Prezydent Miasta Lublin

Zarządzenie nr 755/2009

Prezydenta Miasta Lublin

z dnia 22 października 2009 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie 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. 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 Miasta Lublin, 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 Lublin;
2) kierującym wydziałem – rozumie się przez to osobę kierującą wydziałem, biurem, Kancelarią Prezydenta, Urzędem Stanu Cywilnego, wieloosobowym stanowiskiem pracy oraz samodzielnym stanowiskiem pracy;
3) zarządzającym zbiorem – rozumie się przez to osobę kierującą wydziałem, biurem, Kancelarią Prezydenta, Urzędem Stanu Cywilnego, wieloosobowym stanowiskiem pracy oraz samodzielnym stanowiskiem pracy, która zarządza danymi osobowymi w zbiorze danych osobowych;
4) administratorze systemu – rozumie się przez to osobę upoważnioną do zarządzania systemem lub systemami informatycznymi;
5) dyrektorze IT – rozumie się przez to dyrektora Wydziału Informatyki i Telekomunikacji;
6) administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną imiennie przez administratora danych do nadzorowania

przestrzegania zasad ochrony danych osobowych;

7) osobie upoważnionej – rozumie się przez to osobę upoważnioną przez administratora danych do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zobowiązanej jednocześnie do zachowania w tajemnicy danych osobowych, do których miała dostęp oraz sposobów ich zabezpieczenia;
8) wydziale – rozumie się przez to wydział, biuro, Kancelarię Prezydenta, Urząd Stanu Cywilnego, wieloosobowe stanowisko pracy oraz samodzielne stanowisko pracy;
9) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
10) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
11) GIODO – rozumie się przez to Generalnego Inspektora Ochrony Danych Osobowych;
12) polityce – rozumie się przez to politykę bezpieczeństwa danych osobowych Urzędu Miasta Lublin, stanowiącą załącznik nr 1 do niniejszego Zarządzenia;
13) instrukcji – rozumie się przez to instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu miasta Lublin, stanowiącą załącznik nr 2 do niniejszego Zarządzenia;
14) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
15) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione w sposób nieautoryzowany;
16) poufności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
17) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości pracownika upoważnionego;
18) przetwarzaniu – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych przez osoby upoważnione a zwłaszcza wykonywane w systemach informatycznych;
19) 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;
20) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych i innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
21) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych i innych, znany jedynie osobie upoważnionej służący do uzyskania dostępu do systemu informatycznego przetwarzającego dane osobowe;
22) środkach kryptograficznej ochrony – rozumie się przez to mechanizmy szyfrowania danych;

23)systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych w zbiorze danych.

§ 3

Traci moc Zarządzenie Nr 439/2008 Prezydenta Miasta Lublin z dnia 30 czerwca 2008 roku w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miasta Lublin.

§ 4

Nadzór nad wykonaniem Zarządzenia powierzam administratorowi bezpieczeństwa informacji.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Lublin

dr inż. Adam Wasilewski

Rozdzielnik:

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

Administrator Bezpieczeństwa Informacji

Waldemar Ofiarski

DYREKTOR Wydziału Organizacji Urzędu

Monika Madejska

Radca Prawny

Polityka bezpieczeństwa danych osobowych w Urzędzie Miasta Lublin

Rozdział 1
Główne zasady bezpiecznego przetwarzania danych osobowych

§ 1

1. Osoby upoważnione 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;
   3) zobowiązują się do zachowania poufności 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.
2. Zarządzający zbiorami wdrażają systemy informatyczne służące do przetwarzania danych osobowych gwarantujące:
   1) rozliczalność;
   2) integralność;
   3) uwierzytelnianie.

Rozdział 2
Organizacja zabezpieczania danych osobowych przez zarządzającego zbiorem

§ 2

1. Przetwarzając dane osobowe zarządzający zbiorem:
   1) prowadzi teczki aktowe o symbolu liczbowym i tytule:
      a) 5240 – „Wnioski o zgłoszeniu zbioru danych osobowych do rejestracji" kategorii archiwalnej B5;
      b) 5241 – „Wnioski i informacje o zbieraniu, przetwarzaniu i udostępnianiu danych osobowych" kategorii archiwalnej B5;
   2) wyznacza pracownika do prowadzenia powyższej dokumentacji, chyba

BG

że sam wykonuje te czynności;

3) ustala z dyrektorem IT, ewentualnie z kierującym innym wydziałem, kto będzie administratorem systemu lub wyznacza go spośród sobie podległych osób upoważnionych, chyba że powierzył przetwarzanie w tym zakresie danych podmiotowi zewnętrznemu;
4) decyduje na podstawie rozporządzenia i zleca administratorowi systemu zastosowanie dla zbioru danych osobowych poziomu bezpieczeństwa:
   a) podstawowego – jeżeli przetwarzane są dane osobowe zwykłe oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
   b) podwyższonego – jeżeli przetwarzane są dane osobowe wrażliwe, wymienione w art. 27 ustawy oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
   c) wysokiego – jeżeli przynajmniej jedno urządzenie systemu informatycznego jest połączone z siecią publiczną;
5) sporządza i prowadzi wykaz zbiorów danych osobowych, którymi zarządza wraz ze wskazaniem programów (systemów) zastosowanych do przetwarzania tych danych zgodnie ze wzorem określonym w załączniku nr 3 do niniejszego Zarządzenia, przekazując, po każdej zmianie, aktualną wersję wykazu administratorowi bezpieczeństwa informacji;
6) wyznacza osoby, które zostaną upoważnione do przetwarzania i określa:
   a) w jakim zakresie (przeglądania danych, modyfikowania danych lub administrowania systemem) będą przetwarzać dane osobowe;
   b) jakie uprawnienia w systemie informatycznym (konkretne czynności charakterystyczne dla danego zbioru), w ramach przyznanego zakresu upoważnienia, będą wykonywać osoby wyznaczone do przetwarzania;
7) przygotowuje upoważnienia do przetwarzania danych osobowych, zgodnie ze wzorem określonym w załączniku nr 4 do niniejszego Zarządzenia w trzech egzemplarzach (jeden dla osoby upoważnionej, drugi do dokumentacji zarządzającego zbiorem, trzeci do teczki akt osobowych pracownika) i przekazuje je administratorowi bezpieczeństwa informacji do podpisu, wraz z podpisanym przez siebie wnioskiem o nadanie uprawnień.

2. Prezydent Miasta upoważni odrębnym zarządzeniem administratora bezpieczeństwa informacji do nadawania upoważnień do przetwarzania danych w imieniu administratora danych. Administrator bezpieczeństwa informacji, zwraca podpisane przez siebie upoważnienia zarządzającemu zbiorem po nadaniu numeracji i wprowadzeniu do rejestru.
3. Zarządzający zbiorem przekazuje upoważnienia administratorowi systemu celem nadania uprawnień w systemie informatycznym.
4. Administrator systemu:
   1) na polecenie zarządzającego zbiorem nadaje w systemie informatycznym uprawnienia osobom uprawnionym, identyfikator i hasło;
   2) uzupełnia część D załącznika nr 4 do niniejszego Zarządzenia wpisując

identyfikator oraz datę nadania hasła i uprawnień w systemie informatycznym i zwraca wnioski zarządzającemu zbiorem;
3) sporządza listę osób upoważnionych, którym nadał uprawnienia w systemie informatycznym i uzyskuje pokwitowanie odbioru identyfikatora i hasła poprzez złożenie podpisu wraz z datą osoby upoważnionej, a następnie przechowuje listę w swojej dokumentacji aktowej.

§ 3

1. Kierujący innym wydziałem, chcąc uzyskać uprawnienia do przetwarzania danych (w zakresie przeglądania, modyfikowania danych lub administrowania systemem) dla osób z własnego wydziału:
   1) uzgadnia z zarządzającym zbiorem możliwy do zaakceptowania przez zarządzającego zakres upoważnień do przetwarzania danych osobowych i zakres uprawnień w systemie informatycznym;
   2) kieruje do zarządzającego zbiorem wniosek na piśmie zawierający:
      a) imiona i nazwiska osób wyznaczonych do przetwarzania danych;
      b) zakres upoważnienia;
      c) zakres uprawnienia w systemie informatycznym;
      d) dokładne określenie obszaru przetwarzania danych (adres wydziału, piętro, nr pokoju).
2. Zarządzający zbiorem może odmówić przyznania uprawnień do przetwarzania danych osobowych w zbiorze jeżeli:
   1) system informatyczny służący do przetwarzania danych osobowych w danym zbiorze nie posiada możliwości zwiększenia liczby użytkowników;
   2) analiza ryzyka przetwarzania danych osobowych przez osoby wyznaczone do przetwarzania nie daje gwarancji ich zabezpieczenia.
3. Kierujący innym wydziałem jest obowiązany do niezwłocznego przekazywania zarządzającemu zbiorem informacji, o których mowa w ust. 1 pkt. 2 w przypadku ich zmiany.
4. Zarządzający zbiorem przygotowuje upoważnienia do przetwarzania danych osobowych. § 2 ust. 1 pkt 7 i ust. 2 – 4 stosuje się odpowiednio.

§ 4

1. Zarządzający zbiorem dopuszcza do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie do przetwarzania.
2. Upoważnienia do przetwarzania danych osobowych są wystawiane:
   1) każdej osobie wyznaczonej do przetwarzania danych osobowych w zbiorze;
   2) na czas określony lub nieokreślony;
   w zakresie przeglądania danych, modyfikowania danych lub administrowania systemem.
3. Zarządzający zbiorem, z własnej inicjatywy lub z inicjatywy kierującego innym wydziałem, przygotowuje wniosek o cofnięcie upoważnień do przetwarzania danych osobowych i odebranie uprawnień w systemie informatycznym zgodnie ze wzorem określonym w załączniku nr 5 do niniejszego Zarządzenia w trzech egzemplarzach (jeden dla osoby upoważnionej, drugi do dokumentacji zarządzającego zbiorem, trzeci do

teczki akt osobowych pracownika) i przekazuje ten wniosek administratorowi bezpieczeństwa informacji celem podpisania cofnięcia upoważnienia i odnotowania w rejestrze. Cofnięcie upoważnienia stanowi podstawę dla administratora systemu do cofnięcia uprawnień w systemie informatycznym.

4. Cofnięcie upoważnienia następuje w szczególności w przypadku:
   1) gdy osoba upoważniona zakończyła zatrudnienie, pracę, staż lub praktykę lub zmieniła zakres upoważnienia;
   2) gdy kierujący innym wydziałem nie spełnia obowiązku o którym mowa w § 3 ust. 3.

Rozdział 3
Organizacja pozostałych czynności związanych z zabezpieczeniem przetwarzania danych osobowych przez zarządzającego zbiorem

§ 5

1. Zarządzający zbiorem :
   1) sporządza i aktualizuje elektroniczną ewidencję osób upoważnionych do przetwarzania danych osobowych w zbiorze zgodnie ze wzorem określonym w załączniku nr 6 do niniejszego Zarządzenia;
   2) sporządza i aktualizuje elektroniczny wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe w zbiorze zgodnie ze wzorem określonym w załączniku nr 7 do niniejszego Zarządzenia;
   3) sporządza i aktualizuje elektroniczny opis struktury zbioru danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zgodnie ze wzorem określonym w załączniku nr 8 do niniejszego Zarządzenia;
   4) sporządza i aktualizuje elektroniczny opis przepływu danych pomiędzy poszczególnymi systemami zgodnie ze wzorem określonym w załączniku nr 9 do niniejszego Zarządzenia;
2. Zarządzający zbiorem:
   1) rejestruje zbiór danych osobowych w rejestrze GIODO wysyłając za pomocą platformy elektronicznej e-Giodo wypełniony i podpisany wspólnie z administratorem danych wniosek zgłoszeniowy, stosując przepisy art. 41.1 ustawy oraz art. 46.2, chyba że administrator danych jest zwolniony z obowiązku rejestracji zbioru zgodnie z art. 43.1 ustawy;
   2) aktualizuje wniosek zgłoszeniowy w terminie 30 dni od dokonania zmian w zbiorze danych osobowych, stosując przepisy art. 41.2 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) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami
   2) merytorycznie poprawne i adekwatne w stosunku do celów

BDy

przetwarzania;
3) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to niezbędne do osiągnięcia celu przetwarzania;
4) przetwarzane zgodnie z prawem, stosując zapisy art. 23 – 30 ustawy odnośnie zasad przetwarzania danych, zbierania danych, przetwarzania danych wrażliwych oraz udostępniania danych;
5) przekazywane do państwa trzeciego, stosując zapisy art. 47 – 48 ustawy.

Rozdział 4
Powierzenie przetwarzania danych osobowych innemu podmiotowi

§ 6

1. Jeżeli Urząd nie dysponuje odpowiednimi środkami sprzętowymi lub programowymi zapewniającymi przetwarzanie danych, Zarządzający zbiorem wnioskuje do administratora danych, po konsultacji z dyrektorem IT, o powierzenie przetwarzania danych innemu podmiotowi.
2. Powierzenie przetwarzania następuje w formie umowy na piśmie zawartej pomiędzy administratorem danych a podmiotem zewnętrznym. Umowa powierzenia, pod rygorem nieważności, musi mieć jasno sprecyzowany cel i zakres przetwarzania oraz określać sposób postępowania z danymi po zakończeniu umowy.
3. Umowę o powierzenie przetwarzania sporządza się zgodnie ze wzorem określonym w załączniku nr 10 do niniejszego Zarządzenia.
4. Zapisy umowy o powierzenie przetwarzania mogą stanowić część innych umów zawartych z podmiotem zewnętrznym.

Rozdział 5
Ochrona danych osobowych i obszaru przetwarzania

§ 7

1. Dokumenty zawierające dane osobowe po zakończeniu przetwarzania lub pracy przechowywane są w szafach zamykanych na klucze, przechowywane w ustalonym miejscu, do którego dostęp mają jedynie osoby upoważnione.
2. Dokumenty zawierające dane osobowe niszczy się w sposób uniemożliwiający ich odczytanie.
3. Dokumenty zawierające dane osobowe transportuje się w zaklejonych kopertach chroniących przed uszkodzeniem lub zniszczeniem.

§ 8

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, goniec 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 na portierni po odnotowaniu w książce pobrań kluczy i tam przechowywane po zakończonej pracy.
5. Stanowiska pracy mają tak zlokalizowane urządzenia informatyczne służące do przetwarzania danych osobowych, żeby osoby nieupoważnione nie mogły widzieć treści wyświetlanych na ekranów monitorów komputerowych.

§ 9

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 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 6
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

§ 10

1. Administrator bezpieczeństwa informacji jest obowiązany poinformować na piśmie administratora danych o przypadkach naruszenia zasad niniejszego Zarządzenia przez osoby upoważnione, administratorów systemu lub zarządzających zbiorami a zwłaszcza o:
   1) przetwarzaniu bez upoważnienia do przetwarzania;
   2) przetwarzaniu niezgodnie z zakresem upoważnienia;
   3) niedopełnieniu obowiązku zgłoszenia zbiorów danych do rejestru GIODO;
   4) złamaniu tajemnicy danych i sposobów ich zabezpieczenia;
   5) niewłaściwym wykorzystaniu sprzętu informatycznego.
2. Osoba upoważniona jest obowiązana powiadomić administratora systemu i zarządzającego zbiorem a ten powiadamia 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 zmian w wyglądzie prezentowanych na ekranie danych,
   5) wykryciu wirusa komputerowego;
   6) utraty tajności kluczy kryptograficznych;
   7) zgubieniu lub kradzieży nośnika danych;

8) podejrzeniu kradzieży sprzętu informatycznego lub dokumentów zawierających dane;
9) zauważeniu śladów włamania do szaf lub pomieszczeń w obszarze przetwarzania;
10) 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 sporządzając raport z naruszenia bezpieczeństwa danych zgodnie ze wzorem określonym w załączniku nr 11 do niniejszego Zarządzenia..

Rozdział 7
Kontrola stanu bezpieczeństwa danych osobowych

§ 11

1. Administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony danych osobowych wykonując kontrole stanu bezpieczeństwa danych osobowych.
2. Kontrole stanu bezpieczeństwa danych osobowych przeprowadza się po akceptacji administratora danych:
   1) na podstawie planu kontroli;
   2) po naruszeniu bezpieczeństwa przetwarzania danych.
3. Administrator bezpieczeństwa informacji, ma prawo:
   1) wstępu do wszystkich pomieszczeń obszaru przetwarzania;
   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) żądania od osób upoważnionych ustnych i pisemnych wyjaśnień
   6) unieważnić osobie upoważnionej upoważnienie do przetwarzania danych osobowych i zlecić zarządzającemu zbiorem odebranie uprawnień w systemie informatycznym w wyniku rażącego naruszenia bezpieczeństwa przetwarzania danych osobowych.
4. Do przeprowadzenia kontroli administrator bezpieczeństwa informacji nie potrzebuje odrębnego upoważnienia.
5. Osoby upoważnione oraz zarządzający danymi są obowiązani do udzielenia w czasie kontroli, wszystkich koniecznych informacji administratorowi bezpieczeństwa informacji.
6. Kwestionariusz kontroli sporządza się zgodnie ze wzorem określonym w załączniku nr 12 do niniejszego Zarządzenia.
7. Kwestionariusz kontroli po podpisaniu przez administratora bezpieczeństwa informacji i zarządzającego zbiorem stanowi podstawę do wydania przez administratora danych zaleceń pokontrolnych.

Radca Prawny

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

Rozdział 1
Podstawowe mechanizmy w jakie powinny być wyposażone urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

§ 1

Systemy informatyczne służące do przetwarzania danych osobowych powinny być wyposażone w mechanizmy:

1) rozliczalności, który pozwala jednoznaczne przypisać wykonanie określonych czynności przetwarzania konkretnemu pracownikowi upoważnionemu;
2) integralności, który pozwala autoryzować czynności zmiany lub zniszczenia danych;
3) tworzenia raportu, który zawiera zakres i treść przetwarzanych danych;
4) uwierzytelniania, który weryfikuje deklarowaną tożsamość osoby upoważnionej.

Rozdział 2
Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 2

1. W celu rozpoczęcia pracy w systemie informatycznym należy:
   1) uruchomić komputer;
   2) zalogować się do systemu poprzez zastosowanie unikalnego identyfikatora oraz indywidualnego, poufnego, własnego hasła, zapewniającego w sposób jednoznaczny przypisanie danej osobie wykonywanych czynności.
2. Trzykrotne, zakończone niepowodzeniem logowanie do systemu powinno powodować zablokowanie dostępu i wymaga interwencji administratora systemu.
3. Monitory komputerów powinny wyłączyć się automatycznie po minimum 15 minutach od przerwania pracy a wznowienie pracy monitora następuje po wprowadzeniu hasła.
4. Udanie się na dłuższą przerwę lub zakończenie pracy na stacji roboczej powinno poprzedzać skuteczne wylogowanie się z systemu informatycznego i wyłączenie komputera.

Rozdział 3
Procedury nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz rejestrowania i wyrejestrowywania tych uprawnień w systemach informatycznych

§ 3

1. O nadanie osobom upoważnionym uprawnień w systemie informatycznym obsługującym zbiór danych osobowych, wnioskuje zarządzający zbiorem wnioskiem sporządzonym zgodnie ze wzorem określonym w załączniku nr 4 do niniejszego Zarządzenia.
2. Zakres uprawnień w systemie odpowiada nazwom czynności charakterystycznych dla danego zbioru, które może wykonywać osoba upoważniona w ramach zakresu upoważnienia.
3. Zarządzający zbiorem wnioskuje o cofnięcie osobie upoważnionej uprawnień w systemie i zleca administratorowi systemu ich wyrejestrowanie przygotowując wniosek zgodnie ze wzorem określonym w załączniku nr 5 do niniejszego Zarządzenia.

Rozdział 4
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 4

1. W przypadku wystąpienia zbieżności identyfikatora z przyznanym już wcześniej, administrator systemu nadaje osobie upoważnionej inny identyfikator.
2. Pierwsze przydzielone hasło powinno być jednorazowe a po jego poprawnym użyciu system powinien automatycznie wymuszać wpisanie nowego hasła do dalszego użytkowania co 30 dni.
3. Hasła zmieniane są przez osoby upoważnione.
4. System powinien zapewniać:
   1) jakość hasła, czyli zastosowanie odpowiedniej ilość znaków, wielkich i małych liter, cyfr lub znaków specjalnych w zależności od poziomu bezpieczeństwa przetwarzania;
   2) generowanie hasła różniącego się od co najmniej trzech ostatnio stosowanych przez osobę upoważnioną.
5. Osoba upoważniona posiadająca hasło dostępu do systemu jest obowiązana zachować je w tajemnicy i nie ujawniać innym osobom.
6. System powinien wymuszać tworzenie haseł składających się z niepowtarzalnego zestawu co najmniej:
   1) sześciu znaków na poziomie bezpieczeństwa podstawowym,
   2) ośmiu znaków w tym dużych i małych liter, cyfr lub znaków specjalnych, na poziomach bezpieczeństwa podwyższonym i wysokim.
7. W przypadku użytkowania systemów informatycznych wyposażonych w karty mikroprocesorowe lub czytniki biometryczne stosuje się instrukcje użytkowania producenta.

Rozdział 5
Procedury tworzenia i przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz sposób, miejsce i okres przechowywania elektronicznych nośników danych

§ 5

1. Kopie zapasowe są tworzone przez administratora systemu w szczególności na:
   1) elektronicznych nośnikach danych;
   2) specjalnie do tego celu przeznaczonych komputerach lub zewnętrznych sieciowych dyskach twardych, z zastrzeżeniem, że nie mogą to być jednocześnie serwery na których są zlokalizowane zbiory danych.
2. Zapasowe kopie zbioru danych powinny być tworzone w systemie informatycznym codziennie, po zakończeniu przetwarzania.
3. Kopie zapasowe konfiguracji programów i narzędzi programowych wraz z uprawnieniami osób upoważnionych powinny być wykonywane w przypadku zmiany systemu informatycznego.
4. Elektroniczne nośniki danych zawierające kopie zapasowe, pozbawia się zapisu poprzez:
   1) zapisanie nowej kopii zapasowej na tym samym nośniku;
   2) skasowanie danych programem usuwającym trwale pliki;
   3) fizyczne zniszczenie.
5. Elektroniczne nośniki danych przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiających ich odczytanie.
6. Kopie zapasowe przechowuje się w zamkniętej szafie w pomieszczeniu, do którego dostęp mają jedynie osoby upoważnione.
7. Elektroniczne nośniki danych zawierające dane osobowe przechowuje się w zamkniętej szafie w obszarze przetwarzania.
8. Kopie zapasowe oraz elektroniczne nośniki danych zawierające dane osobowe usuwa się niezwłocznie po ustaniu ich użyteczności, chyba że przepisy szczegółowe stanowią o ich dłuższym przechowywaniu.

Rozdział 6
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 6

1. Systemy informatyczne chronione są przed działaniem wirusów komputerowych aktualnym, licencjonowanym oprogramowaniem antywirusowym, zainstalowanym przez administratora systemu na serwerach, stacjach roboczych oraz komputerach przenośnych.

2. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad pracą systemu i zasobami danych osobowych na serwerach i stacjach roboczych, poprzez skanowanie dysków.
3. W przypadku wystąpienia wirusów powinno się stosować do zaleceń programu antywirusowego.
4. Oprogramowanie antywirusowe powinno aktualizować się o nową wersję bazy wirusów, zgodnie z instrukcją producenta.
5. Elektroniczne nośniki danych i ich zawartość podlegają kontroli antywirusowej przeprowadzanej każdorazowo przed ich użyciem w stacji roboczej.

Rozdział 7
Wymagania wobec systemu informatycznego przetwarzającego dane osobowe

§ 7

1. Systemy informatyczne powinny rejestrować:
   1) identyfikator osoby upoważnionej, przetwarzającej dane osobowe w systemie i przypisywać tę czynności tylko jej;
   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;
2. Systemy informatyczne powinny zapewnić sporządzanie dla każdej osoby, której dane są przetwarzane w systemie informatycznym, raportu zawierającego:
   1) datę pierwszego wprowadzenia danych do systemu;
   2) identyfikator osoby upoważnionej wprowadzającej te dane;
   3) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą;
   4) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione;
   5) dacie i zakresie udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   6) sprzeciwu wobec przetwarzania danych osobowych o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
3. Rejestracja, o której mowa w ust. 1 następuje przez automatyczny zapis w systemie.
4. Raport, o którym mowa w ust. 2 musi być zrozumiały dla przeciętnego odbiorcy, czyli powinien prezentować informacje w pełnym brzmieniu, poprzedzone nazwą opisową danego pola (nie w postaci kodowanej lub skróconej) a raport powinien generować dane tylko i wyłącznie jednej osoby.
5. Systemy służące do przetwarzania danych osobowych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie nie muszą generować raportu, o którym mowa w punkcie 2.

Rozdział 8
Procedury wykonywania przeglądów i konserwacji systemów oraz elektronicznych nośników danych służących do przetwarzania danych osobowych

§ 8

1. Przeglądy i konserwacje systemów informatycznych powinny odbywać się przy zachowaniu pełnej separacji danych osobowych od osób nieupoważnionych do przetwarzania, pod nadzorem administratora systemu lub w obecności osoby upoważnionej.
2. Elektroniczne nośniki danych przeznaczone do przekazania osobie nieupoważnionej pozbawia się wcześniej zapisu danych osobowych w sposób uniemożliwiający odzyskanie danych.
3. Elektroniczne nośniki danych przeznaczone do naprawy pozbawia się wcześniej zapisu danych osobowych lub naprawia się je pod nadzorem osoby upoważnionej.
4. Elektroniczne nośniki danych nie nadające się do dalszego użytkowania należy zniszczyć mechanicznie.

Rozdział 9
Przetwarzanie danych osobowych na komputerach przenośnych

§ 9

1. Decyzję o przetwarzaniu danych osobowych na komputerach przenośnych podejmuje zarządzający zbiorem po konsultacji ryzyka przetwarzania z Dyrektorem IT.
2. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują te same zasady jak przy pracy na komputerach stacjonarnych oraz stosowanie mechanizmów kryptograficznych wobec danych osobowych.
3. Po ustaniu powodu przetwarzania danych osobowych na komputerach przenośnych, dane te należy przenieść na serwer a następnie trwale usunąć z pamięci komputera przenośnego.
4. Osoby upoważnione użytkujące komputer przenośny zawierający dane osobowe zachowują szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania.

Rozdział 10
Zasady zarządzania środkami kryptograficznej ochrony

§ 10

1. Środki kryptograficznej ochrony stosuje się przy:
   1) przesyłaniu danych osobowych metodą teletransmisji siecią publiczną;
   2) przenoszeniu danych na nośnikach danych poza obszar przetwarzania;

3) przetwarzaniu danych za pomocą komputerów przenośnych.
2. Dyrektor IT decyduje o rodzaju zastosowanych środków kryptograficznej ochrony i zapewnia instruktaż z zakresu ich użytkowania.
3. Administrator systemu zarządza:
   1) aplikacjami kryptograficznymi;
   2) generowaniem kluczy kryptograficznych;
   3) wycofywaniem kluczy kryptograficznych.

Rozdział 11
Zasady dostępu do sieci publicznej dla administratora systemu

§ 11

1. 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.
2. 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 osobie upoważnionej: 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.
3. 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.
4. Administrator systemu konfiguruje zabezpieczenia logiczne zapory sieciowej, tak aby 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.

Prezydent Miasta Lublin

dr inż. Adam Wasilewski

Radca Prawny

Anna Bukowska

Prezydent Miasta Lublin

Załącznik nr 3 do Zarządzania nr 755/2009 Prezydenta Miasta Lublin
z dnia 22. października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów (systemów) zastosowanych do przetwarzania tych danych

Uwagi:

1. *W przypadku przetwarzania danych osobowych w zbiorze papierowym, należy wpisać „zbiór papierowy" w 3 kolumnie.*
2. *W przypadku przetwarzania danych osobowych w zbiorze papierowym z użyciem edytora tekstu, należy wpisać jego nazwę.*
3. *Jeden program może przetwarzać dane osobowe zarówno w jednym, jak i wielu zbiorach, lub odwrotnie – kilka różnych programów (systemów)przetwarza dane stanowiące jeden zbiór.*
4. *Nowe pola do wprowadzania – zaznacz wiersz/tabela/wstaw wiersze.*

Lp.	Nazwa zbioru danych osobowych / nr rejestru GIODO	Nazwa programu (systemu) przetwarzającego dane osobowe	Poziom bezpieczeństwa przetwarzania danych osobowych	Imię i nazwisko administratora systemu
1.				
2.				
3.				
4.				
5.				
6.				
7.				

.....

Zarządzający zbiorem

Radca Prawny
Anna Bukowska

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Część A
Wniosek o nadanie upoważnienia

Wnioskuję o nadanie upoważnienia do przetwarzania danych osobowych:

Pani Pan	imię_nazwisko
wydział biuro ssp	wydział
w zbiorze danych osobowych	nazwa_zbioru_danych_osobowych
na czas trwania zatrudnienia, pracy, stażu, praktyki lub innego stosunku prawnego	data_początkowa_i_końcowa_(lub)_na_czas_nieokreślony
zakres upoważnienia	przeglądanie_danych_(lub)_modyfikowanie_danych_(lub)_administrowanie systemem
zakres uprawnień w systemie informatycznym	zakres uprawnień w systemie informatycznym

.....
Zarządzający zbiorem

Część B
Upoważnienie
do przetwarzania danych osobowych Nr ...../...../.....

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.) nadaję upoważnienie do przetwarzania danych osobowych dla:

Pani Pan	imię_nazwisko
wydział biuro ssp	wydział
w zbiorze danych osobowych	nazwa_zbioru_danych_osobowych
na czas trwania zatrudnienia, pracy, stażu, praktyki lub innego stosunku prawnego	data_początkowa_i_końcowa_(lub)_na_czas_nieokreślony
zakres upoważnienia	przeglądanie_danych_(lub)_modyfikowanie_danych_(lub)_administrowanie_systemem
zakres uprawnień w systemie informatycznym	zakres uprawnień w systemie informatycznym

.....
Data – z up. Administratora Danych
Administrator Bezpieczeństwa Informacji

Część C
Oświadczenie osoby upoważnionej do przetwarzania danych osobowych:

Zaznajomiłam/em się z:

1. Polityką bezpieczeństwa;
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 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)

i zobowiązuję się do przetwarzania danych osobowych wyłącznie w zakresie upoważnienia do przetwarzania i przyznanych mi uprawnień w systemie informatycznym oraz do zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia.

.....
Data, czytelny podpis osoby upoważnionej

Część D
Nadanie uprawnień w systemie informatycznym

Nadanie uprawnień w systemie informatycznym, identyfikatora i hasła dla osoby upoważnionej:

Identyfikator - .....

.....
Data – Administrator Systemu

Radca Prawny

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Część A
Wniosek o cofnięcie upoważnienia

Wnioskuję o cofnięcie upoważnienia do przetwarzania danych osobowych:

Pani Pan	imię_nazwisko
wydział biuro ssp	wydział
w zbiorze danych osobowych	nazwa_zbioru_danych_osobowych
na czas trwania zatrudnienia, pracy, stażu, praktyki lub innego stosunku prawnego	data_początkowa_i_końcowa_(lub)_na_czas_nieokreślony
zakres upoważnienia	przeglądanie_danych_(lub)_modyfikowanie_danych_(lub)_administrowanie systemem
zakres uprawnień w systemie informatycznym	zakres uprawnień w systemie informatycznym

.....
Zarządzający zbiorem

Część B
Cofnięcie upoważnienia
do przetwarzania danych osobowych Nr ...../...../.....

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.) cofam upoważnienie do przetwarzania danych osobowych dla:

Pani Pan	imię_nazwisko
wydział biuro ssp	wydział
w zbiorze danych osobowych	nazwa_zbioru_danych_osobowych
na czas trwania zatrudnienia, pracy, stażu, praktyki lub innego stosunku prawnego	data_początkowa_i_końcowa_(lub)_na_czas_nieokreślony
zakres upoważnienia	przeglądanie_danych_(lub)_modyfikowanie_danych_(lub)_administrowanie_ systemem
zakres uprawnień w systemie informatycznym	zakres uprawnień w systemie informatycznym

.....
Data – z up. Administratora Danych
Administrator Bezpieczeństwa Informacji

Część C
Cofnięcie uprawnień w systemie informatycznym

Wycofano uprawnienia w systemie informatycznym oraz identyfikator i hasło.

.....
Data – Administrator Systemu

Radca Prawny

Prezydent Miasta Lublin

Załącznik nr 6 do Zarządzania nr 255/2009 Prezydenta Miasta Lublin
z dnia 22 października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Nazwa_zbioru_danych_osobowych
Ewidencja osób upoważnionych do przetwarzania danych osobowych

Uwagi:

1. ***Nowe pola do wprowadzania – zaznacz wiersz/tabela/wstaw wiersze.***

Lp.	Nazwisko i imię Wydział	Zakres upoważnienia: przeglądanie danych/modyfikowanie danych/ administrowanie systemem *(wpisać właściwe)*	Data nadania upoważnienia	Identyfikator	Data ustania upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					

.....

Zarządzający zbiorem

Radca Prawny
Anna Bukowska

Prezydent Miasta Lublin

Załącznik nr 7 do Zarządzania nr 235/2009 Prezydenta Miasta Lublin
z dnia 22 października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Nazwa_zbioru_danych_osobowych
Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe w zbiorze

Uwagi:

1. *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, pomieszczenia archiwum czy szafy z komputerowymi nośnikami informacji, pomieszczenia serwerowni, oraz np. sejf bankowy, jeżeli jest to miejsce przechowywania danych osobowych.*
2. *Nowe pola do wprowadzania – zaznacz wiersz/tabela/wstaw wiersze.*

Lp.	Wydział / Adres	Piętro	Nr pokoju
1.			
2.			
3.			
4.			
5.			
6.			

.....

Zarządzający zbiorem

Radca Prawny
Anna Rukowicz

Prezydent Miasta Lublin

Załącznik nr 8 do Zarządzania nr 1257/2009 Prezydenta Miasta Lublin
z dnia 22. października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Nazwa_zbioru_danych_osobowych
Opis struktury zbioru wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Uwagi:

1. *Należy wskazać i nazwać poszczególne grupy informacji (zakresy) i odpowiadające im opisy poszczególnych pól informacyjnych oraz zaznaczyć pogrubioną czcionką ewentualnie istniejące miedzy nimi relacje, celem wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą, identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w zbiorze, np.:*
   - *zakres nr 1 dane adresowe klienta – zawartość pól informacyjnych: **identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/nr mieszkania)*
   - *zakres nr 2 zamówienia klienta – zawartość pól informacyjnych: identyfikator zamówienia, **identyfikator klienta, identyfikator towaru**, ilość towaru, wartość zamówienia, data zamówienia, data odbioru*
   - *zakres nr 3 sprzedawane towary – zawartość pól informacyjnych: **identyfikator towaru**, nazwa towaru, nazwa producenta, data produkcji.*

   W przykładzie, relacje zaznaczone pogrubioną czcionką, wskazują, że faktyczny zakres przetwarzanych o osobie (kliencie) danych wykazanych w zakresie nr 1 powiększa się o dane z zakresu 3 i 2: imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/nr mieszkania), nazwa towaru, nazwa producenta, data produkcji, ilość towaru, wartość zamówienia, data zamówienia, data odbioru.
2. *Nowe pola do wprowadzania – zaznacz wiersz/tabela/wstaw wiersze.*

Zakres	Nazwa zakresu	Zawartość poszczególnych pól informacyjnych
1.		
2.		
3.		
4.		
5.		
6.		
7.		

.....

Zarządzający zbiorem

Radca Prawny
Anna Bukowska

Prezydent Miasta Lublin

Załącznik nr 9 do Zarządzania nr 255/2009 Prezydenta Miasta Lublin
z dnia 22. października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Nazwa_zbioru_danych_osobowych
Opis przepływu danych z lub do systemu informatycznego obsługującego zbór danych o nazwie

Uwagi:

1. *Opis zawiera relacje pomiędzy danymi w różnych zbiorach poprzez przedstawienie współpracy różnych systemów informatycznych te zbiory obsługujących:*
   - *kierunek przepływu danych ze zbioru do zbioru;*
   - *zakres danych osobowych: imię, nazwisko, kod pocztowy, miejscowość itd.;*
   - *przepływ informacji: jednokierunkowy – informacje tylko do odczytu lub dwukierunkowy – informacje do odczytu i zapisu;*
     sposób przepływu: manualny – przy wykorzystaniu zewnętrznych nośników danych lub półautomatyczny – za pomocą teletransmisji w określonych odstępach czasu lub automatycznie.
2. *Nowe pola do wprowadzania – zaznacz wiersz/tabela/wstaw wiersze.*

Lp.	Kierunek przepływu danych osobowych		Zakres danych osobowych *(imię, nazwisko, kod pocztowy, miejscowość, itd),*	Przepływ informacji *(jednokierunkowy dwukierunkowy)*	Sposób przepływu *(manualny, półautomatyczny, automatyczny)*
	ze zbioru *(nazwa zbioru)*	do zbioru *(nazwa zbioru)*			
1.					
2.					
3.					
4.					
5.					

.....

Zarządzający zbiorem

Radca Prawny
Anna Bukowska

Umowa powierzenia przetwarzania danych osobowych

zawarta w Lublinie w dniu dd.mm.rrrr roku pomiędzy

Gminą Lublin

reprezentowaną przez:

imię_i_nazwisko stanowisko
imię_i_nazwisko stanowisko

zwaną dalej **Zleceniodawcą**

a

Firmą nazwa_firmy
z siedzibą w nazwa_miejscowości ul. adres_firmy
NIP NIP
REGON REGON

imię_i_nazwisko stanowisko

zwaną dalej **Zleceniobiorcą**.

§ nn

1. Zleceniodawca oświadcza, że powierza Zleceniobiorcy a Zleceniobiorca oświadcza, że wyraża zgodę na przetwarzanie danych osobowych zawartych w zbiorze danych osobowych o nazwie nazwa_zbioru .
2. Umowa powierzenia zostaje zawarta na okres czas trwania umowy .
3. Dane osobowe będą przetwarzane w celu cel_przetwarzania .
4. Zakres przetwarzanych danych obejmuje następujące kategorie danych: kategorie_danych_osobowych .

§ nn

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

BY

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).

2. Zleceniobiorca po zakończeniu umowy o powierzenie przetwarzania danych osobowych zobowiązuje się przekazać Zleceniodawcy wszystkie przetwarzane dane osobowe oraz trwale usunąć je ze swojego systemu informatycznego lub innych nośników.
3. Zleceniobiorca odpowiada za wszelkie szkody wyrządzone osobom trzecim, które powstały w związku z nienależytym przetwarzaniem powierzonych do przetwarzania danych osobowych.

§ nn

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

Radca Prawny

Anna Bukowska

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r.

Nazwa_zbioru_danych_osobowych

Raport z naruszenia bezpieczeństwa przetwarzania danych osobowych

1. Data: data dd.mm.rrrr Godzina: godzina gg.mm
2. Imię i nazwisko / stanowisko / wydział osoby powiadamiającej o zaistniałym zdarzeniu:
   imię_i_nazwisko_/_wydział
3. Rodzaj naruszenia bezpieczeństwa przetwarzania danych osobowych i okoliczności towarzyszące:
   rodzaj_naruszenia_bezpieczeństwa_i_okoliczności_towarzyszące
4. Przyczyny wystąpienia zdarzenia:
   przyczyny_wystąpienia_zdarzenia
5. Podjęte działania:
   podjęte_działania
6. Postępowanie wyjaśniające:
   postępowanie_wyjaśniające
7. Uwagi:
   uwagi

.....
podpis Administratora Bezpieczeństwa Informacji

10. Decyzja co do dalszego postępowania:
    decyzja_co_do_dalszego_postępowania

.....
podpis Administratora Danych

Radca Prawny

Prezydent Miasta Lublin

Załącznik nr 12 do Zarządzania nr 255/2009 Prezydenta Miasta Lublin
z dnia 22.. października 2009 r.

KO.SP.5241-nn/09

Lublin, dnia dd.mm.2009 r

Nazwa_zbioru_danych_osobowych

Kwestionariusz kontroli bezpieczeństwa danych osobowych

Informacje ogólne		
1.	Imię i nazwisko zarządzającego zbiorem	
2.	Nazwa zbioru danych osobowych	
3.	Nazwa systemu informatycznego przetwarzającego dane osobowe	
4.	Adres, piętro, nr pokoju	
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			

BM

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 wygaśnięcie czasu obowiązywania hasła dostępu do stacji roboczej			
24.	System informatyczny umożliwia sporządzenie 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 zapasowe			
35.	Nośniki z kopiami zapasowymi są przechowywane w zamkniętych szafach			
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 pracownika upoważnionego			
40.	Dokumenty zawierające dane osobowe przechowuje się w zamykanych szafach, do których klucze znajdują się w ustalonym miejscu			
41.	Robocze wydruki danych osobowych po wykorzystaniu są niszczone			
42.	Dokumenty zawierające dane osobowe transportuje się w bezpiecznych kopertach			
43.	Klucze do pomieszczeń w obszarze przetwarzania są pobierane i deponowane na portierni			

IBG

44.	Pomieszczenia serwerowni są prawidłowo zabezpieczone			
45.	Stanowiska komputerowe mają prawidłowo ustawione ekrany monitorów			
46.	Ekrany komputerów są wyposażone w wygaszacze włączające się automatycznie po upływie ustalonego czasu nieaktywności			
47.	Do kwestionariusza dołącza się (stanowiące jego integralną część) załączniki, jak dodatkowe protokóły, ekspertyzy, dowody, itp.			
48.	Dodatkowe spostrzeżenia			
49.	Uwagi zarządzającego zbiorem			
50.	Zarządzający zbiorem został powiadomiony o prawie zgłoszenia zastrzeżeń do faktów ujętych w kwestionariuszu i złożenia wyjaśnień			
51.	Jeżeli zarządzający zbiorem odmawia podpisania kwestionariusza, obowiązany jest złożyć pisemne wyjaśnienie o przyczynach tej odmowy, stanowiące załącznik do kwestionariusza			
52.	Zalecenia pokontrolne wraz z terminami ich realizacji zostaną przedstawione w ciągu 5 dni roboczych, odrębnym pismem, podpisanym przez Administratora danych			
53.	Kwestionariusz sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden otrzymuje zarządzający zbiorem, drugi kontrolujący			
54.	Kontrolę przeprowadził:			
55.	Lublin, dnia			

.....
Kontrolujący

.....
Zarządzający zbiorem

Radca Prawny