KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik nr. 1 do Zarządzania NR 54/2015
Burmistrza Miasta i Gminy Chmielnik
Z dnia 30 marca 2015 roku

Polityka Bezpieczeństwa

Polityka Bezpieczeństwa Przetwarzana Danych Osobowych Urzędu Miasta i Gminy w Chmielniku

Projekt „e-Urząd – satysfakcja, komfort i wygoda dla Mieszkańców" współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

Urząd Miasta i Gminy
Chmielnik

• • •

• • •

26-020 Chmielnik

Plac Kościuszki 7

Powiat Kielecki

Województwo
Świętokrzyskie

• • •

www.chmielnik.com

umig@chmielnik.com

Wstęp

Celem polityki bezpieczeństwa przetwarzania danych w tym danych osobowych jest zabezpieczenie przetwarzania informacji stanowiących dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.). oraz realizacja § 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. z 2004 r. Nr 100, poz. 1024)

Spis treści

Wstęp 1

1. Definicje 4
2. Zakres stosowania Polityki Bezpieczeństwa Przetwarzania Danych Osobowych 8
3. Podstawa prawna 8
4. Struktura dokumentów Polityki Bezpieczeństwa Przetwarzania Danych Osobowych 9
5. Zakres rozpowszechniania 10
6. Obowiązki Administratora Danych Osobowych 10
7. Powołanie, rejestracja, zmiana i odwołanie Administratora Bezpieczeństwa Informacji. 11
8. Administrator Bezpieczeństwa Informacji 13
9. Administrator Systemów Informatycznych 16
10. Osoby odpowiedzialne za przetwarzanie danych osobowych 18
11. Podstawowe zasady ochrony danych osobowych 19
12. Upoważnienia do przetwarzania danych osobowych 20
13. Powierzenie przetwarzania danych osobowych 21
14. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. 22
15. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. 22
16. Opis struktury zbiorów 22
17. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami. 23
18. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. 23

Środki ochrony fizycznej 23

Środki sprzętowe, informatyczne i telekomunikacyjne 24

Środki ochrony w ramach oprogramowania systemu 24

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych 24

Środki organizacyjne 24

19. Archiwizowanie informacji zawierających dane osobowe 25
20. Instrukcja alarmowa w przypadku wystąpienia zagrożenia lub incydentu naruszającego ochronę danych osobowych 25
21. Działania korygujące i zapobiegawcze 27
22. Przepisy karne i porządkowe 28
23. Postanowienia końcowe 29
24. Dokumentacja powiązana ..... **Błąd! Nie zdefiniowano zakładki.**
25. Spis wzorów dokumentów 29

1. Definicje

Ilekroć w niniejszej Polityce Bezpieczeństwa Przetwarzania Danych Osobowych mowa o:

1) **komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały i komórki organizacyjne, o których mowa w § 17 Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Chmielniku stanowiącego załącznik do zarządzenia nr 47/2015 Burmistrza Miasta i Gminy Chmielnik z dnia 11 marca 2015 r.

2) **Kierowniku komórki organizacyjnej** – rozumie się przez to kierownika wydziału, referatu, biura, koordynatora i samodzielne stanowiska pracy;

3) **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych jest Burmistrz Miasta i Gminy Chmielnik;

4) **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to pracownika Urzędu Miasta i Gminy wyznaczonego przez Administratora Danych Osobowych, nadzorującego przestrzeganie zasad, o których mowa w art. 36 ust. 1 u.o.d.o.;

5) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika Urzędu Miasta i Gminy, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

6) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu Miasta i Gminy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

7) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;

8) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym Urzędu Miasta i Gminy;

9) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na

numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

10) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

11) **Przetwarzaniu danych osobowych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

12) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

13) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

14) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

15) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

16) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;

17) **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:

    a) osoby, której dane dotyczą,

    b) osoby upoważnionej do przetwarzania danych osobowych,

    c) przedstawiciela, o którym mowa w art. 31a u.o.d.o.,

d) podmiotu, o którym mowa w art. 31 u.o.d.o.,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

18) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

19) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

20) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego Urzędu Miasta i Gminy;

21) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;

22) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

23) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

24) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

25) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło

26) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym Urzędu Miasta i Gminy;

27) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;

28) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w Urzędzie Miasta i Gminy;

29) **Sieć publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 ust. 22 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852 z późn. zm.);

30) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym Urzędu Miasta i Gminy;

31) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej Urzędu Miasta i Gminy;

32) **Incydent** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;

33) **Zagrożenie** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

34) **Działa korygujące** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

35) **Działania zapobiegawcze** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

2. Zakres stosowania Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

Zakresy określone przez Politykę Bezpieczeństwa Danych Osobowych mają zastosowanie do całego systemu informacyjnego Urzędu Miasta i Gminy w Chmielniku, a w szczególności do:

1) wszelkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów prowadzonych w formie tradycyjnej, w których przetwarzane są dane osobowe;

2) informacji zawierających dane osobowe, których Administratorem Danych Osobowych jest Burmistrz Miasta i Gminy Chmielnik lub przetwarzanych w celu realizacji zadań zleconych Miastu i Gminie, a których administratorem są organy centralne administracji rządowej lub samorządowej;

3) wszystkich nośników magnetycznych, optycznych lub papierowych, na których są lub będą znajdować się informacje zawierające dane osobowe;

4) wszystkich obszarów (budynki, pomieszczenia, części pomieszczeń), w których są lub będą przetwarzane dane osobowe;

5) wszystkich pracowników Urzędu Miasta i Gminy w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów, wolontariuszy a także innych podmiotów lub osób fizycznych, które współuczestniczą w procesie przetwarzania danych osobowych.

3. Podstawa prawna

Polityka Bezpieczeństwa Danych Osobowych odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w:

1) ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.)

2) rozporządzeniu 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 2004r., Nr 100, poz. 1024);

3) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229 poz. 1536);

4) ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (t.j. Dz. U. 2013 poz. 262);

5) ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. 2013 poz. 1422);

6) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 nr 10 poz. 68);

7) rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526 ze zm.)

8) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. z 2006 r., Nr 206, poz. 1517);

9) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. z 2006 r., Nr 206, poz. 1518);

10) rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. z 2002 r., Nr 167, poz. 1375).

4. Struktura dokumentów Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

Zestaw dokumentacji Polityki Bezpieczeństwa Przetwarzania Danych Osobowych składa się z:

1) Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miasta i Gminy Chmielnik.

2) Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

3) Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

4) Opisu struktury zbiorów danych osobowych;

5) Opisu sposobu przepływu danych pomiędzy poszczególnymi systemami;

6) Określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;

7) Wzorów formularzy pomocniczych.

Wyżej wymienione dokumenty będą prowadzone w formie odrębnej dokumentacji, przez Administratora Bezpieczeństwa Informacji na podstawie wzorów stanowiących załączniki do niniejszej Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.

5. Zakres rozpowszechniania

Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie osoby posiadające dostęp do danych osobowych na podstawie nadanych upoważnień przez Administratora Danych Osobowych.

Dokument ten może być także udostępniany partnerom przetwarzającym dane osobowe Urzędu, z którym Urząd Miasta i Gminy Chmielnik związany jest odpowiednimi umowami.

6. Obowiązki Administratora Danych Osobowych

Do podstawowych obowiązków Administratora Danych Osobowych należy:

1) przetwarzanie danych osobowych zgodnie z prawem;

2) dopełnienie obowiązku zgłoszenia zbiorów danych osobowych do rejestracji GIODO, za wyjątkiem przypadków określonych w art. 43 ustawy. Obowiązkowi rejestracji zbiorów danych osobowych z wyjątkiem zbiorów zawierających dane wrażliwe nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi Ochrony Danych osobowych do rejestracji.

3) dopełnienie obowiązku informacyjnego ustanowionego w art. 24 ust. 1 oraz art. 25 ust. 1 u.o.d.o.;

4) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą;

5) respektowanie prawa osób, których dane dotyczą;

6) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,

zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

7) wydawanie i odbieranie upoważnień do przetwarzania danych;

8) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;

9) podejmowanie działań w przypadku wykrycia naruszeń w systemie bezpieczeństwa danych osobowych;

10) kontrolowanie, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;

11) udzielanie informacji o zakresie przetwarzanych danych osobowych;

12) spełnienie obowiązku uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;

13) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych.

7. Powołanie, rejestracja, zmiana i odwołanie Administratora Bezpieczeństwa Informacji.

1) Administrator Danych Osobowych może powołać administratora bezpieczeństwa informacji (**Załącznik Nr 1**).,

2) Administratorem Bezpieczeństwa Informacji może być osoba, która:

2.1) ma pełną zdolność do czynności prawnych oraz korzystania z pełni praw publicznych,

2.2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,

2.3) nie była karana za umyślne przestępstwo.

3) Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

4) Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:

4.1) oznaczenie administratora danych i adres jego siedziby lub zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;

4.2) dane administratora bezpieczeństwa informacji:

a) imię i nazwisko,

b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,

c) adres do korespondencji, jeżeli jest inny niż adres o którym mowa w pkt.4.1),

4.3) datę powołania,

4.4) oświadczenie administratora danych o spełnieniu przez administratora bezpieczeństwa informacji warunków określonych w pkt 2).

5) Wzory zgłoszeń powołania, zmiany informacji objętych zgłoszeniem i odwołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, określają załączniki do Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).

6) Administrator danych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w pkt 4), w terminie do 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.

7) Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań określonych w pkt. 8. Administrator Bezpieczeństwa Informacji.

8) Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w pkt. 2).

9) Administrator Bezpieczeństwa Informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem Danych.

10) W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w pkt. 8. Administrator Bezpieczeństwa Informacji, z wyłączeniem obowiązku sporządzenia sprawozdania, wykonuje administrator danych.

8. Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1) prowadzenie dokumentacji dotyczącej bezpieczeństwa danych osobowych;
2) prowadzenie i nadzorowanie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
3) prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów o których mowa w art. 43 ust. 1,
4) opracowanie sprawozdania z sprawdzenia wykonywanego na wniosek Generalnego Inspektora u administratora danych, który go powołał. Zawartość sprawozdania określa art. 36c. u.o.d.o.;
5) prowadzenie ewidencji zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy;
6) prowadzenie wykazu obszarów przetwarzania danych osobowych w Urzędzie Miasta i Gminy;
7) wydawanie i odbieranie upoważnień do przetwarzania danych;
8) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
9) sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miasta i Gminy w Chmielniku;
10) sprawowanie nadzoru nad fizycznym zabezpieczeniem obszarów przetwarzania danych osobowych oraz kontrolę przebywających w nich osób;
11) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
12) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;

13) sprawowanie nadzoru nad instalacjami i konfiguracjami oprogramowania systemowego, sieciowego oraz bazodanowego;

14) sprawowanie nadzoru nad profilaktyką antywirusową;

15) sprawowanie nadzoru w zakresie wykonywanych kopii zapasowych danych osobowych;

16) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;

17) sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych Urzędu Miasta i Gminy oraz kontrolę dostępu do danych;

18) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone mogą być dane osobowe przetwarzane w Urzędzie Miasta i Gminy;

19) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych;

20) przeprowadzanie kontroli w zakresie ochrony danych osobowych;

21) określanie potrzeb w zakresie zabezpieczenia danych osobowych ;

22) aktualizacje jawnego rejestru zbiorów danych osobowych przetwarzanych przez Urząd Miasta i Gminy;

23) podejmowanie odpowiednich działań w przypadkach naruszenia bezpieczeństwa danych osobowych;

24) prowadzenie rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;

25) zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń wnioskowanych i obowiązujących w Urzędzie Miasta i Gminy;

26) dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur;

27) umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;

28) sprawowanie nadzoru nad procesem przyznawania praw dostępu;

29) organizowanie szkoleń z zakresu ochrony danych osobowych;

30) opiniowanie zakupów nowych systemów informatycznych;

31) opiniowanie wzorów dokumentów i umów;

32) nadzorowanie Administratora Systemów Informatycznych;

33) nadzorowanie osób upoważnionych do przetwarzania danych osobowych;

34) prowadzenie aktualnego wykazu zbiorów danych osobowych;

35) prowadzenie metryczek zbiorów danych osobowych;

36) zapewnienie, aby dane osobowe prowadzone zbiorach były:

   a) przetwarzane zgodnie z prawem,

   b) zbierane dla oznaczonych i zgodnych z prawem celów,

   c) merytorycznie poprawne i adekwatne w stosunku do celu w jakich są przetwarzane,

   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą;

37) przygotowywanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych;

38) prowadzenie aktualnego wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;

39) zapewnienie poufności, integralności i rozliczalności danych osobowych;

40) określenie indywidualnych obowiązków i odpowiedzialności osób upoważnionych do przetwarzania danych osobowych;

41) sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi;

42) zapewnienie szkoleń osobom, które będą dopuszczone do przetwarzania danych osobowych;

43) dopuszczanie do przetwarzania danych osobowych wyłącznie osób upoważnionych do przetwarzania danych osobowych;

44) sprawowanie nadzoru nad właściwym eksploatowaniem systemów informatycznych;

45) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;

9. Administrator Systemów Informatycznych

Administrator Systemów Informatycznych odpowiedzialny jest za:

1) bieżący nadzór oraz zapewnienie ciągłości działania systemów informatycznych;

2) optymalizację wydajności systemów informatycznych;

3) zabezpieczenie systemów informatycznych;

4) zarządzanie konfiguracją systemów i urządzeń wchodzących w skład systemu informatycznego;

5) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych w systemach informatycznych;

6) dokonywanie okresowej analizy ryzyka dla poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;

7) prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe;

8) przyznawanie na wniosek Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do systemów informatycznych;

9) współpracę z dostawcami aplikacji i sprzętu komputerowego w tym sieciowego i serwerowego;

10) wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń;

11) opracowywanie procedur dotyczących bezpieczeństwa i standardów zabezpieczeń w systemach informatycznych;

12) udostępnianie danych zgromadzonych w systemach informatycznych na wniosek Administratora Danych Osobowych oraz za zgodą Administratora Bezpieczeństwa Informacji;

13) bieżące wykonywanie kopii systemowych jak i kopii baz danych i aplikacji wykorzystywanych do przetwarzania danych osobowych;

14) świadczenie wsparcia technicznego w ramach oprogramowania oraz serwis sprzętu komputerowego wchodzącego w skład systemów informatycznych Urzędu Miasta i Gminy;

15) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz utrzymywanie kontaktu z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego;

16) prowadzenie dokumentacji dotyczącej opisu struktury zbiorów danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;

17) prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;

18) prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych;

umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;

19) sprawowanie nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;

20) wykonywanie napraw oraz konserwacji systemów informatycznych a także likwidację urządzeń komputerowych oraz elektronicznych nośników zawierających dane osobowe;

21) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;

22) sprawowanie nadzoru nad profilaktyką antywirusową;

23) zapewnienie szkoleń Pracowników Urzędu w zakresie prawidłowego korzystania z aplikacji i urządzeń wchodzących w skład systemów informatycznych służących do przetwarzania danych osobowych;

24) opiniowanie zakupów dotyczących urządzeń sieciowych i serwerowych;

25) opiniowanie zakupów dotyczących oprogramowania sieciowego, serwerowego oraz narzędziowego;

10. Osoby odpowiedzialne za przetwarzanie danych osobowych

Osoby upoważnione do przetwarzania danych osobowych odpowiedzialne są za:

1) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miasta i Gminy w Chmielniku;
2) stosowanie się do zaleceń Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych w zakresie ich kompetencji;
3) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
4) niezwłoczne informowanie Administratora Bezpieczeństwa Informacji o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta i Gminy;
5) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
6) korzystanie z systemów informatycznych Urzędu Miasta i Gminy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
7) zachowanie w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji;
8) wszelkie operacje wykonywane w systemach informatycznych przy użyciu ich identyfikatora oraz hasła;
9) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

11. Podstawowe zasady ochrony danych osobowych

1) Wszystkie dane osobowe w Urzędzie Miasta i Gminy w Chmielniku należy przetwarzać zgodnie z obowiązującymi przepisami prawa;
2) W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów u.o.d.o.;
3) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami;
4) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane;
5) Przetwarzane dane osobowe należy przechowywać w postaci umożliwiającej identyfikację osób, których te dane dotyczą;
6) Dane osobowe w Urzędzie Miasta i Gminy można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania;
7) Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w Urzędzie Miasta i Gminy;
8) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem;
9) Przetwarzanie danych osobowych w Urzędzie Miasta i Gminy może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;
10) W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych;
11) Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

12. Upoważnienia do przetwarzania danych osobowych

Do przetwarzania danych osobowych oraz obsługi zbiorów informatycznych zawierających te dane mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Bezpieczeństwa Informacji z upoważnienia Administratora Danych Osobowych. Upoważnienie wydaje się na wniosek Kierownika Komórki Organizacyjnej, osobie która złożyła stosowne oświadczenie dot. właściwej realizacji przepisów u.o.d.o.

Upoważnienie powinno mieć charakter imienny. Powinno też określać dozwolony okres i zakres przetwarzania danych. Upoważnienia mogą być wydawane bezterminowo (wynikające z treści umowy o pracę) lub na czas określony.

Procedura nadawania upoważnienia do przetwarzania danych osobowych:

1) W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Kierownik Komórki Organizacyjnej zobowiązany jest zwrócić się do Administratora Bezpieczeństwa Informacji na wniosku (wzór wniosku stanowi **Załącznik Nr 2**) o wydanie upoważnienia do przetwarzania danych osobowych.

2) W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, przełożony lub osoba pełniąca samodzielne stanowisko zobowiązani są bezzwłocznie skierować wniosek (wzór wniosku stanowi **Załącznik Nr 2**) do Administratora Bezpieczeństwa Informacji o wydanie lub cofnięcie upoważnienia.

3) Nowy pracownik podpisuje oświadczenie (wzór oświadczenia stanowi **Załącznik Nr 3**) dot. właściwej realizacji przepisów u.o.d.o.

3) Administrator Danych Osobowych wydaje upoważnienie (wzór upoważnienia stanowi **Załącznik Nr 4**) do przetwarzania danych osobowych po spełnieniu procedury określonej w ust. 1 i 2 oraz 3.

4) Rozwiązanie stosunku pracy powoduje wygaśnięcie upoważnienia.

5. Ewidencję pracowników, upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji (wzór ewidencji stanowi **Załącznik Nr 5**).

13. Powierzenie przetwarzania danych osobowych

Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.

W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:

a) cel i zakres przetwarzania danych osobowych;

b) obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych;

c) konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy;

d) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

W umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie, których dochodzi do wymiany informacji uwzględni należy następujące elementy:

a) definicje informacji, która ma być chroniona;

b) spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy;

c) odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji;

d) własność informacji;

e) dozwolone użycie danych osobowych oraz praw sygnatariusza do jej użycia;

f) prawa do audytu i monitorowania działań związanych z ochrona danych osobowych;

g) proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych;

h) wymagane działania w momencie zakończenia umowy, np.: zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.

Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

14. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji opisującej obszar przetwarzania danych osobowych w siedzibie Urzędu Miasta i Gminy w Chmielniku który stanowią pomieszczenia, w których przetwarzane są dane osobowe z użyciem sprzętu komputerowego lub w formie kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych.

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Chmielniku, prowadzona jest zgodnie ze wzorcem (wzór wykazu stanowi **Załącznik Nr 6**).

15. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miasta i Gminy w Chmielniku, prowadzona jest zgodnie ze wzorem (wzór wykazu stanowi **Załącznik Nr 7)**.

Wykaz zbiorów prowadzony jest zarówno w formie papierowej jak i elektronicznej.

16. Opis struktury zbiorów

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Chmielniku. Dokumentacja opracowana została w oparciu o materiały dostarczone przez producentów oprogramowania i prowadzona jest w konsultacji z Administratorem Systemów

Informatycznych. Dokumentacja prowadzona jest zgodnie ze wzorem (wzór opisu stanowi **Załącznik Nr 8**).

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miasta i Gminy w Chmielniku. Prowadzona jest zarówno w formie papierowej jak i elektronicznej.

17. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

Administrator Systemów Informatycznych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami. Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miasta i Gminy w Chmielniku. Dokumentacja prowadzona jest zarówno w formie papierowej jak i elektronicznej. Wszelkie zmiany ww. dokumencie są opiniowane i zatwierdzane przez Administratora Bezpieczeństwa Informacji.

18. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Środki ochrony fizycznej

- obszar, w którym przetwarzane są dane osobowe po godzinach pracy urzędu chroniony jest alarmem;
- obszar, w którym przetwarzane są dane osobowe całodobowo jest monitorowany wizyjnie z miesięczną rejestracją oraz jest nadzorowany przez pracowników ochrony;
- wszystkie pomieszczenia w których przetwarzane są dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy;
- przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych jest możliwy tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności naczelnika wydziału.
- Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze do szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych;
- Ustawianie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.

Środki sprzętowe, informatyczne i telekomunikacyjne

- Nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
- sieć lokalna jest podłączona do Internetu za pomocą komputera spełniającego funkcję Servera Proxy oraz Firewalla;
- wszystkie stanowiska komputerowe wyposażone są w indywidualną ochronę antywirusową;
- wszystkie stanowiska komputerowe oraz serwery są chronione przed zanikiem zasilania przez stosowanie zasilaczy zapasowych UPS;
- kopie awaryjne wykonuje się na płytach DVD-R, zapisuje się je również na serwerze plików,
- każdy komputer zabezpieczony jest przez indywidualny identyfikator użytkownika i cyklicznie zmieniane hasło;
- podłączenie urządzenia końcowego (komputera, drukarki) do sieci lokalnej dokonywane jest przez Administratora Systemu Informatycznego.

Środki ochrony w ramach oprogramowania systemu

- ile istnieje taka możliwość, w systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę hasła dostępu do systemu;
- ile istnieje taka możliwość, zastosowano identyfikator i hasło dostępu na poziomie aplikacji;
- konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych jedynie za pośrednictwem aplikacji;
- system informatyczny pozwala zdefiniować odpowiednie prawa do zasobów informatycznych systemu.

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji;
- dla każdego użytkownika systemu nadawany jest odrębny identyfikator;

Środki organizacyjne

- wyznaczono Administratora Bezpieczeństwa Informacji,
- osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
- ustalono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
- zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych;
- zapoznano i zobowiązano na piśmie pracowników urzędu do przestrzegania przepisów i zasad związanych z bezpieczeństwem przetwarzania danych osobowych.

19. Archiwizowanie informacji zawierających dane osobowe

Zasady archiwizowania informacji zawierających dane osobowe w Urzędzie Miasta i Gminy w Chmielniku regulują następujące przepisy:

1) Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2011 nr 123 poz. 698)
2) Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacja , zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U. 2002 nr 167 poz. 1375)
3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych (Dz. U. Nr 206, poz. 1519);
4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. Nr 206, poz. 1518);
5) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. Nr 206, poz. 1517);

20. Instrukcja alarmowa w przypadku wystąpienia zagrożenia lub incydentu naruszającego ochronę danych osobowych

Celem Instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń oraz występowania incydentów w przyszłości. Poniższe zasady postępowania mają zastosowanie zarówno w przypadku danych osobowych przetwarzanych w formie tradycyjnej (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych) jak i w systemach informatycznych Urzędu Miasta i Gminy.

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) brak lub niewłaściwe zabezpieczenia fizyczne pomieszczeń, urządzeń i dokumentów;

2) brak lub niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych;

3) niestosowanie zasad ochrony danych osobowych przez osoby upoważnione w tym:

   a) nieprzestrzeganie zasad czystego biurka i ekranu,
   b) ochrony haseł,

c) niezamykanie pomieszczeń, szafek, biurek itp.

Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne:
   - pożar obiektu lub pomieszczenia,
   - zalanie wodą,
   - utrata zasilania,
   - utrata łączności itp.;

b) zdarzenia losowe wewnętrzne
   - awarie sprzętu komputerowego lub oprogramowania,
   - pomyłki Administratora Systemów Informatycznych lub osób upoważnionych,
   - utrata/zagubienie nośników zawierających dane osobowe itp.;

c) umyślne incydenty:
   - nieuprawniony dostęp do systemów informatycznych lub pomieszczeń (włamanie),
   - wyciek danych osobowych,
   - ujawnienie danych osobowych osobom nieupoważnionym,
   - działanie wirusów lub innego szkodliwego oprogramowania,
   - świadome zniszczenie danych,
   - kradzież danych itp.

Przed przystąpieniem do pracy osoby upoważnione zobowiązane są do zwrócenia szczególnej uwagi, czy nie zaszły okoliczności wskazujące na wystąpienie zagrożenia lub incydentu naruszającego ochronę danych osobowych.

W przypadku stwierdzenia zagrożenia lub incydentu naruszenia ochrony danych osobowych, należy niezwłocznie poinformować o tym fakcie Administratora Bezpieczeństwa Informacji. W sytuacji braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji należy powiadomić Sekretarza Gminy.

Informację o pojawieniu się zagrożenia lub incydentu należy przekazać osobiście lub telefonicznie. Informacja ta powinna zawierać imię i nazwisko osoby zgłaszającej, miejsce i czas wystąpienia zagrożenia lub incydentu oraz krótki opis sytuacji. Osoba zgłaszająca wystąpienie zagrożenia lub incydentu może zostać poproszona o potwierdzenie zgłoszenia na piśmie.

Do czasu przybycia Administratora Bezpieczeństwa Informacji lub Sekretarza Gminy, zgłaszający:

a) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również do podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;

b) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;

c) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utrata danych osobowych.

Dokonywanie zmian w miejscu wystąpienia zagrożenia lub incydentu jest dopuszczalne w przypadku, gdy zachodzi konieczność ratowania osób lub mienia albo zapobieżenia wystąpienia niebezpieczeństwa.

W sytuacji stwierdzenia wystąpienia zagrożenia lub incydentu zagrażającemu bezpieczeństwu danych osobowych, użytkownik może kontynuować prace dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji lub Sekretarza Gminy. W przypadku, gdy zagrożenie lub incydent jest wynikiem uchybienia obowiązującej w firmie dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności zaistniałej sytuacji i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem zagrożenia lub incydentu związanego z naruszeniem ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych. Rejestr incydentów prowadzony jest zgodnie ze wzorem (wzór rejestru **Załącznik Nr 9**).

21. Działania korygujące i zapobiegawcze

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Źródłami informacji o incydentach, zagrożeniach lub słabościach są:

a) zgłoszenia od pracowników;

b) wyniki kontroli.

W przypadku, gdy Administrator Bezpieczeństwa Informacji stwierdza konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

a) źródło powstania incydentu lub zagrożenia;

b) zakres działań korygujących lub zapobiegawczych;

c) termin realizacji;

d) osobę odpowiedzialną.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad poprawą i terminowością wdrażanych działań korygujących lub zapobiegawczych.

Po wprowadzeniu działań korygujących lub zapobiegawczych, Administrator Bezpieczeństwa Informacji jest zobowiązany do oceny efektywności ich zastosowania.

22. Przepisy karne i porządkowe

Wobec osoby, która w przypadku naruszenia zasad ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiednich osób zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.

Osoba upoważniona dopuszczająca się nieuprawnionego ujawniania lub wykorzystywania danych osobowych w sposób sprzeczny z ich przeznaczeniem, czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie Miasta i Gminy w Chmielniku zasadami i procedurami, może zostać ukarany karą upomnienia lub karą nagany.

Naruszenie zasad ochrony danych osobowych przez osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych może skutkować postawieniem zarzutu popełnienia jednego z przestępstwa określonych w Rozdziale 8 u.o.d.o. lub przestępstwa określonego w art. 266 Kodeksu Karnego.

Przepisy karne i porządkowe reguluje:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) - art. 49-54;

2) ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 1997 r., Nr 88, poz. 553, z późn. zm.) - art. 266;

3) ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 1998 r., Nr 21, poz. 94, z późn. zm.) - art. 52 oraz art. 108;

4) ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz. U. z 2008 r., Nr 223, poz. 1458, z późn. zm.);

23. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści oraz odbycia szkolenia w zakresie bezpieczeństwa danych osobowych.

Polityka Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie za wyjątkiem osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Chmielniku.

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. 2014 r. poz. 1182 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

24. Spis wzorów dokumentów

Załącznik Nr 1 – Wzór powołania Administratora Bezpieczeństwa Informacji.

Załącznik Nr 2 – Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 3 – Wzór oświadczenia.

Załącznik Nr 4 – Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 5 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik Nr 6 – Wzór wykazu pomieszczeń.

Załącznik Nr 7 – Wzór wykazu zbiorów.

Załącznik Nr 8 – Wzór opisu struktury zbiorów

Załącznik Nr 9 – Wzór rejestru *incydentów*.

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 1 (wzór)

Powołanie na stanowisko Administratora Bezpieczeństwa Informacji

Na podstawie art. 36a ust. 1 Ustawy o Ochronie Danych Osobowych z 29 sierpnia 1997 roku (Dz. U. z 2014 r. poz. 1182, z późn. zm.), z dniem ..... wyznaczam:

Panią/Pana

.....

/Imię i Nazwisko/

na

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Zakres zadań, upoważnień i odpowiedzialności Administratora Bezpieczeństwa Informacji określa Polityka Bezpieczeństwa Danych Osobowych.

Administrator Danych Osobowych	**Administrator Bezpieczeństwa Informacji**
.....	.....
/data, pieczęć i podpis ADO/	/data i podpis ABI/

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 2 (wzór)

Wniosek o wydanie, zmianę, cofnięcie upoważnienia

W związku z: (należy zaznaczyć odpowiednie pole):

Zatrudnienie nowego pracownika	Zmiana stanowiska	Zmiana zakresu obowiązków
☐	☐	☐
Tworzenie nowego zbioru danych	**Inne**	**Inne (opis)**
☐	☐	

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych proszę o wydanie / cofnięcie / zmianę (upoważnienia z dnia .....) do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych dla:

Imię:	Nazwisko:
Stanowisko:	**Komórka:**

Opis zakresu uprawnień:

Data i podpis wnioskodawcy

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 3 (wzór)

Oświadczenie
osoby dopuszczonej do przetwarzania danych osobowych

Ja niżej podpisana/ny oświadczam, że:

1. przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie,
2. zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w:
   - Polityce Bezpieczeństwa
   - Instrukcji Zarządzania Systemem Informatycznym

   oraz zobowiązuję się do ich przestrzegania,
3. uczestniczyłam/em w szkoleniu z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w Urzędzie Miasta i Gminy w Chmielniku.
4. Ponadto zobowiązuję się zachować w tajemnicy dane osobowe, które będę przetwarzać oraz znane mi sposoby zabezpieczenia danych osobowych stosowane w Urzędzie Miasta i Gminy w Chmielniku, przez cały okres zatrudnienia u Administratora Danych Osobowych / świadczenia usług na rzecz Administratora Danych Osobowych*, również po ustaniu zatrudnienia / zakończenia świadczenia usług na rzecz Administratora Danych Osobowych*, do momentu ich upublicznienia.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów karnych ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, z późn. zm.).

.....

/podpis składającego oświadczenie/

* niepotrzebne skreślić

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 4 (wzór)

Upoważnienie nr .....
do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy o Ochronie Danych Osobowych z 29 sierpnia 1997 roku (Dz. U. z 2014 r. poz. 1182 z późn. zm.), upoważniam Panią/Pana:

.....

/Imię i Nazwisko/

zatrudnioną/-nego na stanowisku: .....

do przetwarzania od dnia ..... r. danych osobowych w następującym zakresie:

- wykonywanie obowiązków służbowych na stanowisku pracy i poleceń przełożonego*

- wykonywanie obowiązków zleceniobiorcy*

i w systemie informatycznym nadaję identyfikator: .....

Niniejsze upoważnienie jest ważne w okresie od ..... do

.....

Administrator Danych Osobowych

.....

/podpis/

* niepotrzebne skreślić

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 5 (wzór)

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Lp.	Imię i Nazwisko, zajmowane stanowisko /data zmiany danych	Identyfikator w systemie informatycznym*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia
1	2	3	4	5	6
1					
	Zmiana danych**				
2					
	Zmiana danych**				
3					
	Zmiana danych**				

4					
	Zmiana danych**				
5					
	Zmiana danych**				

* Identyfikator jest wymagany jeśli dane są przetwarzane w systemie informatycznym.

** W przypadku zmiany danych wypełnić należy te rubryki, których zmiany dotyczą – pozostałe należy przekreślić.

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 6 (wzór)

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

Lp.	Miejsce przetwarzania danych osobowych /adres/	Obszar przetwarzania danych osobowych /nazwa pomieszczenia, nr itp./
1	2	3
1		

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 7 (wzór)

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych.

Lp.	Zbiór danych osobowych	Zastosowany program do przetwarzania danych
1	2	3
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 8 (wzór)

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Zbiór danych osobowych	Opis struktury zbioru
2	3

Urząd Miasta i Gminy w Chmielniku
Załącznik Nr 9 (wzór)

Ewidencja incydentów bezpieczeństwa i działań korygujących oraz zapobiegawczych.

L.p.	Incydent/zadanie /problem	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację	Przyczyna niezgodności	Działania korygujące /zapobiegawcze	Ocena skuteczności

L.p.	Incydent/zadanie /problem	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację	Przyczyna niezgodności	Działania korygujące /zapobiegawcze	Ocena skuteczności