Zarządzenie nr 439/2008
Prezydenta Miasta Lublin
z dnia 30 czerwca 2008 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miasta Lublin

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) oraz art. 3 ust. 1, art. 7 pkt 4 i art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) w związku z § 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. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Urzędzie, zarówno manualnie, np. w wykazach, kartotekach, zbiorach ewidencyjnych, jak i za pomocą systemów informatycznych, wprowadzam:

1) politykę bezpieczeństwa danych osobowych, stanowiącą załącznik nr 1 do niniejszego Zarządzenia;
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do niniejszego Zarządzenia.

§ 2

Ilekroć w Zarządzeniu jest mowa o:

1) administratorze danych – rozumie się przez to Prezydenta Miasta;
2) zarządzającym danymi – rozumie się przez to osobę kierującą wydziałem, biurem, Kancelarią Prezydenta, Urzędem Stanu Cywilnego oraz samodzielnym stanowiskiem pracy;
3) dyrektorze IT – rozumie się przez to dyrektora Wydziału Informatyki i Telekomunikacji;
4) administratorze systemu – rozumie się przez to pracownika wyznaczonego przez dyrektora IT lub w uzasadnionych względami organizacyjnymi sytuacjach, przez zarządzającego danymi, do zarządzania systemem lub systemami informatycznymi, który w zakresie zarządzania systemami informatycznymi stosuje się do poleceń dyrektora IT;
5) administratorze bezpieczeństwa informacji – rozumie się przez to osobę

wyznaczoną do kontroli stanu bezpieczeństwa danych osobowych i przestrzegania zasad ochrony danych osobowych;

6) pracowniku upoważnionym – rozumie się przez to pracownika, praktykanta, stażystę lub inną osobę, zobowiązaną do zachowania w tajemnicy danych osobowych, do których miała dostęp oraz sposobów ich zabezpieczenia, upoważnioną na piśmie przez administratora danych do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło, jeżeli to przetwarzanie ma miejsce w systemie informatycznym;
7) przetwarzaniu – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych przez pracowników upoważnionych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza wykonywane w systemach informatycznych;
8) przekazaniu danych osobowych – rozumie się przez to przekazanie danych pomiędzy wydziałami, biurami, Kancelarią Prezydenta, Urzędem Stanu Cywilnego oraz samodzielnymi stanowiskami pracy;
9) udostępnianiu danych osobowych – rozumie się przez to udostępnie danych innemu administratorowi danych, który decyduje o celach i środkach przetwarzania danych;
10) powierzeniu przetwarzania danych osobowych – rozumie się przez to wykonywanie przez podmiot zewnętrzny jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza tych, które wykonuje się w systemach informatycznych;
11) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych i innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
12) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych i innych, znany jedynie osobie upoważnionej do dostępu do systemu informatycznego przetwarzającego dane osobowe;
13) mechanizmach kryptograficznych – rozumie się przez to mechanizmy szyfrowania danych;
14) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

§ 3

Traci moc Zarządzenie Wewnętrzne Nr 488/2000 Prezydenta Miasta Lublina z dnia 29 grudnia 2000 roku w sprawie wykonywania czynności kancelaryjnych, postępowania w sytuacjach naruszenia ochrony danych osobowych oraz zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w jednostkach organizacyjnych Urzędu Miejskiego.

§ 4

Wykonanie Zarządzenia powierzam administratorowi bezpieczeństwa informacji.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

z up. PREZYDENTA LUBLINA

prof. nadzw. dr hab. inż. Stanisław Fic
Zastępca Prezydenta

Polityka bezpieczeństwa danych osobowych Urzędu Miasta Lublin

Rozdział 1
Wykazy i opisy wymagane w procesie przetwarzania danych osobowych

§ 1

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszary, w których przetwarzane są dane osobowe sporządza się zgodnie ze wzorem określonym w załączniku nr 3 do niniejszego Zarządzenia.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych sporządza się zgodnie ze wzorem określonym w załączniku nr 4 do niniejszego Zarządzenia.
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi sporządza się zgodnie ze wzorem określonym w załączniku nr 5 do niniejszego Zarządzenia.
4. Opis przepływu danych pomiędzy poszczególnymi systemami sporządza się zgodnie ze wzorem określonym w załączniku nr 6 do niniejszego Zarządzenia.
5. Wykaz osób upoważnionych do przetwarzania danych osobowych sporządza się zgodnie ze wzorem określonym w załączniku nr 7 do niniejszego Zarządzenia.
6. Upoważnienie do przetwarzania danych osobowych sporządza się zgodnie ze wzorem określonym w załączniku nr 8 do niniejszego Zarządzenia.

Rozdział 2
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

§ 2

1. Dokumenty zawierające wydruki danych osobowych po zakończeniu przetwarzania lub pracy przechowywane są w szafach zamykanych na klucze, przechowywane w ustalonym przez zarządzającego danymi miejscu, do którego dostęp mają jedynie pracownicy upoważnieni.
2. Robocze wydruki z systemu komputerowego zawierające dane osobowe pracownicy upoważnieni niszczą w niszczarce przed zakończeniem pracy.
3. Dokumenty zawierające wydruki danych osobowych transportuje się w zaklejonych kopertach chroniących przed uszkodzeniem lub zniszczeniem.

§ 3

1. Dane osobowe są przetwarzane w pomieszczeniach lub częściach

pomieszczeń, do których dostęp mają pracownicy upoważnieni lub posiadający zgodę zarządzającego danymi na przebywanie w obecności osoby upoważnionej i tylko na czas związany z pełnieniem obowiązków służbowych.
2. Interesanci i osoby postronne mogą przebywać w tych pomieszczeniach jedynie w miejscach dla nich przeznaczonych.
3. Administrator budynku, goniec oraz osoby utrzymujące czystość mogą przebywać w obszarze przetwarzania danych osobowych bez prawa dostępu do danych.
4. Klucze do pomieszczeń, w których przetwarza się dane osobowe są wydawane pracownikom upoważnionym na portierni po odnotowaniu w książce pobrań kluczy i tam przechowywane po zakończonej pracy.
5. Pomieszczenia obszaru przetwarzania są wyposażone w instrukcję bhp przy obsłudze sprzętu komputerowego.
6. Stanowiska pracy mają tak zlokalizowane urządzenia informatyczne służące do przetwarzania danych osobowych, żeby:
   1) osoby nieupoważnione nie mogły widzieć zawartości ekranów monitorów komputerowych;
   2) nie pozostawały w zasięgu osób nieupoważnionych.

§ 4

1. Dostęp do pomieszczeń, w których pracują serwery mają: zarządzający danymi, dyrektor IT, administrator systemu i administrator bezpieczeństwa informacji oraz pracownicy upoważnieni wydziału informatyki.
2. Pomieszczenia, w których pracują serwery są zabezpieczone drzwiami antywłamaniowymi oraz dodatkowo kratami w oknach, jeżeli pomieszczenia te są zlokalizowane w piwnicy, na parterze, pierwszym lub ostatnim piętrze budynku.
3. Okablowanie sieciowe musi być zaprojektowane w sposób umożliwiający dostęp do linii transmisyjnych jedynie w pomieszczeniach zamykanych na klucz.
4. Systemy informatyczne posiadają zasilacze awaryjne, pozwalające poprawnie zapisać dane osobowe i bezpiecznie wyłączyć system.

Rozdział 3
Organizacja przetwarzania danych osobowych

§ 5

Administrator danych:
1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych;
2) decyduje o udostępnieniu danych osobowych podmiotom zewnętrznym po konsultacji z zarządzającym danymi;
3) decyduje o powierzeniu przetwarzania danych osobowych innym podmiotom po konsultacji z zarządzającym danymi;
4) zatwierdza podpisem wymaganą prawem dokumentację prowadzoną przez administratora bezpieczeństwa informacji;
5) decyduje o działaniach dyscyplinujących, podejmowanych w przypadku

naruszenia procedur przetwarzania danych osobowych;
6) akceptuje roczny plan kontroli, sprawozdanie z jego wykonania i podejmuje decyzje o kontrolach doraźnych;
7) wyznacza administratora bezpieczeństwa informacji.

§ 6

Pracownicy upoważnieni do przetwarzania danych osobowych:
1) zapewniają ochronę danych osobowych przed:
   a) udostępnieniem osobom nieupoważnionym;
   b) zabraniem przez osobę nieuprawnioną;
   c) przetwarzaniem z naruszeniem ustawy;
   d) zmianą;
   e) utratą;
   f) uszkodzeniem;
   g) zniszczeniem;
2) przetwarzają dane osobowe wyłącznie w zakresie upoważnienia do przetwarzania danych osobowych i tylko w celu wykonania obowiązków służbowych nałożonych przez zarządzającego danymi;
3) zobowiązują się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie, jak i po zakończeniu pracy, praktyki lub stażu oraz odwołaniu upoważnienia lub upływie jego ważności, podpisując upoważnienie do przetwarzania danych osobowych;
4) organizują stanowiska pracy tak aby osoby nieupoważnione nie miały dostępu do danych osobowych;
5) używają własnego, unikalnego identyfikatora i hasła do zalogowania się w systemie, zapewniającego im w sposób jednoznaczny przypisanie wykonanych czynności;
6) chronią hasło do systemu informatycznego przetwarzającego dane osobowe przed ujawnieniem innym osobom;
7) powiadamiają zarządzającego danymi o naruszeniu bezpieczeństwa przetwarzania danych osobowych.

§ 7

Zarządzający danymi:
1) zapewniają przetwarzanie danych osobowych zgodnie z celami i środkami przetwarzania danych określonymi przez administratora danych;
2) zapewniają poprawność merytoryczną danych osobowych gromadzonych w zbiorach danych;
3) decydują o poziomach bezpieczeństwa przetwarzania danych osobowych zgodnie z rozporządzeniem;
4) stwarzają warunki organizacyjne i techniczne umożliwiające spełnienie obowiązujących wymogów prawnych w zakresie ochrony danych osobowych;
5) określają, którzy pracownicy i w jakim zakresie mogą przetwarzać dane osobowe;
6) występują na piśmie do administratora danych o upoważnienie pracowników do przetwarzania danych osobowych, załączając wypełnione

upoważnienia;
7) powiadamiają administratora bezpieczeństwa informacji o zmianach w: obszarach przetwarzania, wykazie zbiorów danych osobowych, wykazie osób upoważnionych do przetwarzania;
8) wydają zgodę na przebywanie w obszarze przetwarzania w celach służbowych w obecności pracowników upoważnionych do przetwarzania danych osobowych, osobom nieposiadającym takich upoważnień;
9) powiadamiają administratora bezpieczeństwa informacji lub administratora systemu o naruszeniu bezpieczeństwa przetwarzania danych osobowych;
10) sporządzają wnioski rejestracyjne i aktualizacyjne do Generalnego Inspektora Ochrony Danych Osobowych;
11) decydują o przekazaniu danych osobowych;
12) udostępniają dane osobowe innym podmiotom po otrzymaniu zgody administratora danych;
13) powierzają dane osobowe do przetwarzania innym podmiotom po otrzymaniu zgody administratora danych.

§ 8

Administrator systemu informatycznego:
1) zarządza systemem lub systemami informatycznymi w sposób zapewniający bezpieczeństwo i ciągłość działania systemu;
2) instaluje i konfiguruje sprzęt sieciowy i oprogramowanie systemowe;
3) tworzy i likwiduje kopie zapasowe danych osobowych i systemów informatycznych, w których są przetwarzane;
4) nadaje identyfikator wraz z hasłem oraz uprawnienia do przetwarzania danych osobowych a także modyfikuje te uprawnienia na wniosek zarządzającego danymi lub administratora bezpieczeństwa informacji;
5) nadzoruje działanie mechanizmów uwierzytelniania osób upoważnionych do przetwarzania danych osobowych w systemie oraz działanie mechanizmów kontroli dostępu do systemu informatycznego;
6) wyrejestrowuje osoby upoważnione do przetwarzania danych osobowych w sytuacji naruszenia bezpieczeństwa ich przetwarzania na wniosek zarządzającego danymi lub administratora bezpieczeństwa informacji;
7) informuje zarządzającego danymi oraz administratora bezpieczeństwa informacji o naruszeniu bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym i przechowuje dokumentację tego typu zdarzeń w oparciu o logi systemowe;
8) zapewnia ochronę systemów przetwarzających dane osobowe przez stosowanie zapór sieciowych i decyduje za zgodą dyrektora IT o ich wyborze;
9) zapewnia ochronę systemów informatycznych przed działaniem złośliwego oprogramowania, decydując za zgodą dyrektora IT o wyborze programów antywirusowych;
10) zapewnia bezpieczne zwiększenie ilości stacji roboczych systemu;
11) zapewnia wyposażenie systemów informatycznych przesyłających dane osobowe do sieci publicznej w mechanizmy kryptograficzne i decyduje za zgodą dyrektora IT o ich wyborze;
12) zapewnia bezpieczne przekazywanie lub udostępnianie danych

osobowych stosując metody kryptograficzne;
13) zabezpiecza system informatyczny po powzięciu wiadomości o naruszeniu bezpieczeństwa danych osobowych;
14) dokonuje przeglądów i napraw systemów informatycznych oraz urządzeń komputerowych, na których zapisane są dane osobowe oraz usuwa dane osobowe z tych elementów systemów informatycznych, które są przekazywane do naprawy innym podmiotom;
15) nadzoruje współpracę z dostawcami usług informatycznych;
16) powiadamia administratora bezpieczeństwa informacji o zmianach w strukturze zbioru danych oraz w sposobie przepływu danych pomiędzy poszczególnymi systemami;
17) podejmuje działania służące zapewnieniu ciągłości zasilania urządzeń przetwarzających dane osobowe.

§ 9

Administrator bezpieczeństwa informacji:

1) sprawuje nadzór nad stosowaniem, opisanych w ustawie o ochronie danych osobowych, rozporządzeniu do ustawy oraz w polityce bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, środków organizacyjnych, technicznych oraz fizycznych, zapewniających bezpieczne przetwarzanie danych osobowych;
2) weryfikuje pod względem zgodności z przepisami prawnymi politykę bezpieczeństwa i instrukcję;
3) prowadzi oraz przechowuje wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe administratora danych;
4) prowadzi oraz przechowuje wykaz zbiorów danych osobowych administratora danych ze wskazaniem programów zastosowanych do przetwarzania tych danych;
5) prowadzi oraz przechowuje opis struktury zbiorów danych osobowych administratora danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
6) prowadzi oraz przechowuje opis przepływu danych osobowych pomiędzy poszczególnymi systemami administratora danych;
7) prowadzi oraz przechowuje wykaz osób upoważnionych przez administratora danych do przetwarzania danych osobowych;
8) ewidencjonuje sposoby udostępniania danych osobowych odbiorcom danych i innym podmiotom;
9) nadzoruje przygotowywanie wniosków rejestracyjnych i aktualizacyjnych przez zarządzających danymi oraz prowadzi w tej sprawie korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych;
10) przedstawia administratorowi danych raport z przebiegu dochodzenia w sprawie naruszenia bezpieczeństwa przetwarzania danych osobowych;
11) przedstawia do akceptacji roczny plan kontroli i proponuje kontrole doraźne w miarę potrzeb;
12) prowadzi szkolenia pracowników upoważnionych do przetwarzania danych osobowych oraz osób upoważnionych do przebywania w obszarze

przetwarzania podczas nieobecności osób upoważnionych oraz zgłasza potrzebę szkoleń zewnętrznych.

Rozdział 4
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

§ 10

1. Administrator bezpieczeństwa informacji przedstawia co pół roku administratorowi danych raport ze stanu bezpieczeństwa danych osobowych.
2. Administrator bezpieczeństwa informacji jest obowiązany poinformować na piśmie administratora danych o przypadkach naruszenia zasad niniejszego Zarządzenia przez pracowników upoważnionych, administratorów systemu lub zarządzających danymi, a w szczególności o:
   1) przetwarzaniu danych osobowych niezgodnie z procedurami;
   2) przetwarzaniu danych bez upoważnienia do przetwarzania;
   3) przetwarzaniu danych niezgodnie z zakresem upoważnienia;
   4) niedopełnieniu obowiązku zgłoszenia zbiorów danych do rejestru GIODO;
   5) udostępnianiu danych osobom nieupoważnionym lub podmiotom nieupoważnionym;
   6) przetwarzaniu danych w szerszym zakresie niż prawnie dozwolony;
   7) naruszeniu praw osób, których dane są przetwarzane;
   8) złamaniu tajemnicy danych i sposobów ich zabezpieczenia;
   9) zniszczeniu lub utracie dokumentów lub nośników informatycznych zawierających dane osobowe;
   10) niewłaściwym wykorzystaniu sprzętu informatycznego.
3. Pracownik upoważniony jest obowiązany powiadomić administratora systemu i zarządzającego danymi a ten powiadamia dyrektora IT i administratora bezpieczeństwa informacji o każdym 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) pojawieniu się niestandardowych komunikatów generowanych przez system informatyczny;
   5) pojawieniu się zmian w wyglądzie prezentowanych na ekranie danych,
   6) częściowym lub całkowitym braku danych;
   7) wykryciu wirusa komputerowego;
   8) znacznym spowolnieniu pracy systemu informatycznego;
   9) utraty tajności kluczy kryptograficznych;
   10) zgubieniu lub kradzieży nośnika informatycznego z danymi;
   11) podejrzeniu kradzieży sprzętu informatycznego lub dokumentów zawierających dane;
   12) zauważeniu śladów włamania do szaf lub pomieszczeń w obszarze przetwarzania
   13) zauważeniu innych niepokojących faktów.

4. Do czasu przybycia administratora systemu pracownicy upoważnieni:
   1) o ile to możliwe, podejmują czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia;
   2) o ile to możliwe, wstrzymują bieżącą pracę na sprzęcie informatycznym w celu zabezpieczenia miejsca zdarzenia;
   3) stosują się do innych instrukcji i regulaminów, jeżeli odnoszą się do zaistniałego zdarzenia;
5. Administrator systemu podejmuje działania zmierzające do ochrony systemu informatycznego przed dalszym naruszeniem.
6. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia o naruszeniu bezpieczeństwa przetwarzania danych osobowych przeprowadza postępowanie wyjaśniające, mające na celu ustalenie okoliczności zaistniałego zdarzenia.
7. Z faktu naruszenia bezpieczeństwa przetwarzania danych osobowych administrator bezpieczeństwa informacji sporządza raport zgodnie ze wzorem określonym w załączniku nr 9 do niniejszego Zarządzenia i przekazuje go administratorowi danych.
8. Administrator danych, po zapoznaniu się z raportem podejmuje decyzję o dalszym trybie postępowania.

Rozdział 5
Przekazywanie danych osobowych

§ 11

1. Zarządzający danymi przekazuje dane osobowe po otrzymaniu pisemnego wniosku zawierającego:
   1) cel przekazania i przeznaczenie danych;
   2) zakres danych adekwatny do celu przekazania i przeznaczenia;
   3) osoby upoważnione do odbioru danych.
2. Przekazanie danych osobowych następuje:
   1) na piśmie – za pokwitowaniem;
   2) na nośniku informatycznym – protokółem przekazania, który sporządza się zgodnie ze wzorem określonym w załączniku nr 10 do niniejszego Zarządzenia, po uprzednim zastosowaniu mechanizmów kryptograficznych;
   3) z zastosowaniem metody teletransmisji – protokółem, który sporządza się zgodnie ze wzorem określonym w załączniku nr 10 do niniejszego Zarządzenia, po uprzednim zastosowaniu mechanizmów kryptograficznych.
3. Zarządzający danymi, który otrzymał dostęp do danych osobowych metodą teletransmisji jest obowiązany niezwłocznie przekazać administratorowi bezpieczeństwa informacji wykazy i opisy wymienione w § 7 pkt 7 niniejszego Załącznika.

Rozdział 6
Udostępnianie danych osobowych

§ 12

1. Zarządzający danymi udostępnia dane osobowe po otrzymaniu zgody administratora danych oraz po analizie otrzymanego pisemnego wniosku określającego:
   1) cel udostępnienia i przeznaczenie danych;
   2) zakres danych adekwatny do celu udostępnienia i przeznaczenia;
   3) osoby upoważnione do odbioru danych;
   4) podstawę prawną udostępnienia danych osobowych albo wiarygodne uzasadnienie potrzeby posiadania danych.
2. Udostępnienie danych osobowych następuje poprzez przekazanie danych:
   1) na piśmie – listem poleconym za potwierdzeniem odbioru lub za pokwitowaniem, osobie imiennie wskazanej przez odbiorcę ;
   2) na nośniku informatycznym – po zastosowaniu mechanizmów kryptograficznych listem poleconym za potwierdzeniem odbioru osobie imiennie wskazanej przez odbiorcę lub protokółem przekazania, który sporządza się zgodnie ze wzorem określonym w załączniku nr 11 do niniejszego Zarządzenia;
   3) metodą teletransmisji – po zastosowaniu mechanizmów kryptograficznych protokółem przekazania, który sporządza się zgodnie ze wzorem określonym w załączniku nr 11 do niniejszego Zarządzenia .
3. Administrator systemu zarządza:
   1) aplikacjami kryptograficznymi;
   2) generowaniem kluczy kryptograficznych;
   3) wycofywaniem kluczy kryptograficznych.

Rozdział 7
Przetwarzanie danych osobowych na komputerach przenośnych

§ 13

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone przez zarządzających danymi do niezbędnego minimum.
2. Komputery przenośne przetwarzające dane osobowe pozostają zawsze pod opieką pracownika upoważnionego.
3. Dostęp do komputera przenośnego zawierającego dane osobowe jest możliwy po wprowadzeniu identyfikatora i hasła przez pracownika upoważnionego.
4. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują te same zasady jak przy pracy na komputerach stacjonarnych, a zwłaszcza:
   1) mogą na nich pracować tylko pracownicy upoważnieni do przetwarzania;
   2) pliki zawierające dane osobowe są przechowywane z zastosowaniem mechanizmów kryptograficznych i opatrzone hasłem dostępu;
   3) jest zabronione przetwarzanie na komputerach przenośnych całych

zbiorów danych osobowych;
5. Po ustaniu powodu przetwarzania danych osobowych na komputerach przenośnych, dane te należy przenieść na serwer a następnie trwale usunąć z pamięci komputera przenośnego.

Rozdział 8
Powierzenie przetwarzania danych osobowych

§ 14

1. Powierzenie przetwarzania dokonuje się umową na piśmie zawartą pomiędzy administratorem danych a podmiotem zewnętrznym.
2. Umowa powierzenia musi mieć jasno sprecyzowany cel i zakres przetwarzania, pod rygorem nieważności.
3. Przetwarzanie danych osobowych w celu wykonania serwisowania i konserwacji systemów informatycznych oznacza zapisanie w umowie jako celu – wykonania naprawy sprzętu lub systemu, natomiast zakres – obejmuje wszystkie dane zawarte w pamięci komputera.
4. Przykładowe zapisy umowy o powierzenie przetwarzania sporządza się zgodnie ze wzorem określonym w załączniku nr 12 do niniejszego Zarządzenia.
5. Zapisy umowy o powierzenie przetwarzania mogą być częścią zapisów innych umów.

Rozdział 9
Kontrola stanu bezpieczeństwa danych osobowych

§ 15

1. Kontrole stanu bezpieczeństwa danych osobowych przeprowadza się:
   1) w celu ustalenia ewentualnych przyczyn i skutków przetwarzania danych niezgodnego z ustawą o ochronie danych osobowych i rozporządzeniem do niej oraz przepisami wewnętrznymi dotyczącymi ochrony danych osobowych;
   2) w celu wskazania osób odpowiedzialnych za nieprawidłowości;
   3) w celu wskazania sposobów i środków likwidujących nieprawidłowości.
2. Kontrole stanu bezpieczeństwa danych osobowych przeprowadza się na podstawie rocznego planu kontroli, który zatwierdza administrator danych, a następnie akceptuje sprawozdanie z jego wykonania.
3. Doraźne kontrole stanu bezpieczeństwa danych osobowych przeprowadza się w zależności od potrzeb.
4. O przeprowadzeniu kontroli zarządzający danymi zostaje poinformowany z pięciodniowym wyprzedzeniem.
5. Informacja o przeprowadzeniu kontroli zawiera: datę i miejsce przeprowadzenia kontroli i okres czasu objęty kontrolą.
6. Kontrole przeprowadza administrator bezpieczeństwa informacji, który ma prawo:
   1) wstępu do wszystkich pomieszczeń obszaru przetwarzania;
   2) asystowania przy wszystkich czynnościach związanych

z przetwarzaniem danych osobowych;
3) wglądu do wszystkich dokumentów związanych z przetwarzaniem danych osobowych;
4) żądania od pracowników upoważnionych ustnych i pisemnych wyjaśnień.

7. Do przeprowadzenia kontroli administrator bezpieczeństwa informacji nie potrzebuje odrębnego upoważnienia.
8. Pracownicy upoważnieni oraz zarządzający danymi są obowiązani do udzielenia w czasie kontroli, wszystkich koniecznych informacji administratorowi bezpieczeństwa informacji.
9. Kwestionariusz kontroli sporządza się zgodnie ze wzorem określonym w załączniku nr 13 do niniejszego Zarządzenia.
10. Kwestionariusz kontroli po podpisaniu przez administratora bezpieczeństwa informacji i zarządzającego danymi stanowi podstawę do wydania przez administratora danych zaleceń pokontrolnych.

Rozdział 10
Szkolenia z zakresu bezpieczeństwa przetwarzania danych osobowych

§ 16

1. Pracownicy upoważnieni podlegają przeszkoleniu z zakresu bezpieczeństwa przetwarzania danych osobowych, które przeprowadza administrator bezpieczeństwa informacji.
2. Tematyka szkolenia obejmuje:
   1) przepisy ustawy o ochronie danych osobowych;
   2) przepisy wewnętrzne dotyczące ochrony danych osobowych.
3. Fakt przeszkolenia pracownicy upoważnieni potwierdzają podpisem w wykazie osób przeszkolonych.
4. Zaświadczenie o przeszkoleniu jest przechowywane w aktach osobowych pracownika.

w z. PREZYDENTA LUBLINA

prof. (nadzw.) dr hab. inż. Stanisław Fic
Zastępca Prezydenta

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Lublin

Rozdział 1
Poziomy bezpieczeństwa przetwarzania danych osobowych i dostęp do sieci publicznej

§ 1

1. Zarządzający danymi stosują środki bezpieczeństwa na poziomie co najmniej:
   1) podstawowym, jeżeli w systemie informatycznym nie są przetwarzane wrażliwe dane osobowe, wymienione w art. 27 ustawy oraz żadne urządzenie systemu informatycznego nie jest połączone z siecią publiczną - izolacja fizyczna;
   2) podwyższonym, jeżeli w systemie informatycznym przetwarzane są wrażliwe dane osobowe, wymienione w art. 27 ustawy oraz żadne urządzenie systemu informatycznego nie jest połączone z siecią publiczną - izolacja fizyczna;
   3) wysokim, jeżeli przynajmniej jedno z urządzeń systemu informatycznego połączone jest z siecią publiczną, przy czym połączenie to jest realizowane wyłącznie przy użyciu serwera terminali i przypisanego do niego oprogramowania klienckiego, ograniczającego ruch sieciowy do niezbędnego minimum oraz jest kontrolowane poprzez program typu zapora sieciowa – izolacja logiczna.
2. Dostęp do sieci publicznej za pomocą serwera terminali jest uzależniony od:
   1) zainstalowania i skonfigurowania oprogramowania przez administratora systemu;
   2) posiadania konta na serwerze z przypisanym do niego identyfikatorem oraz niepowtarzalnego hasła.
3. Administrator systemu konfiguruje oprogramowanie serwera terminali tak żeby:
   1) uniemożliwiało przenoszenie jakichkolwiek treści pomiędzy stacjami roboczymi a siecią publiczną i odwrotnie;
   2) uniemożliwiało zapisanie jakichkolwiek treści z sieci publicznej na stacji roboczej;
   3) odnotowało i jednoznacznie przypisało pracownikowi upoważnionemu: adres IP komputera, identyfikator, użycie hasła, godzinę zalogowania się, czas trwania połączenia oraz wszystkie wydarzenia, które miały miejsce podczas logowania;
   4) odnotowało i jednoznacznie przypisało adresowi IP komputera nieautoryzowane próby połączenia się z serwerem, próby wywołania adresów URL;
   5) komunikacja pomiędzy stacjami roboczymi a serwerem odbywała się

poprzez automatyczne szyfrowanie.

4. Jeżeli analiza ryzyka dostępu do sieci publicznej potwierdza możliwość nieuprawnionego dostępu do danych osobowych, Dyrektor IT może podjąć decyzję o fizycznej separacji systemu i blokadzie urządzeń odczytujących dane z nośników informatycznych.
5. Administrator systemu konfiguruje zabezpieczenia logiczne zapory sieciowej, żeby obejmowały :
   1) autoryzację wysyłanych danych;
   2) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
   3) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Rozdział 2
Procedury nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz rejestrowania i wyrejestrowywania tych uprawnień w systemach informatycznych przetwarzających dane osobowe

§ 2

1. Tylko pracownikowi upoważnionemu może zostać przyznany unikalny identyfikator wraz z poufnym hasłem w celu zarejestrowania go jako użytkownika w systemie informatycznym.
2. Tylko identyfikator wraz z prawidłowym hasłem umożliwia pracownikowi upoważnionemu dostęp do systemu.
3. Dostęp pracowników upoważnionych do systemu informatycznego jest kontrolowany za pomocą mechanizmów uwierzytelniania, autoryzacji i rozliczalności:
   1) mechanizm uwierzytelniania dopuszcza do systemu informatycznego po zastosowaniu identyfikatora i hasła dostępu;
   2) mechanizm autoryzacji pozwala przetwarzać dane osobowe tylko w zakresie przyznanych uprawnień dostępu do systemu informatycznego;
   3) mechanizm rozliczalności pozwala jednoznaczne przypisać wykonanie określonych czynności przetwarzania konkretnemu pracownikowi.
4. Rejestracja polega na przyznaniu identyfikatora, na wniosek zarządzającego danymi i na wprowadzeniu go przez administratora systemu do bazy użytkowników systemu oraz na przydzieleniu tymczasowego hasła oraz przekazaniu go pracownikowi.
5. Niezwłocznego zablokowania identyfikatora lub wyrejestrowania pracownika upoważnionego dokonuje administrator systemu na wniosek: administratora danych, zarządzającego danymi lub administratora bezpieczeństwa informacji.
6. Zablokowanie identyfikatora polega na zablokowaniu konta pracownika upoważnionego do czasu ustania przyczyny uzasadniającej blokadę.
7. Przyczyną zablokowania identyfikatora jest:
   1) nieobecność w pracy trwająca dłużej niż 21 dni;
   2) zawieszenie w pełnieniu obowiązków służbowych;
   3) wszczęcie postępowania dyscyplinarnego;

4) wypowiedzenie umowy o pracę.

8. Przyczyną wyrejestrowania uprawnień pracownika upoważnionego jest rozwiązanie lub wygaśnięcie stosunku pracy, w przypadku pracowników lub innego stosunku prawnego, w przypadku praktykantów, stażystów i innych osób, w ramach którego przetwarzano dane osobowe.

Rozdział 3
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 3

1. W przypadku wystąpienia zbieżności identyfikatora z przyznanym już wcześniej, administrator systemu nadaje pracownikowi upoważnionemu inny identyfikator.
2. Administrator systemu nie może przydzielić identyfikatora pracownika upoważnionego, który utracił uprawnienia do przetwarzania danych osobowych.
3. Pracownik upoważniony posiadający hasło dostępu do systemu jest obowiązany zapamiętać go, zachować w tajemnicy i nie ujawniać osobom trzecim, w tym innym pracownikom.
4. Pracownik upoważniony nie może korzystać z identyfikatora i hasła innego pracownika.
5. System powinien wymuszać tworzenie haseł składających się z niepowtarzalnego zestawu co najmniej sześciu znaków na poziomie podstawowym, a z ośmiu znaków w tym dużych i małych liter, cyfr, znaków specjalnych, na poziomach podwyższonym i wysokim.
6. Hasło nie może być identyczne z imieniem i nazwiskiem, datą urodzenia oraz nie może być nazwą pospolitą.
7. Po pierwszym poprawnym zalogowaniu, system wymusza zmianę hasła na hasło spełniające kryteria opisane w niniejszej instrukcji a potem co 30 dni.
8. Hasła są przechowywane w systemach informatycznych w postaci zaszyfrowanej.
9. Uwierzytelnianie pracownika upoważnionego może odbywać się także za pomocą karty mikroprocesorowej lub czytnika biometrycznego.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 4

1. W celu uruchomienia systemu informatycznego pracownik upoważniony powinien:
   1) uruchomić komputer;
   2) wybrać odpowiednią opcję umożliwiającą logowanie do systemu;
   3) zalogować się do systemu poprzez zastosowanie identyfikatora oraz indywidualnego, poufnego i aktualnego hasła.
2. Trzykrotne, zakończone niepowodzeniem logowanie do systemu powoduje

zablokowanie dostępu i interwencję administratora systemu.

3. Pracownik upoważniony podczas logowania do systemu nie może ujawniać oraz zapisywać hasła.
4. Administrator systemu programuje monitory komputerów tak, żeby wyłączyły się automatycznie po 5 minutach od przerwania pracy.
5. Wznowienie pracy monitora następuje po wprowadzeniu hasła przez pracownika upoważnionego.
6. Zakończenie pracy na stacji roboczej polega na skutecznym wylogowaniu się z systemu informatycznego i wyłączeniu komputera przez pracownika upoważnionego.

Rozdział 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 5

1. Kopie zapasowe mogą być: pełne, przyrostowe lub różnicowe.
2. Kopie zapasowe bazy danych tworzone są w systemie informatycznym codziennie, po zakończeniu przetwarzania a nadzór nad ich tworzeniem sprawuje administrator systemu.
3. Administrator systemu dokonuje zapisu bazy danych na nośniku informatycznym co 30 dni.
4. Administrator systemu wykonuje kopie systemu informatycznego na nośniku informatycznym co 30 dni.
5. Nośniki informatyczne zawierające kopie zapasowe przechowuje się w zamykanych na klucz szafach metalowych, zlokalizowanych w innych pomieszczeniach niż służące do bezpośredniego przetwarzania danych osobowych.
6. Nośniki informatyczne zawierające dane osobowe, po wprowadzeniu tych danych do systemu, pozbawia się zapisu poprzez skasowanie danych programem usuwającym trwale pliki lub poprzez ich fizyczne zniszczenie doprowadza do stanu uniemożliwiającego ich odczytanie.
7. Administrator systemu dokonuje co roku przeglądu kopii zapasowych pod względem ich dalszej przydatności do odtworzenia zapisanych danych.
8. Administrator systemu przeznacza kopie zapasowe, których dalsze przechowywanie nie jest uzasadnione potrzebami związanymi z ich przetwarzaniem, do protokólarnego zniszczenia, za zgodą zarządzającego danymi i dyrektora IT.
9. Protokół zniszczenia kopii zapasowych powinien zawierać przynajmniej: datę i miejsce zniszczenia, nazwę wydziału, biura, Kancelarii Prezydenta, Urzędu Stanu Cywilnego lub samodzielnego stanowiska pracy, nazwę zbioru danych osobowych, zakres danych osobowych, numer lub datę wykonania kopii, sposób zniszczenia, podpisy członków komisji.
10. Zniszczenie polega na trwałym wykasowaniu danych z nośnika oraz jego mechnicznym zniszczeniu w niszczarce lub demagnetyzacji.

Rozdział 6
Sposób, miejsce i okres przechowywania elektronicznych nośników informatycznych zawierających dane osobowe oraz kopii zapasowych

§ 6

1. Kopie jednostkowych danych osobowych w postaci zaszyfrowanej administrator systemu przechowuje w zamkniętej szafie znajdującej się w obszarze przetwarzania.
2. Kopie bazy danych na nośnikach informatycznych administrator systemu opisuje i przechowuje w zamkniętej szafie metalowej, w zamkniętym pomieszczeniu, niedostępnym dla osób trzecich, które może być zlokalizowane w innym budynku niż obszar przetwarzania.
3. Administrator systemu opisuje kopie systemu informatycznego i przechowuje je na nośnikach informatycznych w metalowej szafie, do której klucze przechowuje dyrektor IT.
4. Nośniki informatyczne zawierające kopie bazy danych i systemu informatycznego przechowuje się w pomieszczeniach, w których nie przetwarza się danych osobowych.
5. Nośniki informatyczne używane do przechowywania danych osobowych nie mogą być wykorzystywane do innych celów.
6. Czas przechowywania kopii zapasowych zależy od aktualności i przydatności zapisanych danych osobowych, chyba że inne przepisy stanowią o ich dłuższym przechowywaniu.

Rozdział 7
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt. III ppkt 1 załącznika do 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)

§ 7

1. Systemy informatyczne chronione są przed działaniem wirusów komputerowych aktualnym, licencjonowanym oprogramowaniem antywirusowym, zainstalowanym na serwerach, stacjach roboczych oraz komputerach przenośnych, o ile systemy te są narażone na działanie wirusów.
2. Tylko administrator systemu dysponuje mechanizmami pozwalającymi na zarządzanie oprogramowaniem antywirusowym, zarówno na serwerach, jak i na stacjach roboczych.
3. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad pracą systemu i zasobami danych osobowych na serwerach i stacjach roboczych poprzez skanowanie dysków, zaraz po włączeniu komputerów i w trakcie dnia

pracy a przy przesyłaniu danych do systemu – na bieżąco.

4. Administrator systemu, w celu przeciwdziałania atakowi zainfekowanych plików skanuje systemy informatyczne minimum raz na tydzień lub każdorazowo, po powzięciu wiadomości od pracowników upoważnionych o pojawieniu się wirusów.
5. W przypadku braku możliwości automatycznego usunięcia wirusów administrator systemu powinien:
   a) usunąć zainfekowane pliki, o ile nie zagraża to funkcjonalności systemu informatycznego;
   b) ingerować w bezpośrednią zawartość pliku w zależności od posiadanych kwalifikacji;
   c) odtworzyć pliki z kopii awaryjnych po sprawdzeniu czy nie są zainfekowane.
6. Nośniki informatyczne i ich zawartość podlegają kontroli antywirusowej przeprowadzanej przez administratora systemu każdorazowo przed ich użyciem.
7. Administrator systemu aktualizuje oprogramowanie antywirusowe o nową bazę wirusów, zgodnie z instrukcją producenta.

Rozdział 8
Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt. 4 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)

§ 8

1. Systemy informatyczne odnotowują:
   1) identyfikator pracownika upoważnionego, przetwarzającego dane osobowe w systemie i przypisują te czynności tylko jemu;
   2) datę i czas zalogowania i wylogowania z systemu;
   3) tożsamość stacji roboczej;
   4) nieudane i udane próby zalogowania się;
   5) wygaśnięcie czasu obowiązywania hasła dostępu do stacji roboczej i informują o tym fakcie;
   6) sporządzenie dla każdej osoby, której dane są przetwarzane w systemie informatycznym, raportu w formie wydruku zawierającego:
      a) datę pierwszego wprowadzenia danych do systemu;
      b) identyfikator pracownika upoważnionego wprowadzającego te dane;
      c) źródła danych w przypadku zbierania danych od osoby, której one nie dotyczą;
      d) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione;
      e) dacie i zakresie udostępnienia;
      f) sprzeciwu wobec przetwarzania danych osobowych o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie, o którym mowa w punkcie 1 następuje przez automatyczny

zapis w systemie a funkcje wyświetlania i wydruku generują dane tylko i wyłącznie jednej osoby.
3. Odnotowanie, o którym mowa w punkcie 6 musi być zrozumiałe dla przeciętnego odbiorcy, czyli zarówno funkcja wyświetlania jak i wydruku prezentuje informacje w pełnym brzmieniu, poprzedzone nazwą opisową danego pola, nie w postaci kodowanej lub skróconej.
4. System informatyczny posiada mechanizamy zapewniające ochronę przed nieautoryzowanym wprowadzaniem zmian w odnotowaniu.
5. W przypadku kasowania rekordów z danymi osobowymi, kasowanie musi być dokonane w rzeczywistości, np. przez nadpisanie informacją „pustą", a nie przez zaznaczenie rekordu jako skasowanego.

Rozdział 9
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informatycznych służących do przetwarzania danych osobowych

§ 9

1. Przeglądy i konserwacje systemów informatycznych muszą odbywać się przy zachowaniu pełnej separacji danych osobowych od osób nieupoważnionych do przetwarzania oraz pod nadzorem administratora systemu.
2. Administrator systemu dokonuje przeglądów i konserwacji systemów informatycznych w zależności od potrzeb.
3. Administrator systemu przegląda raporty dotyczące działania systemu informatycznego, logi systemowe, nie rzadziej niż raz na tydzień, a każdorazowo po wykryciu naruszenia zasad bezpieczeństwa przetwarzania danych osobowych.
4. Bieżące konserwacje i naprawy urządzeń informatycznych są przeprowadzane przez upoważnionych pracowników wydziału Informatyki i Telekomunikacji lub zewnętrzne podmioty.
5. Naprawy, o których mowa w punkcie 4 odbywają się w siedzibie Urzędu, a jeżeli to niemożliwe, poza siedzibą, ale po wcześniejszym nieodwracalnym usunięciu danych w nich przetwarzanych przez administratora systemu.
6. Uszkodzone nośniki informatyczne administrator systemu niszczy mechanicznie, sporządzając z tej czynności protokół.
7. Wykonywane przez podmiot zewnętrzny przeglądy i konsewacje systemów oraz nośników informatycznych służących do przetwarzania danych osobowych, które zawierają dane osobowe, należy traktować każdorazowo jako przetwarzanie danych i stosować zapisy Rozdziału „Powierzenie przetwarzania danych osobowych" Polityki bezpieczeństwa.

w z. PREZYDENTA LUBLINA
prof. nadzw. dr hab. inż. Stanisław Fic
Zastępca Prezydenta

Prezydent Miasta Lublin

Załącznik nr 3 do Zarządzania nr 439/2008 Prezydenta Miasta Lublin
z dnia 30 czerwca 2008 r.

Lublin, dnia .....

Wykaz budynków i pomieszczeń lub części pomieszczeń w .....[1] tworzących obszar w którym przetwarzane są dane osobowe[2]

Lp.	Adres	Nazwa zbioru danych osobowych	Piętro	Nr pokoju
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

.....
Zarządzający danymi

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.

2 Poprzez pomieszczenia lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe należy rozumieć zarówno te miejsca, w których wykonuje się: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie i usuwanie danych osobowych, jak i przechowuje się nośniki informacji zawierające dane osobowe, jak: szafy z dokumentacją papierową, czy szafy z komputerowymi nośnikami informacji. Do obszaru przetwarzania danych osobowych zaliczamy także pomieszczenia, gdzie składowane są uszkodzone nośniki danych (taśmy, dyski, płyty, uszkodzone komputery, itp) oraz np. sejf bankowy lub archiwum, jeżeli przechowuje się tam dane osobowe.

Lublin, dnia .....

Wykaz zbiorów danych osobowych przetwarzanych w .....[1] wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych[2]

Lp.	Nazwa zbioru danych osobowych	Nazwa programu zastosowanego do przetwarzania danych osobowych
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

.....
Zarządzający danymi

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.

2 Jeden program może przetwarzać dane osobowe zawarte zarówno w jednym, jak i wielu zbiorach. Sytuacja może być również odwrotna, kiedy to wiele różnych programów przetwarza dane osobowe stanowiące jeden zbiór. Programami mogą być także moduły systemu zintegrowanego, z których każdy wykonuje określone, wydzielone funkcjonalnie zadania.

Lublin, dnia .....

Opis struktury zbioru danych
przetwarzanego w ..... [1]
wskazujący zawartość poszczególnych pól informacyjnych
i powiązania między nimi[2]

Zbiór danych osobowych o nazwie .....
posiada następującą strukturę[3]:

1. Dane ..... w tym:
   a) .....
   b) .....
   c) .....
   d) .....
   Powiązanie z danymi: ..... .
2. Dane ..... w tym:
   a) .....
   b) .....
   c) .....
   d) .....
   Powiązanie z danymi: ..... .
   itd. ...

.....
Administrator systemu

---

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.

2 Wypełnia się dla każdego zbioru oddzielnie. Należy przedstawić strukturę danego zbioru i zakres informacji w nim gromadzonych.

3 Opis pojedynczego pola danych w zbiorze, powinien jednoznacznie wskazywać kategorię danych oraz powiązania między polami, np.:
Zbiór danych osobowych o nazwie „Klienci Firmy XYZ"
posiada następującą strukturę:

1. Dane adresowe klienta w tym:
   a) imię
   b) nazwisko
   c) kod pocztowy
   d) miejscowość
   itd. ...
2. Dane wszystkich składanych przez danego klienta zamówień w tym:
   a) nazwa towaru
   b) ilość towaru
   c) wartość zamówienia
   d) data zamówienia
   Powiązanie z danymi: Dane wszystkich składanych przez danego klienta zamówień są powiązane z danymi adresowymi klienta.
   itd. ...

Lublin, dnia .....

Opis przepływu danych pomiędzy poszczególnymi systemami w .....[1]

1. System informatyczny zbioru danych osobowych o nazwie[2] ..... eksportuje dane osobowe[3] ..... do systemu informatycznego zbioru danych osobowych o nazwie .... w sposób[4] ..... .

2. System informatyczny zbioru danych osobowych o nazwie[5] ..... importuje dane osobowe[6] ..... z systemu informatycznego zbioru danych osobowych o nazwie .... w sposób [7]..... .

.....
Administrator systemu

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.
2 Nazwa zbioru danych osobowych.
3 Np.: imię, nazwisko, ulica, nr domu, nr mieszkania, kod pocztowy, nazwa miejscowości, PESEL, itd.
4 W sposób: manualny (przy wykorzystaniu zewnętrznych nośników), albo za pomocą teletransmisji.
5 Nazwa zbioru danych osobowych.
6 Np.: imię, nazwisko, ulica, nr domu, nr mieszkania, kod pocztowy, nazwa miejscowości, PESEL, itd.
7 W sposób: manualny (przy wykorzystaniu zewnętrznych nośników), albo za pomocą teletransmisji.

Prezydent Miasta Lublin

Załącznik nr 7 do Zarządzania nr 439/2008 Prezydenta Miasta Lublin
z dnia 30 czerwca 2008 r.

Lublin, dnia .....

Wykaz osób upoważnionych do przetwarzania danych osobowych

w ..... [1]

Lp.	Nazwisko i imię	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

.....
Zarządzający danymi

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.

Lublin, dnia .....

Upoważnienie
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz w związku z wykonywaniem obowiązków służbowych upoważniam:

Panią/Pana ..... / ..... / ..... [1]

do przetwarzania danych osobowych zgodnie z przydzielonym zakresem czynności w zbiorze (zbiorach) [2].....,
na czas trwania zatrudnienia lub innego stosunku prawnego.

Upoważniony oświadcza, że zapoznał się z:

1. Polityką bezpieczeństwa Urzędu Miasta Lublin;
2. Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
3. Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
4. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzannia 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)

i zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, do których miał dostęp zarówno w trakcie, jak i po zakończeniu pracy, praktyki lub stażu oraz odwołaniu upoważnienia lub upływie jego ważności.[3]

....
Data i podpis upoważnionego *Zarządzający danymi*

....
Administrator Bezpieczeństwa Informacji *Administrator Danych Osobowych*

Pouczenie:
osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności karnej wynikającej z :

1. art. 51- 52 ustawy o ochronie danych osobowych,
2. art. 265 - 269b Kodeksu karnego w zakresie ochrony informacji,
3. art. 270 - 276 Kodeksu karnego w zakresie przestępstw przeciwko wiarygodności dokumentów,
4. art. 52 i 100 Kodeksu pracy w zakresie obowiązków pracowników względem pracodawcy.

1 Imię, nazwisko / stanowisko służbowe / wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.
2 Nazwa zbioru (zbiorów) danych osobowych.
3 Upoważnienie przechowuje się w aktach osobowych pracownika.

Lublin, dnia .....

Raport z naruszenia bezpieczeństwa przetwarzania danych osobowych

1. Data:.....Godzina:.....
2. Imię i nazwisko / stanowisko / wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy osoby powiadamiającej o zaistniałym zdarzeniu:
   .....
   .....
3. Rodzaj naruszenia bezpieczeństwa przetwarzania danych osobowych i okoliczności towarzyszące:
   .....
   .....
   .....
4. Przyczyny wystąpienia zdarzenia:
   .....
   .....
   .....
5. Podjęte działania:
   .....
   .....
   .....
6. Postępowanie wyjaśniające:
   .....
   .....
   .....
7. Uwagi:
   .....
   .....
   .....

.....
podpis Administratora Bezpieczeństwa Informacji

10. Decyzja co do dalszego postępowania:
    .....
    .....
    .....
    .....

.....
podpis Administratora Danych

Lublin, dnia .....

Protokół przekazania danych osobowych

§ 1

.....[1]
przekazuje .....[2]
.....[3]
następujące kategorie danych osobowych :
- .....
- .....
- ..... itd.[4]

z bazy danych o nazwie .....[5]

§ 2

Strony protokółu są świadome, że dane osobowe są chronione ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

§ 3

Następujący pracownicy zostali upoważnieni do dostępu do danych osobowych:
1. .....
2. .....
3. .....[6]

§ 4

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach: jeden dla przekazującego, drugi dla odbierającego.

....
podpis przekazującego *podpis odbierającego*

1 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.
2 Jednorazowo, okresowo lub stale.
3 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.
4 Np.: imię, nazwisko, ulica, nr domu, nr mieszkania, kod pocztowy, nazwa miejscowości, PESEL, itd.
5 Nazwa bazy danych osobowych.
6 Imię i nazwisko pracownika upoważnionego.

Lublin, dnia .....

Protokół udostępnienia danych osobowych innemu administratorowi danych

§ 1

Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy .....Urzędu Miasta Lublin udostępnia .....[1]:
następujące kategorie danych osobowych:

1. .....
2. .....
3. ..... itd.[2]

z bazy danych o nazwie .....[3]

§ 2

Otrzymujący dane osobowe oświadcza że:

1) dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz 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. z 2004 r. Nr 100, poz. 1024);
2) przygotował stosowną dokumentację wymaganą od podmiotu, który przetwarza dane osobowe zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznychi organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
3) odpowiada za wszelkie szkody wyrządzone osobom trzecim, które powstały w związku z nienależytym przetwarzaniem udostępnionych danych osobowych.

1 Nazwa i adres podmiotu, któremu udostępniamy dane osobowe.
2 Np.: imię, nazwisko, ulica, nr domu, nr mieszkania, kod pocztowy, nazwa miejscowości, PESEL, itd.
3 Nazwa bazy danych.

§ 3

Zaszyfrowane dane osobowe udostępniono [4] ..... .

§ 5

Osobami upoważnionymi do odbioru danych osobowych są:

1. ..... .
2. ..... .
3. ..... .[5]

§ 6

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach: jeden dla przekazującego, drugi dla odbierającego.

.....	.....
podpis przekazującego	*podpis odbierającego*

4 Na piśmie, na nośniku informatycznym lub metodą teletransmisji.

5 Imię, nazwisko, nr dowodu osobistego.

Lublin, dnia .....

Umowa powierzenia przetwarzania danych osobowych

zawarta w Lublinie w dniu xx . xx . xxxx roku pomiędzy

Gminą Lublin

reprezentowaną przez:

.... **Prezydenta Miasta**
.... **Dyrektora Wydziału**

zwaną dalej **Zleceniodawcą**

a

Firmą .....
z siedzibą w ..... ul. .....
NIP .....
REGON .....
wpisaną do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w ..... reprezentowaną przez:

.... **Prezesa Zarządu**

zwaną dalej **Zleceniobiorcą**.

§ ...

1. Zleceniodawca oświadcza, że powierza Zleceniobiorcy przetwarzanie danych osobowych zawartych w zbiorze danych osobowych o nazwie ..... .
2. Zleceniobiorca oświadcza, że wyraża zgodę na powierzenie przetwarzania danych osobowych zawartych w zbiorze o nazwie ..... .
3. Dane osobowe będą przetwarzane w celu ..... .
4. Zakres przetwarzanych danych obejmuje następujące kategorie danych: ..... .

§ ...

1. Zleceniobiorca oświadcza, że dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych

osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz 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. z 2004 r. Nr 100, poz. 1024).

2. Zleceniobiorca oświadcza, że przygotował stosowną dokumentację wymaganą od podmiotu, któremu powierzono przetwarzanie danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz 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. z 2004 r. Nr 100, poz. 1024).
3. Zleceniobiorca odpowiada za wszelkie szkody wyrządzone osobom trzecim, które powstały w związku z nienależytym przetwarzaniem powierzonych do przetwarzania danych osobowych.

§ ...

1. W sprawach nieuregulowanych niniejszą umową znajdują zastosowanie przepisy powołanej wyżej: ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz innych przepisów.
2. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

Zleceniodawca *Zleceniobiorca*

Lublin, dnia .....

Kwestionariusz kontroli bezpieczeństwa danych osobowych
w zbiorze .....[1]
w ..... [2]

Informacje ogólne				
1.	**Imię i nazwisko zarządzającego danymi**			
2.	**Nazwa zbioru danych osobowych**			
3.	**Nazwa systemu informatycznego przetwarzającego dane osobowe**			
4.	**Numery kontrolowanych pomieszczeń**			
5.	**Imię i nazwisko administratora systemu informatycznego**			
6.	**Informacji udzielali (imię , nazwisko, stanowisko)**			
Informacje szczegółowe				
Lp.	**Zagadnienie**	**Tak**	**Nie**	**Opis - uwagi**
7.	**Zbiór danych został zgłoszony do GIODO.**			
8.	**Zbiór danych został powierzony do przetwarzania umową**			
9.	**Sporządzono poprawną umowę w zakresie powierzenia przetwarzania danych osobowych**			

1 Nazwa zbioru danych osobowych.
2 Wydział, biuro, Kancelaria Prezydenta, Urząd Stanu Cywilnego lub samodzielne stanowisko pracy.

10.	**Określono poziom bezpieczeństwa przetwarzanych danych osobowych**			
11.	**Dostęp do sieci publicznej jest realizowany za pomocą serwera terminali**			
12.	**Sporządzono wykaz obszarów przetwarzania**			
13.	**Sporządzono wykaz zbiorów danych osobowych**			
14.	**Sporządzono opis struktury zbiorów danych**			
15.	**Opisano sposób przepływu danych pomiędzy systemami**			
16.	**Upoważniono pracowników do przetwarzania danych osobowych**			
17.	**Tylko pracownicy upoważnieni przetwarzają dane osobowe**			
18.	**Sporządzono wykaz osób upoważnionych do przetwarzania danych osobowych**			
19.	**System informatyczny odnotowuje identyfikator pracownika upoważnionego**			
20.	**System informatyczny odnotowuje datę i czas zalogowania i wylogowania z systemu**			
21.	**System informatyczny odnotowuje tożsamość stacji roboczej**			
22.	**System informatyczny odnotowuje nieudane i udane próby zalogowania się**			

23.	System informatyczny odnotowuje wygśnięcie czasu obowiązywania hasła dostępu do stacji roboczej			
24.	System informatyczny umożliwia sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane, raportu zawierającego: •datę pierwszego wprowadzenia danych do systemu; •identyfikator pracownika upoważnionego wprowadzającego te dane; •źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą; •informacje o odbiorcach danych, którym dane osobowe zostały udostępnione; •datę i zakres udostępnienia; •sprzeciw wobec przetwarzania danych osobowych o którym mowa w art. 32 ust. 1 pkt 8 ustawy			
25.	System informatyczny jest zabezpieczony przed awarią zasilania			
26.	Do zalogowania służą indywidualne identyfikatory oraz hasła			
27.	Zablokowane lub wyrejestrowane identyfikatory nie są powtórnie używane			
28.	Zastosowano prawidłowo zbudowane identyfikatory			
29.	Zastosowano adekwatne do poziomu bezpieczeństwa hasła			
30.	Pracownicy upoważnieni utrzymują hasła w tajemnicy			

31.	System wymusza zmianę hasła tymczasowego			
32.	System wymusza zmianę hasła co 30 dni			
33.	Hasła są w systemie zaszyfrowane			
34.	Administrator systemu tworzy regularne kopie systemu i bazy danych			
35.	Nośniki z kopiami są przechowywane w zamkniętych szafach metalowych			
36.	Nośniki z pojedynczymi danymi są przechowywane w zamkniętych szafach			
37.	Oprogramowanie antywirusowe sprawuje ciągły nadzór nad pracą systemu			
38.	Baza wirusów jest uaktualniana			
39.	Przeglądy i konserwacje systemów informatycznych odbywają się pod nadzorem pracowwnika upoważnionego			
40.	Administrator systemu sprawdza okresowo logi systemowe			
41.	Dokumenty zawierające dane osobowe przechowuje się w zamykanych szafach, do których klucze znajdują się w ustalonym miejscu			
42.	Robocze wydruki danych osobowych po wykorzystaniu są niszczone w niszczarce			
43.	Dokumenty zawierające dane osobowe transportuje się w bezpiecznych kopertach			

44.	**Klucze do pomieszczeń w obszarze przetwarzania są pobierane i deponowane na portierni**			
45.	**Pomieszczenia serwerowni są prawidłowo zabezpieczone**			
46.	**W obszarze przetwarzania przebywają jedynie pracownicy upoważnieni**			
47.	**Interesanci mają zorganizowane i wyznaczone miejsce do załatwienia spraw**			
48.	**Stanowiska komputerowe mają prawidłowo ustawione ekrany monitorów**			
49.	**Ekrany komputerów są wyposażone w wygaszacze włączające się automatycznie po upływie ustalonego czasu nieaktywności**			
50.	**Egzemplarz polityki bezpieczeństawa, instrukcji zarządzania systemem, ustawy oraz rozporządzenia jest dostępny w sekretariacie**			
51.	**Do kwestionariusza dołącza się (stanowiące jego integralną część) załączniki, jak dodatkowe protokóły, ekspertyzy, dowody, itp.**			
52.	**Dodatkowe spotrzeżenia .....**			
53.	**Uwagi zarządzającego danymi**			
54.	**Zarządzający danymi został powiadomiony o prawie zgłoszenia zastrzeżeń do faktów ujętych w kwestionariuszu i złożenia wyjaśnień**			
55.	**Jeżeli zarządzający danymi odmawia podpisania kwestionariusza, obowiązany jest złożyć pisemne wyjaśnienie o przyczynach tej odmowy, stanowiące załącznik do kwestionariusza**			

56.	**Zalecenia pokontrole wraz z terminami ich realizacji zostaną przedstwione w ciągu 5 dni roboczych, odrębnym pismem, podpisanym przez Administratora danych**
57.	**Kwestionariusz sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden otrzymuje zarządzający danymi, drugi kontrolujący**
58.	**Kontrolę przeprowadził: .....**
59.	**Lublin, dnia .....**

.....
Kontrolujący

.....
Zarządzający danymi