Załącznik nr. 1 do Zarządzania NR 96/18
Burmistrza Miasta i Gminy Łagów
Z dnia 20.09.2018 roku

Polityka Bezpieczeństwa

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Miasta i Gminy Łagów

Wstęp

Celem Polityki ochrony danych w Urzędzie Miasta i Gminy Łagów, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane, w tym również dane osobowe.
Polityka ochrony danych została opracowana w oparciu o wymagania zawarte w:

- Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 24 maja 2018 r., poz. 1000/,
- 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. z 2017 r., poz. 2247),
- ustawie z dnia 9 lutego 2018r. o ochronie informacji niejawnych (tj. Dz. U. z 2018r., poz.412)
- § 3. i § 4. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych, oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz.1024)

Spis treści

1. Definicje

1) **Administrator** - Urząd Miasta i Gminy Łagów, reprezentowany przez Burmistrza ; ustala cele i sposoby przetwarzania danych osobowych;
2) **Inspektor Ochrony Danych /IDO/** - osoba, wyznaczona przez Administratora lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych;
3) **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
5) **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
6) **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
7) **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

8) **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
10) **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
11) **Zgoda** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

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 Rozdziale ..... Regulaminu Organizacyjnego Urzędu Miasta i Gminy Łagów stanowiącego załącznik do Zarządzenia Nr ..... Burmistrza Miasta i Gminy Łagów z dnia ..... roku.

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

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

4) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu

Gminy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

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

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

7) **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;

8) **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;

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

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

11) **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;

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

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

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

15) **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 Gminy;

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

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

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

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

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

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

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

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

24) **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.);

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

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

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

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

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

30) **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 Łagów, 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 Łagów lub przetwarzanych w celu realizacji zadań zleconych 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 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) Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,
2) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 24 maja 2018 r., poz. 1000/,
3) 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);

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 Łagów.

2) Analizy ryzyka i uzasadnienia dla zastosowania określonych założeń bezpieczeństwa danych osobowych

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

4) Rejestru przetwarzania danych osobowych

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

6) Opisu struktury zbiorów danych osobowych;

7) Opisu sposobu przepływu danych pomiędzy poszczególnymi systemami;

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

9) Wzorów formularzy pomocniczych.

Wyżej wymienione dokumenty będą prowadzone w formie odrębnej dokumentacji, przez Inspektora Ochrony Danych 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 Łagów związany jest odpowiednimi umowami.

6. Obowiązki Administratora Danych Osobowych

Do podstawowych obowiązków Administratora Danych Osobowych należy:

1) 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;

2) wyznaczenie Inspektora Ochrony Danych, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych;

3) podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki;

4) podjęcie decyzji dotyczących przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z Inspektorem Ochrony Danych;

5) wdrożenie rejestru czynności przetwarzania danych osobowych;
6) wdrożenie Polityki ochrony danych osobowych.
7) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą;
8) respektowanie prawa osób, których dane dotyczą;
9) wydawanie i odbieranie upoważnień do przetwarzania danych;
10) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;
11) kontrolowanie, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;
12) udzielanie informacji o zakresie przetwarzanych danych osobowych;
13) 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;
14) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych.

7. Inspektor Ochrony Danych

1) informuje Administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji;
2) prowadzi szkolenia z zakresu ochrony danych osobowych;
3) aktualizuje i sprawuje nadzór nad dokumentacją z zakresu ochrony danych osobowych;
4) opracowuje rejestr czynności przetwarzania danych i dokonuje jego bieżącej aktualizacji;
5) współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych;
6) pełni funkcję punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych.

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

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

9) przeprowadzanie kontroli w zakresie ochrony danych osobowych;

10) określanie potrzeb w zakresie zabezpieczenia danych osobowych ;

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

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

13) opiniowanie wzorów dokumentów i umów;

14) prowadzenie metryczek zbiorów danych osobowych;

15) 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;

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

17) zapewnienie poufności, integralności i rozliczalności danych osobowych;

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

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

8. 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 ściśle określonych praw dostępu do systemów informatycznych;
9) współpracę z dostawcami aplikacji i sprzętu komputerowego w tym sieciowego i serwerowego;
10) opracowywanie procedur dotyczących bezpieczeństwa i standardów zabezpieczeń w systemach informatycznych;
11) bieżące wykonywanie kopii systemowych jak i kopii baz danych i aplikacji wykorzystywanych do przetwarzania danych osobowych;
12) świadczenie wsparcia technicznego w ramach oprogramowania oraz serwis sprzętu komputerowego wchodzącego w skład systemów informatycznych Urzędu Gminy;
13) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz utrzymywanie kontaktu z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego;
14) prowadzenie dokumentacji dotyczącej opisu struktury zbiorów danych osobowych, prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych
15) prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych;

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

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

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

19) sprawowanie nadzoru nad profilaktyką antywirusową;

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

21) opiniowanie zakupów dotyczących urządzeń sieciowych i serwerowych;

22) 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 Łagów;
2) stosowanie się do zaleceń Inspektora Ochrony Danych 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 Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Urzędzie 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 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 Łagów 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 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 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 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 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 Danych Osobowych 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 Danych Osobowych 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 Dział Kadr (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 uwzględní 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.

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji opisującej obszar przetwarzania danych osobowych w siedzibie Urzędu Miasta i Gminy Łagów 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 Łagów, 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.

Administratora Danych Osobowych 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 Łagów, 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

Administratora Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Łagów. 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 Łagów. 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 Łagów. Dokumentacja prowadzona jest zarówno w formie papierowej jak i elektronicznej. Wszelkie zmiany ww. dokumencie są opiniowane i zatwierdzane przez Inspektora Ochrony Danych.

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 kierownika referatu.
- 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 Inspektora Ochrony Danych,
- 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 Łagów 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 dokumentacją, 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 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 Inspektora Ochrony Danych. W sytuacji braku możliwości zawiadomienia Inspektora Ochrony Danych należy powiadomić ??????? .

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 Inspektora Ochrony Danych 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 utratą 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 pracę dopiero po otrzymaniu pozwolenia od Inspektora Ochrony Danych lub Sekretarza Gminy. W przypadku, gdy zagrożenie lub incydent jest wynikiem uchybienia obowiązującej w firmie dyscypliny pracy, Inspektor Ochrony Danych 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.

Inspektor Ochrony Danych 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

Inspektor Ochrony Danych 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 Inspektor Ochrony Danych 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.

Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad poprawą i terminowością wdrażanych działań korygujących lub zapobiegawczych.

Po wprowadzeniu działań korygujących lub zapobiegawczych, Inspektor Ochrony Danych 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 Łagów 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 Łagów.

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 Inspektora Ochrony Danych.

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 9 - Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych,

Załącznik Nr 10 - Wzór odwołania zgody na przetwarzanie danych osobowych,

Załącznik Nr 11 - Wzór klauzuli informacyjnej,

Załącznik Nr 12 - Wzór oświadczenia o zachowaniu w poufności danych,

Załącznik Nr 13 - Wzór umowy powierzenia,

Załącznik Nr 14 - Wzór rejestru umów powierzenia przetwarzania danych osobowych,

Załącznik Nr 15 – Wzór rejestru *incydentów.*

Załącznik Nr 16 - Procedura zgłaszania naruszeń ochrony danych osobowych,

Załącznik Nr 17 - Procedura prawo dostępu do danych,

Załącznik Nr 18 - Procedura prawo do sprostowania danych do danych,

Załącznik Nr 19 - Procedura prawo do bycia zapomnianym,

Załącznik Nr 20 - Procedura prawo do przenoszenia danych,

Załącznik Nr 21 - Procedura prawo do sprzeciwu,

Załącznik Nr 22 - Opis środków technicznych i organizacyjnych,

Załącznik Nr 23 - Oświadczenie o monitorowaniu komputerów służbowych.

Urząd Miasta i Gminy Łagów
Załącznik Nr 1 (wzór)

Powołanie na stanowisko Inspektora Ochrony Danych

Na podstawie art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) – dalej, jako „RODO", wyznaczam

Panią/Pana

.....

/Imię i Nazwisko/

na

Inspektora Ochrony Danych

Zakres zadań, upoważnień i odpowiedzialności **Inspektora Ochrony Danych** określa Polityka Bezpieczeństwa Danych Osobowych.

Administrator Danych Osobowych	**Inspektor Ochrony Danych**
.....	.....
/data, pieczęć i podpis ADO/	/data i podpis IOD/

Urząd Miasta i Gminy Łagów
Załącznik Nr 2

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. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem 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

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 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
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 Łagów.
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 Łagów, 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 Rozporządzenia Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/, oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 24 maja 2018 r., poz. 1000/,

.....

/podpis składającego oświadczenie/

* niepotrzebne skreślić

Upoważnienie nr .....
do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE 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

oraz do przetwarzania danych osobowych w następujących celach:

.....

.....

W systemie informatycznym nadaję identyfikator: .....

Ponadto pracownik posiada dostęp do następujących systemów informatycznych przetwarzających

dane osobowe: .....

.....

Rozwiązanie stosunku pracy/ umowy w przypadku zleceniobiorców skutkuje odwołaniem upoważnienia.

.....

(pieczęć i podpis Administratora)

Niniejszym uprzednio wydane upoważnienie traci moc.

(*niniejsza klauzula ma zastosowanie tylko dla osób którym wcześniej wydano upoważnienie)

Urząd Miasta i Gminy Łagów
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/Cele przetwarzania danych	Data nadania upoważnienia	Data ustania upoważnienia
1.	2	3	4	5	6
1					
	Zmiana danych**				
2					
	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 Łagów
Załącznik Nr 6

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 Gminy ....., Ul. ... ., 26-.....	I piętro - pokoje 1, 5, 7, sekretariat, kasa Urzędu Gminy
		parter – 14, 15

Urząd Miasta i Gminy Łagów
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 Łagów
Załącznik Nr 7 (wzór)

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

L.p.	Zbiór danych osobowych	Zastosowany program do przetwarzania danych
1	2	3
1	Baza danych programu PUMA	Oprogramowanie dziedzinowe PUMA
2	System Rejestrów Państwowych	Program do obsługi Systemu Rejestrów Państwowych - Źródło
3	Baza danych programu KP	Saturn – Zeto Kielce
4		
5		
6		
7		
8		
9		

Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 w celach ....

.....
(data, podpis)

Administratorem danych osobowych przetwarzanych ww. celach jest .....

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 osobie, której dane dotyczą przysługuje prawo:

- żądania dostępu do danych osobowych;
- sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
- wniesienia sprzeciwu;
- cofnięcia zgody w każdym momencie, jednak bez wpływu na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody przed jej cofnięciem;
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa.

Zapoznałam/-em się z treścią powyższego.

.....
(data, podpis)

Wzór odwołania zgody na przetwarzanie danych osobowych

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 odwołuje wyrażoną przeze mnie zgodę na przetwarzanie danych osobowych w celach .....

przez.....

.....

(data, podpis)

Klauzula Informacyjna – wzór

Na podstawie art. 13 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO), informuję, że:

Administrator danych:

Administratorem zbieranych i przetwarzanych przez Urząd Miasta i Gminy w Łagowie danych osobowych jest Burmistrz Miasta i Gminy Łagów.

Adres: ul. Rynek 62, 26-025 Łagów

adres e-mail: urzad@lagowgmina.pl

Inspektor ochrony danych:

Dane kontaktowe inspektora ochrony danych w Urzędzie Miasta i Gminy w Łagowie: tel.: +48 795626770, adres e-mail: iod@abi-net.pl

Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania:

Dane osobowe zbierane i przetwarzane w celu możliwości wykonywania przez Urząd Miasta i Gminy Łagów ustawowych zadań publicznych, określonych min. w ustawie z dnia 8 marca 1990 r. o samorządzie gminnym, art. 6 ust. 1 lit. c ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. *oraz w innych aktach prawa powszechnie obowiązującego do których stosowania z mocy ustawy zobligowany jest Urząd Miasta i Gminy Łagów.*

Okres przechowywania danych osobowych:

Dane osobowe od momentu pozyskania będą przechowywane przez okres wynikający z regulacji prawnych (kategorii archiwalnej dokumentacji, określonej w jednolitym rzeczowym wykazie akt dla organów gmin i związków międzygminnych; umowy o dofinansowanie zawartej między beneficjentem a określoną instytucją; trwałości danego projektu i konieczności zachowania dokumentacji projektu do celów kontrolnych itp.). Kryteria okresu przechowywania ustala się w oparciu o klasyfikację i kwalifikację dokumentacji w jednolitym rzeczowym wykazie akt.

Prawo do dostępu danych osobowych:

Przysługuje Państwu prawo dostępu do treści danych oraz ich sprostowania. Jeżeli przetwarzanie danych odbywa się na podstawie zgody na przetwarzanie, petenci mają prawo do cofnięcia zgody na przetwarzanie ich danych osobowych w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Prawo wniesienia skargi do organu nadzorczego:

Przysługuje Państwu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Odbiorcy danych:

Odbiorcami danych będą instytucje uprawnione z mocy prawa.

W większości przypadków przetwarzanie danych osobowych wynika z przepisów prawa, a ich podawanie jest obowiązkowe. W niektórych sprawach podawanie danych osobowych może być dobrowolne, lecz niezbędne do realizacji celów. W sytuacji dobrowolności podawania danych osobowych osoby zostaną o tym fakcie poinformowane. Niepodanie lub podanie niepełnych danych osobowych może skutkować pozostawieniem wniosku bez rozpatrzenia.

Oświadczenie o poufności

IMIĘ I NAZWISKO

.....

STATUS / STANOWISKO

.....

W związku z dopuszczeniem do przetwarzania danych osobowych oświadczam, że:

Dnia ..... zostałam/zostałem zapoznana/zapoznany z przepisami dotyczącymi:

- ochrony danych osobowych, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"
- zasadami przetwarzania i ochrony danych osobowych opisanymi w Polityce bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wdrożonymi do stosowania u administratora danych.

Zobowiązuję się przestrzegać zasad i przepisów z zakresu ochrony danych osobowych oraz informacji objętych prawem tajemnicy podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do::

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych w celach pozasłużbowych o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne,
- przestrzegania regulaminu ochrony danych osobowych,
- dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych i informacji prawem chronionych,
- przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi administratora danych,
- zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, nieuprawnioną zmianą lub zniszczeniem, utratą, uszkodzeniem.
- zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia

- korzystania z wyposażenia IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy,
- należytej dbałości o wyposażenie IT i oprogramowanie zgodnie z regulaminem ochrony danych osobowych,
- korzystania z komputerów przenośnych zgodnie z regulaminem ochrony danych osobowych,
- zobowiązuję się do zachowania w tajemnicy wszystkich informacji i dokumentów ujawnionych mi lub wytworzonych przeze mnie lub przygotowanych przeze mnie w trakcie lub jako rezultat pracy i zgadzam się, że informacje te powinny być użyte tylko dla celów służbowych i nie mogą zostać ujawnione stronom trzecim,
- nie będę zatrzymywać kopii jakichkolwiek pisemnych lub elektronicznych informacji związanych z pełnioną przeze mnie funkcją i zakresem moich obowiązków.

Znane mi są zasady odpowiedzialności prawnej za niezgodne z ustawą o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u administratora danych, kodeksu pracy, kodeksu cywilnego oraz ustawy o ochronie danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

Powyższe zobowiązanie ma charakter bezterminowy i w szczególności dotyczy informacji i dokumentów, które stanowią tajemnice wynikające z przepisów prawa powszechnie obowiązującego.

Łagów ....
podpis osoby składającej oświadczenie

....
(podpis szkolącego / IOD) (podpis Administratora danych)

.....Łagów .....
(miejscowość, data)

Oświadczenie o zapoznaniu z treścią klauzuli informacyjnej

Ja, niżej podpisany/a

....

Oświadczam, że zostałem/zostałam zapoznany/zapoznana z treścią klauzuli informacyjnej, w tym z przysługującym prawie dostępu do treści moich danych osobowych oraz ich poprawiania, wycofania zgody na ich przetwarzanie w każdym czasie, jak również, że podanie tych danych było dobrowolne.

.....
(podpis osoby składającej oświadczenie)

Umowa powierzenia przetwarzania danych osobowych

z dnia .....

w sprawie powierzenia przetwarzania danych osobowych

zawarta pomiędzy

.....

(nazwa jednostki)

reprezentowaną przez ....., zwanym w dalszej części Administratorem danych osobowych,

a

.....

z siedzibą .....

reprezentowanym przez dyrektora zespołu ..... zwanym w dalszej części umowy Podmiotem przetwarzającym dane osobowe.

Na podstawie art. 28 ust. 3 Rozporządzenia Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO)* strony zawierają umowę następującej treści:

§ 1.

Przedmiotem umowy jest ustalenie celu oraz zakresu przetwarzania danych osobowych powierzonych przez Administratora Podmiotowi przetwarzającemu dane osobowe.

§ 2.

Zakres danych osobowych powierzonych przez Administratora danych Podmiotowi przetwarzającemu dane osobowe oraz kategorie osób, których dane są przetwarzane, wyznaczają przepisy szczególne regulujące sprawy z zakresu *(przykładowo):*

płac,

składek na ubezpieczenie społeczne,

podatków, w tym rocznych rozliczeń podatków od osób fizycznych,

Zakładowego Funduszu Świadczeń Socjalnych,

kasy zapomogowo-pożyczkowej,

ubezpieczeń,

zajęć komorniczych,

odprowadzania składek członków związków zawodowych,

wydawania zaświadczeń na podstawie przetwarzanych danych osobowych,

prowadzenia akt osobowych dyrektora szkoły,

wypłaty stypendiów materialnych o charakterze motywacyjnym dla uczniów,

inne (wymienić).

§ 3.

Powierzenie przetwarzania danych osobowych służy realizacji celów określonych w przepisach szczegółowych regulujących zadania Administratora wymienione w § 2 niniejszej umowy.

§ 4.

Podmiot przyjmujący przetwarzanie danych osobowych może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w niniejszej umowie.

§ 5.

1. Administrator udziela Podmiotowi przetwarzającemu dane osobowe ogólnej pisemnej zgody na korzystanie z usług innego podmiotu przetwarzającego. Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

2. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między Administratorem a Podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym Podmiocie przetwarzającym.

§ 6.

1.Podmiot przetwarzający dane osobowe:

przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora– chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa polskiego, któremu podlega Podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

wyznacza Inspektora Ochrony Danych Osobowych, który realizuje zadania określone w art. 39 RODO;

podejmuje wszelkie środki wymagane na mocy art. 32 RODO;

prowadzi rejestr czynności przetwarzania danych osobowych zaliczonych do szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO;

przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w § 5;

biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;

uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;

po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa polskiego nakazują przechowywanie danych osobowych;

udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem określonym w akapicie pierwszym pkt 10 podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa polskiego o ochronie danych.

2. Jeżeli Podmiot przetwarzający naruszy przepisy RODO przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

§ 7.

W zakresie nieuregulowanym niniejszą umową stosuje się przepisy Rozporządzenia Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w *sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).*

§ 8.

1. Czas przetwarzania danych osobowych dla poszczególnych celów określają przepisy szczegółowe.

2. Umowa została zawarta na czas nieokreślony, z możliwością rozwiązania przez każdą ze stron z zachowaniem trzymiesięcznego okresu wypowiedzenia.

§ 9.

Wszelkie zmiany umowy wymagają formy pisemnej, w postaci aneksu do niniejszej umowy.

§ 10.

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Administrator danych osobowych

przetwarzający dane osobowe

Podmiot

Urząd Miasta i Gminy Łagów
Załącznik Nr 14 (wzór)

Rejestr umów powierzenia danych osobowych

Lp.	Numer umowy	Data zawarcia umowy	Strona umowy	Zakres powierzenia
1.				
2.				

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
1.	Infekcja wirusowa na stacji roboczej/ odwirusowanie stacji roboczej lub reinstalacja systemu	użytkownik	23.03.2015	23.03.2015	Informatyk	brak	Reinstalacja systemu	9/10 – system przeinstalowano , stracono część plików użytkownika – nie były to pliki wrażliwe podlegające ochronie

Procedura zgłaszania naruszeń ochrony danych osobowych

1. Cel procedury

Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości w funkcjonowaniu Jednostki, spowodowanych nieuprawnionym ujawnieniem danych osobowych, udostępnieniem lub umożliwieniem dostępu do nich osobom nieupoważnionym, zabraniem danych przez osobę nieupoważnioną, uszkodzeniem lub usunięciem, a w szczególności:

1. nieautoryzowany dostęp do danych,
1. nieautoryzowane modyfikacje lub zniszczenie danych,
2. udostępnienie danych nieautoryzowanym podmiotom,
3. nielegalne ujawnienie danych,
4. pozyskiwanie danych z nielegalnych źródeł.

2. Klasyfikacja naruszeń

Naruszenia ze względu na ich występowanie możemy podzielić na:

1. zdarzenia losowe **zewnętrzne**, których występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów (np. klęski żywiołowe, przerwy w zasilaniu);
2. zdarzenia losowe **wewnętrzne**, których występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu, może nastąpić naruszenie poufności danych (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu);
3. zdarzenia zamierzone, celowe i świadome, niepowodujące uszkodzenia infrastruktury technicznej i zakłóceń ciągłości pracy możemy podzielić na:
    a) nieuprawniony dostęp do bazy danych z zewnątrz
    b) nieuprawniony dostęp do bazy danych z sieci wewnętrznej
    c) nieuprawniony transfer danych
    d) pogorszenie funkcjonowania sprzętu i oprogramowania np. działania wirusów

e) bezpośrednie zagrożenie materialnych składników systemu np. kradzież sprzętu.

3. Zgłaszanie naruszeń związanych z bezpieczeństwem informacji

W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a następnie postępować stosownie do podjętej przez niego decyzji.

Pracownicy jednostki mają obowiązek zgłaszać zauważone przez siebie naruszenia oraz notować wszystkie szczegóły związane z naruszeniami.

Zgłoszenie powinno zawierać:

a) imię i nazwisko zgłaszającego,
b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
d) określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń w jednostce jest ASI

4. Postępowanie z naruszeniami

Osoba, która otrzymała zgłoszenie dokonuje wstępnej identyfikacji zdarzenia i po konsultacji z Inspektorem Ochrony Danych Osobowych dokonuje jego kwalifikacji jako naruszenie niskie lub wysokie. W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi ***załącznik nr 15*** do PBI. Naruszenia zakwalifikowane jako wysokie podlegają zgłoszeniu do organu nadzorczego niezwłocznie, jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia.

a) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
b) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
c) liczba referatów/komórek organizacyjnych dotkniętych incydentem,
d) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
e) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
f) szacowany poziom szkód,
g) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
h) skutki organizacyjne i prawne (wstępny szacunek).

Po dokonanej analizie Administrator zgłasza naruszenie do organu nadzorczego (wzór zgłoszenia stanowi ***załącznik nr 1*** do niniejszej Procedury), oraz jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (wzór zawiadomienia stanowi ***załącznik nr 2*** do niniejszej Procedury). Zawiadomienie osoby nie jest wymagane jeśli Administrator wdrożył odpowiednie techniczne
i organizacyjne środki, które uniemożliwią osobom nieuprawnionym dostęp do danych, zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Z zawiadomienia, o którym mowa nie należy stosować, gdy wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak wypadku należy opublikować ogłoszenie, zastosować inny, równie skuteczny środek.

Jeżeli z jakiegokolwiek powodu nie uda się przekazać zgłoszenia w tym terminie, do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia. Jeżeli Administrator nie zawiadomił jeszcze o naruszeniu osób, których ono dotyczy, organ nadzorczy może mu to nakazać.

Dodatkowo naruszenia mogą być wykorzystywane przez Inspektora Ochrony Danych podczas szkoleń pracowniczych jako przykład tego, co może się wydarzyć, jak unikać ich w przyszłości i jak reagować, jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowywania poufności.

Załącznik nr: 1

.....dnia.....

Urząd Ochrony Danych Osobowych

.....

Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

Na podstawie obowiązku wynikającego z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Data Naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria tych danych	
Dane Inspektora Danych osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia:	
Konsekwencje naruszenia:	
Zastosowane i proponowane środki zaradcze:	

.....

(Podpis Administratora)

Załącznik nr: 2

.....dnia .....roku

Pan/Pani .....

.....

.....

ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH

Na podstawie obowiązku wynikającego z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w związku z naruszeniem Pana/Pani danych osobowych w zakresie ..... Zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie.....

Urząd podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

Celem uzyskania dodatkowych informacji należy kontaktować się z .....

.....
(Podpis Administratora)

Urząd Miasta i Gminy Łagów
Załącznik Nr 9 (wzór)

Ewidencja incydentów bezpieczeństwa i działań korygujących oraz zapobiegawczych.

L.p.	Incydent/zadanie /problem	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Kwalifikacja naruszenia	Odpowiedzialny za realizację	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby, której dane dotyczą (dotyczy lub nie dotyczy)	Działania korygujące /zapobiegawcze	Ocena skuteczności

Procedura prawo dostępu do danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa dostępu do swoich danych przetwarzanych przez Administratora.

Każdej osobie fizycznej przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia czy dane są faktycznie przetwarzane.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba fizyczna, której dane są przetwarzane ma prawo do uzyskania informacji o:

1) celach, w jakich przetwarzane są dane osobowe;
2) kategoriach danych osobowych, które podlegają przetwarzaniu;
3) odbiorcach lub kategoriach odbiorców;
4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania okresu przechowywania danych;
5) prawie do żądania sprostowania swoich danych osobowych;
6) prawie do usunięcia lub ograniczenia przetwarzania danych osobowych;
7) prawie do wniesienia sprzeciwu wobec konkretnego przetwarzania swoich danych;
8) prawie do wniesienia skargi do organu nadzorczego, na przetwarzanie swoich danych, jeśli są one przetwarzane niezgodnie z obowiązującymi przepisami;
9) w sytuacji, gdy dane osobowe nie zostały zebrane od osoby, której one dotyczą – wszelkich dostępnych informacje o źródle, z którego administrator pozyskał te dane
10) zautomatyzowanym podejmowaniu decyzji, jeżeli Administrator realizuje wobec konkretnej osoby fizycznej taki sposób przetwarzania, w tym informacji o profilowaniu (art. 22 ust. 1 i 4 RODO).

3. Realizacja uprawnienia dostępu do danych

Osoba fizyczna otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie **kopii przetwarzanych danych osobowych.** Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Pierwsza kopia i jej przekazanie odbywa się **bezpłatnie**, lecz za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator będzie miał prawo pobrać „opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora).

Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych. Uzyskując wgląd do swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych.

W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

<u>Terminy na udzielenie odpowiedzi na żądanie:</u>

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące**, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).
3. W przypadku, gdy administrator nie zamierza udzielić odpowiedzi oraz podjęcia działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Wzór odpowiedzi na skierowany wniosek:

Na podstawie art. 15 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Administrator potwierdza, że Pana/Pani dane osobowe są przetwarzane i jednocześnie informuje, że:

1) celem przetwarzania Pani/Pana danych osobowych jest ...;
2) (administrator) przetwarza Pani/Pana dane osobowe w zakresie ... (należy wskazać kategorię danych osobowych);
3) dane osobowe będą ujawniane ... (należy wskazać odbiorcę lub kategorie odbiorców);
4) dane osobowe będą przechowywane przez okres ...;
5) przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;
6) (administrator) uzyskał Pani/Pana dane osobowe z ... (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);
7) (należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

_____

(data, podpis)

Procedura prawo do sprostowania danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca wniosek o sprostowanie/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1) pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),
2) odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym.

4. Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.

Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

<u>Terminy na udzielenie odpowiedzi na żądanie:</u>

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania;
2) jeżeli żądanie ma charakter skomplikowany lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące**, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

5. W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Procedura prawo do bycia zapomnianym

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje prawo żądania usunięcia jej danych osobowych przetwarzanych przez Administratora. Prawo to składa się z następujących uprawnień:

1) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,
2) możliwości żądania, aby Administrator danych poinformował innych Administratorów, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych Administratorów może być ograniczony poprzez: dostępną technologię, koszy, konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych Administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

Każdej osobie fizycznej przysługuje prawo do „bycia zapomnianym." Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;

4) dane osobowe były przetwarzane w sposób „niezgodny z prawem";
5) dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym:

1) istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,
3. istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Procedura prawo do przeniesienia danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi;
2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1) przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;
2) przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Oświadczenie o monitorowaniu komputerów służbowych

Oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerach służbowych i na których wykonuję obowiązki pracownicze, są monitorowane, w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuję się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

....

Data Podpis

Procedura prawo do sprzeciwu

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, (w tym profilowania na podstawie tych przepisów), tj. sytuacji, w której:

1) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
2) przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W sytuacji, gdy Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, to Administratorowi nie wolno już przetwarzać tych danych osobowych do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść bezpłatnie sprzeciw do Administratora, w dowolnym momencie, wobec tego konkretnego przetwarzania, pierwotnego lub dalszego (w tym profilowania), o ile jest ono powiązane z marketingiem bezpośrednim.

Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.

3. Szczególne uprawnienia związane z procesami zautomatyzowanego przetwarzania danych - w tym z profilowaniem

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który odbywa się w sposób automatyczny, ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane. Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

1) osoba profilowana wyrazi na to wyraźną zgodę,
2) profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
3) profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być

szczególny przepis prawa. W przypadku gdy zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

4. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Urząd Miasta i Gminy Łagów
Załącznik Nr 22 (wzór)

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych dla lokalizacji Urząd Miasta i Gminy Łagów, ul. .....

Środek ochrony fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).		
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są **za pomocą krat, rolet lub folii antywłamaniowej.**		
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są **w system alarmowy przeciwwłamaniowy.**		
4. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są **systemem kontroli dostępu.**		
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**		
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.**		
7. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej niemetalowej szafie.**		
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**		
9. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętym sejfie lub kasie pancernej.**		
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej** szafie.		

11. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.		
12. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.		
13. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.		

ŚRODKI TECHNICZNE

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Zastosowano (TAK / NIE)	Uwagi
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.		
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.		
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.		
Użyto system Firewall do ochrony dostępu do sieci komputerowej.		

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych		
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych		
Powołano Administratora Bezpieczeństwa Informacji		
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych		

Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych		
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych		
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego		
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy		
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym		
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco		

Kopie zapasowe

Dane osobowe przetwarzane w formie elektronicznej, w szczególności w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada *informatyk/osoba upoważniona przez Administratora/podmiot zajmujący się obsługą informatyczną jednostki*

Z komentarzem [A1]: Proszę o dookreślenie kto w Państwa jednostce realizuje zadania dotyczące obsługi informatycznej. Informatyk zatrudniony w jednostce, osoba upoważniona przez Administratora, czy podmiot zewnętrzny tj. firma obsługująca.

Kopią zapasową objęte są:

Z komentarzem [A2]: Proszę o uzupełnienie tabelki

	Częstotliwość wykonywania kopii zapasowej	Rodzaj nośnika na jakim wykonano kopię zapasową	Sposób wykonywania kopii	Miejsce przechowywania nośnika na którym zapisano kopię
Bazy danych				
Serwery				
Pliki				

Sposób postępowania z kluczami do pomieszczeń biurowych

Z komentarzem [A3]: Proszę o zweryfikowanie sposobu postępowania z kluczami i dostosowanie zapisów do stanu faktycznego w Państwa jednostce.

Administrator wyznaczył pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki. Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do nieudostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.

Każdy pracownik posiada swój komplet kluczy do budynku UG. Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończonym dniu pracy do sekretariatu. Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed

przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń. W przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń stanowiącą **załącznik nr 16 do niniejszej Polityki.**

Zabrania się pozostawiania kluczy do pomieszczeń obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia zamyka się na czas nieobecności wszystkich pracowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Pracownicy po godzinach pracy jednostki mogą w nim przebywać jedynie za zgodą Administratora. W przypadkach przebywania pracowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.