postępowania z danymi lub dostępem do nich po zakończeniu umowy.
2. Przykładowe zapisy umowy o powierzenie przetwarzania danych osobowych znajdują się w załączniku nr 8 do Polityki.
3. Zapisy umowy o powierzenie przetwarzania mogą stanowić część innych umów zawartych z podmiotem zewnętrznym.

Rozdział V
Ochrona danych osobowych i obszaru przetwarzania

§ 12

1. Osobę upoważnioną obowiązuje na stanowisku pracy zasada „czystego biurka”, czyli nie pozostawianie żadnych dokumentów z danymi osobowymi podczas nieobecności.
2. Osobę upoważnioną obowiązuje na stanowisku pracy zasada „czystego ekranu”, czyli blokowanie stacji roboczej (w systemie Windows kombinacja klawiszy Windows + L) podczas nieobecności.
3. Zakończenie pracy na stacji roboczej wymaga wylogowania się z systemu i wyłączenia komputera.
4. Dokumenty zawierające dane osobowe niszczy się w sposób uniemożliwiający ich odczytanie.

§ 13

1. Dane osobowe są przetwarzane w pomieszczeniach lub częściach pomieszczeń, do których dostęp mają osoby upoważnione.
2. Interesanci mogą przebywać w tych pomieszczeniach wyłącznie w obecności osób upoważnionych.
3. Administrator budynku oraz osoby utrzymujące czystość pomieszczeń mogą przebywać w obszarze przetwarzania danych osobowych w celu wykonania obowiązków służbowych bez możliwości dostępu do danych.
4. Klucze do pomieszczeń, w których przetwarza się dane osobowe, są wydawane osobom upoważnionym po odnotowaniu w książce ewidencji wydawania kluczy.
5. Stanowiska pracy mają tak zlokalizowane urządzenia informatyczne, służące do

przetwarzania danych osobowych, żeby osoby nieupoważnione nie mogły widzieć treści wyświetlanych na ekranach monitorów komputerowych.

§ 14

1. Dostęp do pomieszczeń w których pracują serwery mają: dyrektor IT, administrator systemu, administrator serwera, bazy danych i administrator bezpieczeństwa informacji oraz upoważnieni pracownicy Wydziału Informatyki i Telekomunikacji.
2. Pomieszczenia, w których pracują serwery, są zabezpieczone przynajmniej drzwiami wyposażonymi w zamek patentowy oraz dodatkowo kratami w oknach, jeżeli pomieszczenia te są zlokalizowane w piwnicy, na parterze, pierwszym lub ostatnim piętrze budynku.
3. Systemy informatyczne posiadają zasilacze awaryjne, pozwalające poprawnie zapisać dane osobowe i bezpiecznie wyłączyć system.

Rozdział VI
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

§ 15

1. Administrator bezpieczeństwa informacji jest obowiązany poinformować na piśmie administratora danych o przypadkach naruszenia zasad niniejszego Zarządzenia przez osobę upoważnioną, administratora systemu, administratora serwera, bazy danych lub zarządzającego zbiorem, a zwłaszcza o:
   1) przetwarzaniu bez upoważnienia do przetwarzania;
   2) przetwarzaniu niezgodnie z zakresem upoważnienia;
   3) niedopełnieniu obowiązku zgłoszenia zbioru danych do rejestru GIODO;
   4) złamaniu tajemnicy danych i sposobów ich zabezpieczenia.
2. Osoba upoważniona jest obowiązana powiadomić administratora systemu i zarządzającego zbiorem a ten powiadamia administratora bezpieczeństwa informacji o naruszeniu bezpieczeństwa systemów informatycznych a szczególnie o:
   1) możliwości przetwarzania danych osobowych bez wprowadzenia hasła;
   2) dostępie do danych w szerszym lub węższym zakresie niż przyznany;
   3) podejrzeniu nieautoryzowanej modyfikacji danych;
   4) utraty tajności kluczy kryptograficznych;
   5) zgubieniu lub kradzieży nośnika z danymi lub dokumentów zawierających dane;
   6) podejrzeniu kradzieży sprzętu informatycznego;
   7) zauważeniu śladów włamania do szaf lub pomieszczeń w obszarze przetwarzania;
   8) zauważeniu innych niepokojących faktów.
3. Administrator systemu podejmuje działania zmierzające do ochrony systemu informatycznego przed dalszym naruszeniem.
4. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia o naruszeniu bezpieczeństwa przetwarzania danych osobowych, przeprowadza

postępowanie wyjaśniające, mające na celu ustalenie okoliczności zaistniałego zdarzenia oraz sporządza raport z naruszenia bezpieczeństwa przetwarzania danych osobowych zgodnie ze wzorem określonym w załączniku nr 9 do Polityki.

Rozdział VII
Nadzór przestrzegania zasad ochrony danych osobowych

§ 16

1. Administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony danych osobowych opracowując w tym zakresie sprawozdanie z nadzoru przestrzegania zasad ochrony danych osobowych, które sporządza się zgodnie ze wzorem określonym w załączniku nr 10 do Polityki .
2. Administrator bezpieczeństwa informacji, ma prawo:
   1) wstępu do wszystkich pomieszczeń;
   2) asystowania przy wszystkich czynnościach związanych z przetwarzaniem danych osobowych;
   3) wglądu do dokumentów zawierających dane osobowe;
   4) wglądu do systemu informatycznego służącego do przetwarzania danych osobowych;
   5) żądać od osób upoważnionych ustnych i pisemnych wyjaśnień;
   6) unieważnić upoważnienie do przetwarzania danych osobowych osobie upoważnionej, jeżeli rażąco naruszyła przestrzeganie zasad ochrony danych osobowych.
3. Osoby upoważnione, wnioskujący o wydanie lub cofnięcie upoważnienia oraz zarządzający zbiorami są obowiązani do udzielenia w czasie nadzoru przestrzegania zasad ochrony danych osobowych wszelkich informacji administratorowi bezpieczeństwa informacji.

Rozdzielnik:
1. Oryginał: Wydział Organizacji Urzędu.
2. Kopia użytkowa: www.bip.lublin.eu, intranet.