Polityka ochrony danych osobowych – dokument główny

Wersja dokumentu 2.00 z dnia 15 października 2018 roku

ZATWIERDZAM
BURMISTRZ
mgr Piotr Ćwiąka

.....

Burmistrz Łobza

Łobez październik 2018 roku

METRYKA

Nazwa jednostki	Urząd Miejski w Łobzie		
Tytuł dokumentu	Polityka ochrony danych osobowych		
Opis	W skład dokumentu wchodzą: Polityka ochrony danych osobowych wraz z załącznikami		
Zastosowanie	Wszystkie komórki organizacyjne		
Plik	Polityka ochrony danych osobowych		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia .... listopada 2018 r.	Liczba stron	24

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	15.07.2018	utworzenie	wszystkie	Krzysztof Rychel	
2.00	15.10.2018	weryfikacja i modyfikacja	proces nadania upoważnień	Sekretarz Gminy	

* Np.: utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Postanowienia wstępne

1.1 *Polityka ochrony danych osobowych w Urzędzie Miejskim w Łobzie* (dalej: Urząd) jest zbiorem zasad i procedur, obowiązujących przy realizacji wszystkich czynności przetwarzania i wykorzystywania danych osobowych administrowanych przez Urząd Miejski w Łobzie. Celem wprowadzenia polityki jest ograniczenie ryzyka naruszenia praw i wolności osób fizycznych, w tym w szczególności mieszkańców gminy, klientów Urzędu i pracowników jednostki, jakie może spowodować przetwarzanie ich danych w związku z realizowanymi przez Urząd zadaniami i obowiązkami. Ponadto polityka ma na celu wykazanie realizacji zasady rozliczalności, przez prowadzenie w jednostce odpowiedniej dokumentacji, opisującej sposoby ochrony danych, na którą składa się niniejsza polityka wraz z załącznikami stanowiącymi jej integralną część. Niniejsze zasady zostały opracowane z uwzględnieniem zasady: „Człowiek może zawieść – system nie powinien".

1.2 Niniejsza polityka dotyczy wszystkich czynności przetwarzania danych osobowych w zidentyfikowanych, jak i niezidetyfikowanych zbiorach danych osobowych, jak również czynności przetwarzania danych osobowych realizowanych w sposób ciągły, jak i doraźny. W polityce przyznano wyższy priorytet realizowanym czynnością przetwarzania danych osobowych i ich identyfikacj w odniesieniu do obowiązku identyfikacji zbiorów danych osobowych. Polityka jest polityką ochrony danych osobowych w rozumieniu *rozporzędzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz. Urz. UE L 119, s.1) – dalej: RODO.*

1.3 Dane osobowe w Urzędzie Miejskim w Łobzie mogą być przetwarzane zarówno w sposób tradycyjny w księgach, aktach, wykazach i innych papierowych zbiorach ewidencyjnych, jak i w systemach informatycznych.

1.4 Niniejszy dokument ma za zadanie stanowić mapę wymogów, zasad i regulacji zwiazanych z obszarem ochrony danych osobowych w Urzędzie Miejskim w Łobzie i zawiera:

- ✓ opis zasad ochrony danych obowiazujących w Urzędzie;
- ✓ odwołania do załączników stanowiących wzorce zachowań, procedur lub dokumentów.

1.5 Odpowiedzialnym za wdrożenie i utrzymanie niniejszej polityki jest najwyższe kierownictwo Urzedu w osobie Burmistrza Łobza.

2. Definicje

Ilekroć w polityce użyte zostaną nw. określenia to oznaczają one:

- ✓ **„administrator danych osobowych"** (dalej:**ADO**) – Burmistrz Łobza;
- ✓ **„administrator systemu informatycznego"** (dalej **ASI**) – pracownik lub podmiot zewnętrzny odpowiadający za administrowanie systemem informatycznym;
- ✓ **„czynność przetwarzania danych"** – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie, archiwizowanie;

- ✓ **"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;

- ✓ **"dane biometryczne"** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak **wizerunek twarzy** lub dane daktyloskopijne;

- ✓ **"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;

- ✓ **"dane genetyczne"** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

- ✓ **„dostępność danych"** - właściwość określająca, że zasób przetwarzanych danych osobowych, niezależnie od sposobu ich przetwarzania jest możliwy do wykorzystania na żądanie, w założonym czasie, przez użytkownika;

- ✓ **„integralność danych"** – określana również, jako spójność polegająca na zachowaniu własności przez dane osobowe wykluczające wprowadzenie do nich zmian w nieautoryzowany sposób;

- ✓ **„jednostka"** – Urząd Miejski w Łobzie;

- ✓ **„kategoria czynności przetwarzania"** (kategoria przetwarzań) to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.

- ✓ **„komórka organizacyjna"** – jedno lub wieloosobowy zespół znajdujący wyodrębnienie w strukturze organizacyjnej, ustanowiony do wykonywania określonych zadań w jednostce organizacyjnej podlegający konkretnej osobie sprawującej nadzór nad jej działaniami. W jednostce zgodnie z przyjętym schematem organizacyjnym **(załącznik nr 1)** wyróżnia się wydziały, samodzielne stanowiska oraz merytoryczne samodzielne stanowiska (np.: radca prawny, audytor).

- ✓ **„kierownik komórki organizacyjnej"** – rozumie się przez to osoby kierujące lub nadzorujące pracę innych osób lub osobę zajmujące samodzielne stanowisko;

- ✓ **"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;

- ✓ **„ograniczenie przetwarzania"** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- ✓ **„osoba upoważniona do przetwarzania danych osobowych lub użytkownik systemu"** – rozumie się przez to osobę, która została upoważniona pisemnie przez ADO oraz dopuszczona, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu;
- ✓ **"organ nadzorczy"** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 – Prezes Urzędu Ochrony Danych Osobowych;
- ✓ **"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;
- ✓ **"podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- ✓ **„poufności danych"** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- ✓ **„profilowanie"** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- ✓ **„przetwarzanie danych osobowych"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
- ✓ **"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;
- ✓ **RODO** – rozumie się przez to rozumie się przez to 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);
- ✓ **RCPD** – Rejestr czynności przetwarzania danych osobowych;

- ✓ **„rozliczalność danych"** - właściwość pozwalająca przypisać określone działanie związane z przetwarzaniem danych osobowych do osoby fizycznej zatrudnionej w Urzędzie Miejskim, procesu, miejsca oraz umiejscowić je w czasie;
- ✓ **„serwisancie"** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;
- ✓ **"strona trzecia"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
- ✓ **„systemie informatycznym"** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- ✓ **„użytkownik"** – pracownik Urzędu Miejskiego w Łobzie lub inna osoba zatrudniona w Urzędzie na podstawie umowy cywilnej, upoważniona do przetwarzania danych osobowych, w tym w systemie informatycznym, programie komputerowym, aplikacji;
- ✓ **„Urząd"** – Urząd Miejski w Łobzie;
- ✓ **„uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika;
- ✓ **„zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- ✓ **"zgoda"** osoby, której dane dotyczą 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;

3. Organizacja przetwarzania danych osobowych

3.1 Przetwarzanie danych osobowych w Urzędzie jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów RODO.

3.2 Urząd przetwarza dane osobowe zgodnie z zasadami wskazanymi w art. 5 i art. 25 RODO, które stanowią filary ochrony danych osobowych, czyli zgodnie z zasadą:

- ✓ zgodności z prawem,
- ✓ rzetelności i przejrzystości,
- ✓ zasadą ograniczenia celu,
- ✓ minimalizacji danych,
- ✓ prawidłowości danych,
- ✓ ograniczenia przechowywania,
- ✓ integralności i poufności,

- ✓ ochrony danych w fazie projektowania,
- ✓ domyślną ochroną danych
- ✓ zasadą przestrzegania praw jednostki.

3.3 Zasada zgodności z prawem (art. 5 ust. 1 lit. a RODO) oznacza, iż Urząd przetwarza dane osobowe na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych wynikających z art. 6, 9 bądź 10 RODO. Urząd, jako jednostka samorządowa realizuje zadania wynikające z przepisów prawa w szczególności ustawy z dnia 8 marca 1990 r. o samorządzie gminnym i, co do zasady przetwarzanie danych osobowych w jednostce odbywa się w oparciu o przesłanki wskazane art. 6 ust. 1 lit. c, e lub art. 9 ust. 2 lit. b lub art. 10 RODO. Stosowanie przedmiotowej zasady zobowiązuje pracowników jednostki w odniesieniu do realizowanych czynności przetwarzania danych osobowych, identyfikowanie podstawy prawnej w postaci konkretnej normy prawnej i jej wskazywanie w **Rejestrze czynności przetwarzania danych osobowych** (dalej: **RCPD**), o którym mowa w art. 30 ust. 1 RODO. Wzór rejestru stanowi **załącznik nr 2.**

3.4 Rejestr czynności przetwarzania danych osobowych jest prowadzony odrębnie na poziomie każdej komórki organizacyjnej, w tym również na samodzielnych stanowiskach, nawet w sytuacji, gdy komórka organizacyjna składa się z 1 osoby. Za prowadzenie przedmiotowego rejestru, odpowiedzialna jest osoba pełniąca funkcję kierownika komórki lub sprawująca nadzór nad jej działaniem lub osoba sprawująca nadzór nad działaniem samodzielnych stanowisk oraz

3.5 Zasadę rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO) Urząd realizuje poprzez wypełnianie obowiązków informacyjnych wskazanych w art. 13 i art. 14 RODO oraz udzielanie odpowiedzi na wnioski osób, których dane dotyczą, szczególnie w zakresie wynikającym z art. 15 RODO. Obowiązki informacyjne realizowane są przez poszczególnych pracowników Urzędu, którym powierzono prowadzenie sprawy lub jej prowadzenie wynika z przyjętego zakresu obowiązków. Za realizację przedmiotowego obowiązku informacyjnego odpowiada pracownik oraz jego bezpośredni przełożony. Sposób realizacji obowiązku informacyjnego określa **Procedura realizacji obowiązku informacyjnego (Książka procedur).** Procedura jest dokumentem jawnym i może zostać upubliczniona na stronie internetowej Urzędu.

3.6 Urząd, jako administrator przetwarza dane osobowe jedynie w celach związanych z realizacją zadań wynikających w szczególności z ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Wyjątek od tej reguły stanowi dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (zasada ograniczenia celu art. 5 ust. 1 lit. b RODO). Wskazanie celu przetwarzania stanowi obligatoryjny element ***Rejestru czynności przetwarzania danych osobowych*** oraz informacji udzielanej właścicielowi danych osobowych.

3.7 Urząd, jako podmiot przetwarzający w sytuacji, gdy powierzono jemu dane przez innego administratora i na mocy przyjętego w formie pisemnej umowy powierzenia zobowiązania, polegającego na przetwarzaniu danych w imieniu i na rzecz innego podmiotu (art. 30 ust. 2 RODO), prowadzi ***Rejestr kategorii czynności przetwarzania,*** stanowiący **załącznik nr 3**. ***Rejestr kategorii czynności przetwarzania***, podobnie jak ***Rejestr czynności przetwarzania danych osobowych*** jest prowadzony odrębnie na poziomie każdej komórki organizacyjnej, w tym na samodzielnych stanowiskach, nawet w sytuacji, gdy komórka organizacyjna składa się z 1 osoby. Za prowadzenie

przedmiotowego rejestru odpowiedzialna jest osoba sprawująca nadzór nad działaniem komórki lub też osoba pełniąca funkcję kierownika komórki oraz osoba nadzorująca pracę samodzielnych stanowisk.

3.8 ***Rejestr kategorii czynności przetwarzania*** oraz ***Rejestr czynności przetwarzania danych osobowych*** stanowią formę dokumentowania czynności przetwarzania danych osobowych i są kluczowymi elementami umożliwiającymi realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych – czyli zasady rozliczalności.

3.9 Dla celów zgodności z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) w Urzędzie przetwarza się wyłącznie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania, a osoba przetwarzająca w kontekście realizowanego zadania jest w stanie uzasadnić potrzebę przetwarzania każdej kategorii danych, wskazując przy tym właściwy przepis prawa. Za adekwatność zakresu przetwarzanych danych osobowych ponosi odpowiedzialność pracownik realizujący czynność przetwarzania i jego bezpośredni przełożony. Kategorie danych podlegające przetwarzaniu muszą znaleźć swoje odzwierciedlenie w ***Rejestrze czynności przetwarzania danych osobowych***, o którym mowa w art. 30 ust. 1 RODO, w odniesieniu do konkretnie realizowanej czynności przetwarzania.

3.10 Przetwarzaniu podlegają dane osobowe prawidłowe, aktualne, i odpowiadające faktycznemu stanowi rzeczy, co zapewnia zadośćuczynienie zasadzie prawidłowości danych (art. 5 ust. 1 lit. d RODO). Obowiązkiem pracownika przetwarzającego dane jest podjęcie możliwych starań w celu upewnienia się, co do stanu aktualności przetwarzanych danych osobowych.

3.11 Wychodząc naprzeciw zasadzie ograniczenia przechowywania danych osobowych (art. 5 ust. 1 lit. e RODO), dane osobowe w Urzędzie przechowuje się wyłącznie przez okres niezbędności dysponowania dokumentacją dla realizowania zadań lub przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt, odpowiadający wymogom ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, z właściwym archiwum państwowym. Realizacja zasady ograniczenia przechowywania, następuje przez dokumentowanie procesu brakowania dokumentacji niearchiwalnej lub przekazywania materiałów archiwalnych do właściwego archiwum państwowego. Usuwanie danych zawartych w dokumentacji niearchiwalnej następuje w momencie niszczenia dokumentacji na podstawie zgody właściwego archiwum państwowego, po spełnieniu się łącznie dwóch warunków: upływ okresu przechowywania dokumentacji oraz jej zbędność do celów służbowych. Realizacja zasady ograniczenia przechowywania następuje również przez wskazanie planowanych terminów przetwarzania danych w ***Rejestrze czynności przetwarzania danych osobowych***, o którym mowa w art. 30 ust. 1 RODO.

3.12 Proces przetwarzania danych osobowych odpowiada zasadzie integralności i poufności (art. 5 ust. 1 lit. f RODO), co zapewnia, dopuszczenie do przetwarzania danych osobowych jedynie osoby upoważnione oraz zastosowanie takich środków technicznych i organizacyjnych, by dane nie były zmieniane przez osoby nieupoważnione, zmienione nieumyślnie lub by dane nie były udostępniane osobom nieupoważnionym.

3.13 Zgodnie z zasadą ochrony danych w fazie projektowania (art. 25 ust. 1 RODO), ochrona prywatności i poufności przetwarzania danych osobowych winna być wbudowana w każdy nowy projekt na etapie jego planowania. W szczególności zasada ta będzie realizowana w zamówieniach publicznych, czy przy zawieraniu umów powierzenia przetwarzania danych osobowych. Wyrazem

spełnienia tej zasady jest wprowadzanie obowiązku ochrony przetwarzanych danych bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą.

3.14 Mając na uwadze aktualność zapisów zawartych w ***Rejestrze czynności przetwarzania danych osobowych*** i w ***Rejestrze Kategorii przetwarzania*** administrator danych osobowych zobowiązany jest do przeprowadzenia okresowej inwentaryzacji:
a) realizowanych czynności przetwarzania w odniesieniu, do których pełni funkcję administratora,
b) realizowanych czynności przetwarzania powierzonych jemu danych, które wykonuje w drodze zawartych umów powierzenia danych osobowych do dalszego przetwarzania.

3.15 Inwentaryzacja, o której mowa powyżej jest wykonywana nie rzadziej niż raz w ciągu roku lub każdorazowo na uzasadniony wniosek Inspektora Ochrony Danych. Czynności inwentaryzacyjne przeprowadzane są przez kierowników komórek organizacyjnych oraz wszystkie samodzielne stanowiska.

4. Obsługa praw jednostki

4.1 Urząd spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w szczególności poprzez:

- ✓ **spełnienie obowiązku informacyjnego** – Urząd przekazuje informacje właścicielom danych osobowych w formie informacji, której minimalny zakres określono w art. 13 oraz 14 RODO. Informacje są przekazywane, właścicielom danych osobowych, których dane są przetwarzane lub ich opiekunom prawnym. Wzory **stosownych informacji** zostały określone w **załączniku nr 4**, a sposób realizacji obowiązku informacyjnego określa ***Procedura realizacji obowiązku informacyjnego.***
- ✓ **możliwość wykonania żądań** – Urząd w związku z przyjętą strukturą organizacyjną weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu takiego żądania;
- ✓ **obsługa żądań** – Urząd zapewnia odpowiednie nakłady, aby żądania były realizowane w terminach określonych w RODO i należycie dokumentowane. Bezpośredni nadzór nad realizacją zgłaszanych żądań sprawuje administrator danych osobowych lub osoba upoważniona przez niego (posiadająca pisemne upoważnienie lub wskazanie w indywidualnym zakresie czynności).

4.2 Urząd dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
4.3 Urząd ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczanie na swojej stronie internetowej informacji lub odwołań do informacji o prawach osób i sposobie korzystania z nich (w postaci linków) .
4.4 Urząd przestrzega prawnych terminów dotyczących obowiązków informacyjnych względem osób fizycznych oraz dokumentuje ich obsługę oraz obsługę zawiadomień i żądań osób.
4.5 Urząd określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych tam, gdzie jest to możliwe (np. tablica informująca o objęciu obszaru monitoringiem wizyjnym).
4.6 Urząd informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych – chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
4.7 W przypadku stwierdzonego naruszenia ochrony danych osobowych, Urząd bez zbędnej zwłoki zawiadomi właściciela danych, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw

i wolności tej osoby (art. 34 RODO) – ***Procedura postępowania przy stwierdzeniu naruszenia,*** **(Książka procedur)**

5. Administrator Danych Osobowych (ADO)

5.1 Administratorem Danych Osobowych (dalej: ADO, administrator) w rozumieniu art. 4 pkt 7 RODO jest Burmistrz Łobza.

5.2 Głównym zadaniem ADO jest ustalenie charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych i wdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zapewnienie procesowi przetwarzania zgodność z przepisami wskazanymi w RODO (art. 32 RODO).

5.3 Aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać ADO odpowiada w szczególności za:

- ✓ sporządzenie analizy ryzyka wszystkich zidentyfikowanych zagrożeń dla procesu przetwarzania danych osobowych. Minimalny zakres zagrożeń uwzględnianych w przedmiotowej analizie wynika z zakresu określonego w załączniku C (Przykłady typowych zagrożeń) do PN-ISO/IEC 27005;
- ✓ opracowanie, wprowadzenie i wdrożenie odpowiedniej polityki ochrony danych osobowych;
- ✓ określenie częstotliwość dokonywania przeglądu przedmiotowej polityki pod kątem jej aktualności. Tym samym korzystając z posiadanych kompetencji ADO ustanawia, że przedmiotowy przegląd będzie realizowany, co najmniej raz w roku lub każdorazowo w przypadku istotnych zmian w strukturze organizacyjnej lub zakresie realizowanych zadań;
- ✓ podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie;
- ✓ organizuje administrowanie danymi oraz określa właściwe techniki zabezpieczenia danych osobowych;
- ✓ na wniosek sporządzony przez samodzielne stanowisko ds. kadr, sporządzony wg wzoru stanowiącego **załącznik nr** 5 – ***Wniosek o nadanie upoważnienia do przetwarzania danych osobowych,*** upoważnia poszczególne osoby niezależnie od zajmowanego stanowiska do czynności przetwarzania danych osobowych w zakresie, odpowiadającym powierzonym czynnościom na danym stanowisku pracy (art. 29 RODO). Przy wydawaniu upoważnień administrator kieruje się tzw. zasadą wiedzy koniecznej w stosunku do osoby upoważnianej;
- ✓ na wniosek samodzielnego stanowiska ds. kadr odwołuje wcześniej wydane upoważnienia do przetwarzania danych osobowych (**załącznik nr 6 – *Wniosek o odwołanie upoważnienia do przetwarzania danych osobowych***);
- ✓ nadawanie i odbieranie upoważnień określa ***Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych*** **(Książka procedur)**;
- ✓ zlecenie i nadzór nad prowadzeniem ewidencji wydanych i odwołanych upoważnień do przetwarzania danych osobowych ***(wg załącznika nr 7 – Rejestr wydanych i odwołanych upoważnień),*** prowadzonej przez samodzielne stanowisko ds. kadr

- ✓ nadzór nad pozostałą dokumentacją z zakresu ochrony danych osobowych;
- ✓ zapewnienie pracownikom odpowiedniego wyposażenia stanowiska pracy i warunków pracy, umożliwiających przetwarzanie danych zgodnie z niniejszą polityką;
- ✓ wyznaczenie i powołanie Inspektora Ochrony Danych (dalej: IOD, inspektor) zgodnie z art. 37 oraz 38 RODO oraz wskazanie osoby lub podmiotu, który będzie administrował użytkowanymi w Urzędzie systemami informatycznymi oraz określenie zakresu zadań tej osoby.
- ✓ podejmowanie w porozumieniu z IOD odpowiednich działań w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia przetwarzania danych osobowych, w tym w szczególności jego niezwłoczne zgłoszenie organowi nadzorczemu w nieprzekraczalnym terminie 72 h (art. 33 RODO);
- ✓ we współpracy z IOD dokonuje oceny skutków przetwarzania danych osobowych dla praw lub wolności osób fizycznych (art. 35 RODO) lub zleca IOD przeprowadzenie tej oceny;
- ✓ sprawowanie nadzoru nad przestrzeganiem przyjętych zasad ochrony danych osobowych;
- ✓ sprawowanie nadzoru nad działaniami osoby administrującej systemami informatycznymi w Urzędzie;
- ✓ przeprowadzenie wspólnie z IOD analizy ryzyka procesu przetwarzania danych osobowych w formie zgodnej z przyjętą ***Metodologią analizy ryzyka*** stanowiącą **Załącznik nr 8** do niniejszej polityki informacji, pod kątem utraty atrybutów: poufności, dostępności, integralności. Przedmiotowa analiza jest wykonywana nie rzadziej niż raz w roku lub na skutek istotnych zmian organizacyjnych, czy też zmian zakresu działań realizowanych przez jednostkę;
- ✓ samodzielne lub we współpracy z IOD zorganizowanie, co najmniej raz w roku szkolenia z zakresu zasad przetwarzania danych osobowych dla pracowników jednostki. Szkolenie może przeprowadzić IOD;
- ✓ powierzenie w drodze pisemnego upoważnienia realizację swoich poszczególnych obowiązków jeżeli w jego ocenie istnieje taka konieczność: swojemu zastępcy, sekretarzowi Urzędu, samodzielnemu stanowisku ds. kadr, co jednak nie zwalnia go z odpowiedzialności za sposób ich realizacji;
- ✓ dobór podmiotów przetwarzających dane na rzecz Urzędu. Określa wymogi w stosunku do podmiotów przetwarzających, co do warunków przetwarzania, które są zawarte w umowie powierzenia danych osobowych do dalszego przetwarzania. Wzór ***Umowy powierzenia danych osobowych do dalszego przetwarzania*** stanowi **załącznik nr 9;**

6. Osoba/podmiot administrujący systemem informatycznym (ASI)

6.1 Administrator wyznacza, powołuje, zatwierdza wybór osoby, która będzie administrowała systemami informatycznymi użytkowanymi w Urzędzie. Niezależnie od sposobu powołania Administratora Systemu informatycznego (dalej: ASI), Burmistrz o fakcie tym powiadamia pracowników w drodze stosownego zarządzenia lub w innej formie przyjętej dla tego rodzaju komunikatów.

6.2 Funkcję administrowania systemem informatycznym może pełnić: pracownik jednostki lub podmiot zewnętrzny na zasadzie świadczenia usług. Niezależnie od sposobu powierzenia funkcji administratora systemu informatycznego, osoba ta realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemami informatycznymi, w tym zwłaszcza:

- ✓ nadzoruje i zarządza systemami informatycznymi, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- ✓ konfiguruje wszystkie stacje robocze w jednostce w sposób zapewniający, iż tylko z pozycji administratora dostępne będą opcje związane z konfiguracją zainstalowanego systemu operacyjnego oraz instalacją i aktualizacją zainstalowanego oprogramowania;
- ✓ instalację i usuwania oprogramowania systemowego, narzędziowego i jego aktualizację, gdyż jest jedyną osobą uprawnioną do tego rodzaju działań w Urzędzie. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania zadań Urzędu i posiadających ważną licencję użytkownika oraz dostęp do właściwych aktualizacji;
- ✓ opracowuje i aktualizuje dokumentację opisującą wykorzystywane w Urzędzie systemy informatyczne;
- ✓ podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego;
- ✓ opiniuje wszelkie przedsięwzięcia związane z wprowadzeniem nowych rozwiązań funkcjonalnych, oprogramowania oraz urządzeń w odniesieniu do funkcjonującego w Urzędzie systemu informatycznego. Wydane przez ASI opinie mogą mieć charakter wiążący i rozstrzygający;
- ✓ sprawuje nadzór nad wdrożonymi oraz wdrażaniem nowych środków technicznych i organizacyjnych zapewniających ochronę systemów informatycznych;
- ✓ nadzoruje stosowanie środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa użytkowanych systemów informatycznych w Urzędzie;
- ✓ przeciwdziała dostępowi osób niepowołanych do systemów informatycznych, w tym w szczególności do zasobów, w których przetwarzane są dane osobowe;
- ✓ na wniosek samodzielnego stanowiska ds. kadr **(sporządzony wg załącznika nr 5)** po uprzednim nadaniu uprawnień wskazanych we wniosku przez ADO, określa dla użytkownika dostęp do poszczególnych zasobów informatycznych funkcjonujących w Urzędzie, przydzielając każdemu z nich indywidualny login oraz dokonuje ewentualnych modyfikacji uprawnień do systemów informatycznych;
- ✓ prowadzi rejestr przydzielonych poszczególnym pracownikom loginów w odniesieniu do użytkowanych systemów informatycznych oraz pozostałe rejestry wymienione w niniejszym dokumencie;
- ✓ nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do zasobów informatycznych;
- ✓ podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

- ✓ wyrejestrowuje użytkowników systemu informatycznego na wniosek **(sporządzony wg załącznika nr 6)** przez samodzielne stanowisko ds. kadr, po uprzednim odebraniu uprawnień wskazanych we wniosku przez ADO wniosku przełożonych użytkownika;
- ✓ zapewnia i nadzoruje zmianę haseł w poszczególnych stacjach roboczych w sposób gwarantujący ich znajomość wyłącznie danemu użytkownikowi oraz, w razie stanu wyższej konieczności ADO;
- ✓ w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO oraz IOD o naruszeniu i współdziała z nimi przy usuwaniu skutków naruszenia;
- ✓ prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych zgodnie z wymogami określonymi w RODO;
- ✓ sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń i nośników komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych i ich przechowywaniem oraz okresowym ich sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych, w przypadki awarii systemu informatycznego;
- ✓ podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

6.3 Administrator systemu informatycznego ma prawo do:

- ✓ wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną systemów informatycznych funkcjonujących w Urzędzie;
- ✓ opiniowania możliwości wdrażania i rozbudowy systemów informatycznych o dodatkowe elementy (urządzenia, programy);
- ✓ wstępu do pomieszczeń w których użytkowane są systemy informatyczne i przeprowadzania niezbędnych badań lub innych czynności mających na celu zapewnienie prawidłowego funkcjonowania użytkowanych systemów informatycznych, w tym również poza godzinami pracy Urzędu po wcześniejszym ustaleniu tego z ADO;
- ✓ wnioskowania o złożenie pisemnych lub ustnych wyjaśnień przez pracowników Urzędu lub osób współpracujących w zakresie niezbędnym do ustalenia stanu faktycznego odnoszącego się do funkcjonowania systemów informatycznych oraz przyjętych zabezpieczeń;
- ✓ wglądu do dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli przyczyn naruszenia;
- ✓ dokonywania oględzin urządzeń, nośników służących do przetwarzania danych w systemach informatycznych Urzędu.

8. Inspektor Ochrony Danych

8.1 Burmistrz Łobza, jako administrator i podmiot przetwarzający jest obowiązany do wyznaczenia Inspektora Ochrony Danych na zasadach określonych w art. 37 RODO.

8.2 Administrator danych osobowych zapewnia:

- ✓ włączenie IOD we wszystkie sprawy dotyczące ochrony danych osobowych;
- ✓ wsparcie IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO;
- ✓ powstrzymywanie się przed wydawaniem IOD instrukcji dotyczących sposobu wykonywania zadań przez IOD;
- ✓ zobowiązanie się IOD do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań.

8.3 Do zadań IOD należy:

- ✓ informowanie Burmistrza oraz pracowników Urzędu, przetwarzających dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszej polityki oraz innych przepisów, w tym w szczególności RODO i doradzanie im w materii ochrony danych osobowych;
- ✓ monitorowanie przestrzegania niniejszej polityki, przepisów RODO, innych przepisów Unii lub państw członkowskich o ochronie danych, w tym podejmowanie działań zwiększających świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania oraz przeprowadzanie powiązanych z tym audytów;
- ✓ udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania zgodnie z art. 35 RODO;
- ✓ udzielanie wyjaśnień i pomocy w obszarze ochrony danych osobowych w reakcji na prośbę administratora lub Jego pracowników;
- ✓ weryfikacja pod katem zgodności z RODO opracowywanych umów powierzenia danych osobowych, klauzul informacyjnych i innych dokumentów z obszaru ochrony danych osobowych przedkładanych przez administratora lub jego pracowników;
- ✓ współpraca z organem nadzorczym, którym jest Prezes Urzędu Ochrony Danych Osobowych;
- ✓ pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz osób, których dane są przetwarzane we wszystkich kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
- ✓ przeprowadzenie minimum raz w roku szkolenia z obszaru ochrony danych osobowych dla wszystkich pracowników Urzędu oraz wystawienie imiennych zaświadczeń potwierdzających udział w szkoleniu;
- ✓ przeprowadzenie szkolenia wstępnego z zakresu ochrony danych osobowych nowo zatrudnionego pracownika w terminie 30 dni od dnia jego zatrudnienia;

- ✓ wykonanie na zlecenie ADO analizy ryzyka dla obszaru związanego z przetwarzaniem i ochroną danych osobowych.

- ✓ prowadzenie rejestru naruszeń.

9. Kierownik komórki organizacyjnej (samodzielne stanowisko)

9.1 Kierownik komórki organizacyjnej jest odpowiedzialny za ochronę danych osobowych w podległej jemu strukturze organizacyjnej.

9.2 Do jego obowiązków należy:

- ✓ określenie na poziomie zarządzanej komórki katalogu czynności przetwarzania danych osobowych i bieżące prowadzenie ***Rejestru czynności przetwarzania danych osobowych*** oraz ***Rejestru kategorii czynności przetwarzania***;

- ✓ określenie w ramach użytkowanej przez zarządzaną komórkę przestrzeni: miejsca przetwarzania i przechowywania danych osobowych w podziale na poszczególne pomieszczenia zajmowane przez komórkę, zgodnie z **załącznikiem nr 10 - *Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania***;

- ✓ sporządzenie wykazu zbiorów danych osobowych w zarządzanej komórce ze wskazaniem ich struktury, wykorzystywanych aplikacji do ich przetwarzania oraz wskazania miejsca przetwarzania (odrębnie dla każdego istniejącego zbioru danych osobowych);

- ✓ określenie w indywidualnych zakresach czynności poszczególnych pracowników, rodzaju czynności przetwarzania danych osobowych, które będą realizowane przez pracownika ze względu na powierzone obowiązki;

- ✓ bieżący nadzór nad funkcjonowaniem ustanowionych zabezpieczeń i przestrzeganiem zasad przetwarzania danych osobowych, określonych w **Rozdziale 3. Organizacja przetwarzania danych osobowych** oraz w **Rozdziale *13. Pozostałe zasady bezpiecznego przetwarzania danych osobowych,*** ze szczególnym uwzględnieniem prowadzenia i aktualizowania właściwych rejestrów;

- ✓ przeprowadzenie szkolenia stanowiskowego dla pracownika z uwzględnieniem przyjętych w jednostce zasad ochrony danych osobowych wynikających z niniejszego dokumentu.

- ✓ bieżące aktualizowanie indywidualnych zakresów obowiązków podległych pracowników pod katem realizowanych przez nich czynności przetwarzania danych osobowych;

- ✓ określenie wykazu czynności przetwarzania danych osobowych realizowanych przez każdego podległego pracownika oraz jego bieżące aktualizowanie i przekazanie do samodzielnego stanowiska ds. kadr;

- ✓ każdorazowo przy planowaniu powierzenia danych osobowych, przedłożenie IOD projektu umowy/porozumienia powierzenia danych. Przedmiotowe przedłożenie winno być zrealizowane odpowiednio wcześnie, aby umożliwić IOD zajęcie stanowiska w sprawie;

9.3. Dodatkowo do obowiązków **samodzielnego stanowiska ds. kadr** należy wnioskowanie do ADO o nadanie upoważnienia do czynności przetwarzania danych osobowych ujętych w RCPD dla poszczególnych użytkowników zgodnie z ich indywidualnymi zakresami czynności.

9.4 Upoważnienia o których mowa w pkt. 9.3 samodzielne stanowisko ds. kadr sporządza w3 egzemplarzach i odpowiada za ich obieg zapewniający uzyskanie odpowiedniego zatwierdzenia przez ADO oraz ASI.

9.5 Po nadaniu właściwych uprawnień przez ADO i ASI, pracownik zajmujący samodzielne stanowisko ds. kadr przekazuje wszystkie 3 egzemplarze do podpisu upoważnionemu użytkownikowi, który zatrzymuje jeden egzemplarz dla siebie, drugi egzemplarz pracownik ds. kadr przekazuje bezpośredniemu zwierzchnikowi użytkownika, a trzeci dołącza do prowadzonego **Rejestru wydanych odwołanych upoważnień do przetwarzania danych osobowych wg załącznika nr 7** do niniejszego dokumentu.

9.6 Upoważnienia sporządzone wg załącznika nr 5 są przechowywane przez okres zatrudnienia pracownika, a po zakończeniu zatrudnienia przez okres kolejnych 10 lat.

9.7 W przypadku nadania uprawnień do przetwarzania danych osobowych przez pracownika zajmującego samodzielne stanowisko ds. kadr, wniosek wg załącznika nr 5 sporządza pracownik zajmujący przedmiotowe stanowisko, wnioskując o nadanie przysługujących jemu uprawnień do czynności przetwarzania danych osobowych.

9.8 Wykaz czynności przetwarzania danych osobowych ujętych w RCPD, do których uprawniony jest pracownik na samodzielnym stanowisku ds. kadr określa ADO w jego indywidualnym zakresie obowiązków

10. Osoba upoważniona do przetwarzania danych osobowych

10.1 Osoba upoważniona do przetwarzania danych osobowych (użytkownik), to każda osoba spełniająca kryteria definicji zawartej w Rozdziale **2. Definicje**, w tym również kierownik komórki oraz osoby na samodzielnych stanowiskach.

10.2 Każdy użytkownik bez jakiegokolwiek wyjątku jest zobowiązany do przestrzegania zasad przetwarzania danych osobowych określonych w niniejszym dokumencie, ze szczególnym uwzględnieniem zapisów zawartych ***Rozdziale 3. Organizacja przetwarzania danych osobowych*** oraz w **Rozdziale *13. Pozostałe zasady bezpiecznego przetwarzania danych osobowych.***

10.3 Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do złożenia pisemnego oświadczenia o zachowaniu w tajemnicy danych osobowych i przestrzegania zasad i procedur określonych niniejszym dokumentem przez cały okres zatrudnienia oraz zachowania tajemnicy danych osobowych po ustaniu okresu zatrudnienia – treść oświadczenia zawiera wniosek o udzielenie upoważnienia (załącznik nr 5).

10.4 Naruszenie przez osobę upoważnioną do przetwarzania danych osobowych, zasad określonych niniejszą polityką, w tym w szczególności tajemnicy danych osobowych lub procedur bezpiecznego ich przetwarzania na skutek świadomego działania, będzie traktowane, jako ciężkie naruszenie obowiązków pracowniczych, uzasadniające rozwiązanie umowy o pracę bez wypowiedzenia.

10.5 Użytkownik może przetwarzać dane osobowe wyłącznie w zakresie objętym upoważnieniem i tylko w celu wykonywania nałożonych na niego obowiązków służbowych.

10.6 W przypadku sytuacji niezamierzonego nieuprawnionego przetwarzania danych osobowych (np.

na skutek otrzymania pisma zawierającego niechciane i zbędne kategorie danych), użytkownik taki stan rzeczy odnotowuje w ***Rejestrze zdarzeń nieuprawnionego przetwarzania danych osobowych*** (wzór stanowi **załącznik nr 11**), który jest prowadzony na szczeblu każdej komórki organizacyjnej oraz samodzielnego stanowiska.

10.7 Dane osobowe będące przedmiotem niezamierzonego nieuprawnionego przetwarzania, winny bezzwłocznie zostać zanonimizowane (zatarte, zakorektorowane w sposób uniemożliwiający ich odczytanie).

10.8 Wszyscy użytkownicy przetwarzający dane osobowe zobowiązani są do:

- ✓ zapoznania się przepisami Polityki ochrony danych osobowych wraz ze wszystkimi dokumentami wchodzącymi w jej skład oraz z przepisami prawa w zakresie ochrony danych osobowych, w tym w szczególności z przepisami RODO;
- ✓ odpowiedniego zabezpieczania danych osobowych przed ich udostępnieniem osobom nieupoważnionym;
- ✓ korzystania z systemu informatycznego administratora danych w sposób zgodny z Instrukcją zarządzania systemem informatycznym oraz zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
- ✓ korzystania z urządzeń wchodzących w skład systemu informatycznego, tylko i wyłacznie w celach służbowych.

11. Środki techniczne i organizacyjne, służące zapewnieniu bezpieczeństwa procesowi przetwarzania danych

11.1 Opisane środki techniczne i organizacyjne są stosowane, aby zapewnić bezpieczeństwo danych osobowych, przetwarzanych w Urzędzie, a tym samym ograniczyć ryzyko naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane.

11.2 Środki techniczne i organizacyjne, które zostały wskazane w niniejszym rozdziale są efektem przeprowadzonej analizy ryzyka zagrożeń procesów przetwarzania danych osobowych w Urzędzie, w sposób zgodny z metodologią wskazaną w **załączniku nr 8** *(Metodologia analizy ryzyka),* do niniejszej polityki.

11.3 Na zabezpieczenia o charakterze technicznym składają się:

- ✓ ochrona przed nieuprawnionym dostępem do obszarów przetwarzania realizowana poprzez:
  - o stosowanie systemów alarmowych załączanych po godzinach pracy Urzędu, monitorowanych przez zewnętrzną, llicencjonowaną firmę z branży ochrony osób i mienia,
  - o stosowanie zamków mechanicznych do pomieszczeń stanowiących miejsca przetwarzania danych osobowych,
  - o zabezpieczenie obszarów przetwarzania danych w godzinach pracy przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych oraz po

godzinach pracy z wykorzystaniem zamków mechanicznych, w które są wyposażone drzwi do wszystkich obszarów przetwarzania,
- ograniczenie możliwości przebywania w obszarach przetwarzania danych osobowych, osób nieupoważnionych tylko i wyłącznie do sytuacji, kiedy jest to realizowane w obecności upoważnionych pracowników Urzędu,
- zastosowanie monitoringu wizyjnego na terenie Urzędu umożliwiającego odtworzenie dowolnego przedziału czasowego za okres do 1 miesiąca wstecz;

✓ ochrona nośników danych osobowych realizowana jest poprzez:
- przechowywanie nośników zawierających dane osobowe w miejscach ich przetwarzania wyłącznie w szafach, kontenerach lub biurkach które są wyposażonych w zamknięcia mechaniczne,
- wyposażenie wszystkich pomieszczeń znajdujących się w wykazie miejsc przetwarzania danych osobowych w miarę możliwości w mechaniczne niszczarki dokumentów,
- okresowe działania o charakterze konserwacyjnym w odniesieniu do infrastruktury technicznej, związanej z przetwarzaniem danych osobowych;

✓ ochrona przeciwpożarowa realizowana poprzez, wyposażenie pomieszczeń składających się na obszary przetwarzania danych osobowych w sprzęt p.poż.;

✓ ochrona przed awariami realizowana jest:
- wyposażenie urządzeń serwerowych w awaryjne zasilanie tzw. UPS,
- klimatyzowanie pomieszczeń, w których zlokalizowane są serwery (jeżeli serwery znajdują się na terenie Urzędu i są pod nadzorem Urzędu);

✓ zabezpieczenia realizowane we własnym zakresie przez użytkownika, wynikające z przyjętych przez Urząd standardów, do których możemy zaliczyć:
- ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
- dbania o prawidłową wentylację komputerów (kategoryczny zakaz ustawiania jednostek komputerowych w sposób zasłaniający kratki wentylatorów meblami, ścianą),
- niepodłączania do listew, podtrzymujących napięcie, przeznaczonych dla zasilania sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejnikiów, czajników, wentylatorów),
- wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie,
- kończenia pracy stacji roboczej poprzez prawidłowe wylogowanie się z systemu i wyłączenie komputera,
- niszczenie w niszczarce lub chowanie do szaf zamykanych na klucz, wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy,
- niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,

- umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
- zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
- zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
- zamykania drzwi na klucz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym kierownika komórki, który w danym dniu zgłasza osobie sprzątającej, jednorazową rezygnację z wykonywania usługi sprzątania,
- przestrzeganie „zasady czystego biurka i ekranu" zgodnie, z którą nie należy pozostawiać na biurku po zakończeniu pracy lub na czas krótkotrwałej nieobecności dokumentów oraz niewygaszonych monitorów wyświetlających informacje. Powyższa zasada ma zastosowanie również do urządzeń typu skaner, drukarka, niszczarka. Za niedopuszczalne należy uznać pozostawiania na ww. urządzeniach wydrukowanych, poddawanych skanowaniu, czy też przeznaczonych do zniszczenia dokumentów;
- niezwłoczne usuwanie skanowanych dokumentów z pamięci urządzeń skanujących natychmiast po ich wykorzystaniu (zapisaniu skanu na nośniku lub wydrukowaniu),
- natychmiastowe kasowanie danych na dyskach przenośnych po ich wykorzystaniu,
- chwilowe opuszczanie stanowiska pracy jest możliwe po uprzednim aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

✓ pozostałe zabezpieczenia o charakterze technicznym w odniesieniu do wykorzystywanych systemów informatycznych zostały określone w ***Instrukcji zarządzania systemem informatycznym,*** stanowiącym integralną część systemu ochrony danych osobowych.

11.4 Na zabezpieczenia o charakterze organizacyjnym składają się:

✓ dokumentacja składająca się na Politykę ochrony danych osobowych zawierająca:
- opis zasad i wymogów w odniesieniu do procesu bezpiecznego przetwarzania danych osobowych,
- opis procesu reakcji na stwierdzone naruszenie – ***Procedura reakcji na ujawnione naruszenie*** **(Książka procedur),**
- podział obowiązków i kompetencji uczestników procesu przetwarzania danych osobowych,
- obowiązki dokumentowania istotnych okoliczności związanych z przetwarzaniem danych osobowych w formie właściwych rejestrów,
- obowiązek realizacji okresowych rocznych przeglądów wdrożonego systemu bezpieczeństwa,
- realizowany w sposób bieżący nadzór nad adekwatnością przyjętych rozwiązań w stosunku do istniejących zagrożeń, wynikający z faktu przeprowadzenia okresowych analiz ryzyka zagrożeń,

✓ środki o charakterze osobowym, do których zalicza się:

- obowiązek przedłożenia Informacji z Krajowego Rejestru Karnego o niekaralności za przestępstwa umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwa skarbowe przez pracownika zatrudnianego na stanowisku urzędniczym,

- obowiązek złożenia zobowiązania w formie oświadczenia przez wszystkich pracowników jednostki (zajmujących stanowiska urzędnicze w treści załącznika nr 5, jak i nieurzędnicze wg wzoru stanowiącego załącznik nr 12) o zachowaniu w poufności danych osobowych, do których przetwarzania zostali upoważnieni oraz danych osobowych, do których uzyskali dostęp w sposób niezamierzony – wzór ***Oświadczenia dla osób zatrudnionych na nieurzędniczych stanowiskach pracy*** stanowi **załącznik nr 12**;

✓ objęcie systemem szkoleń indywidualnych i grupowych wszystkich użytkowników z zakresu:
- przepisów i procedur, dotyczących ochrony danych osobowych,
- sposobów ochrony danych przed osobami postronnymi i procedur udostępniania danych osobom, których dane dotyczą,
- obowiązków osób upoważnionych do przetwarzania danych osobowych,
- odpowiedzialności za naruszenie obowiązków z zakresu ochrony danych osobowych;

✓ zabezpieczenia realizowane we własnym zakresie przez użytkownika, wynikające z przyjętych przez Urząd standardów, do których możemy zaliczyć:
- niepozostawienia bez kontroli dokumentów i nośników danych, w strefach określanych mianem publicznych, do których zaliczamy ciągi komunikacyjne oraz miejsca w Urzędzie, do których mają dostęp klienci,
- pilnego strzeżenia akt i wymiennych nośników pamięci,
- nieużywania powtórnie dokumentów zadrukowanych jednostronnie,
- niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,
- powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych, przed samodzielną ingerencją w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
- niewynoszenia poza siedzibę Urzędu, na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
- zachowania tajemnicy danych, w tym także wobec najbliższych,
- przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego loginu i hasła oraz stosowania się do zaleceń ASI,
- kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania powierzonych pracownikowi obowiązków. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne, elektroniczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane

✓ powołanie Inspektora Ochrony Danych, który ze względu na posiadaną autonomię w

działaniu, wspomaga administratora w sprawowaniu nadzoru nad procesami związanymi z przetwarzaniem danych osobowych.

12. Infrastruktura przetwarzania danych osobowych

12.1 Infrastrukturę przetwarzania danych osobowych tworzą budynki i pomieszczenia, systemy informatycznie oraz pozostałe aktywa będące nosnikami danych wykorzystywane przez Urząd.

12.2 Opis infrastruktury informatycznej oraz nośników danych wykorzystywanych przez Urząd zawiera dokument ***Instrukcja zarządzania systemem informatycznym.***

12.3 ***Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania (załącznik nr 10)*** określa wszystkie pomieszczenia, w których:

- ✓ dokonuje się przetwarzania danych osobowych;
- ✓ przechowuje się wszelkie nośniki zawierające dane osobowe;
- ✓ przechowuje się uszkodzone, wycofane z użytku komputery, nośniki danych.

12.4 ***Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania*** jest prowadzony odrębnie na poziomie każdej komórki organizacyjnej. Za bieżace prowadzenie wykazu odpowiedzialność ponosi kierownik komórki organizacyjnej bądź odpowiednio osoba zajmująca samodzielne stanowisko.

12.5 Ze względu na nagromadzenie danych osobowych, szczególnie chronione powinny być pomieszczenia:

- ✓ serwerowni jeżeli jednostka je posiada;
- ✓ w których przechowywana jest dokumentacja kadrowo - płacowa;
- ✓ w których przechowywana jest dokumentacja związana z ewidencją ludności;
- ✓ pomieszczenia archiwum.

12.6 W pomieszczeniach, o których mowa w pkt. 12.5 mogą przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych, pracownicy merytoryczni, których stanowiska pracy są przypisane do przedmiotowych pomieszczeń, ADO, ASI, IOD, a inne osoby wyłącznie pod ich nadzorem.

12.7 Zabrania się przetwarzania danych osobowych w pomieszczeniach innych niż wymienione w wykazie, o którym mowa w pkt. 12.3 i 12.4.

12.8 Informacje zawarte w **załączniku nr 10** do niniejszej polityki mają charakter informacji wyłącznie do użytku wewnętrznego i nie podlegają upublicznieniu.

13. Pozostałe zasady bezpiecznego przetwarzania danych osobowych

13.1 Wykorzystywanie akt i dokumentów, zawierających dane osobowe po godzinach pracy jednostki poza jej siedzibą tj. poza określonymi w **załącznku nr 10** obszarami jest zabronione.

13.2 Wykorzystywanie służbowych urządzeń przenośnych służących przetwarzaniu danych osobowych (laptopy, netbooki) jest możliwe tylko po uzyskaniu pisemnej zgody, udzielanej przez ADO oraz zgłoszeniu tego faktu administratorowi systemu informatycznego. Wzór ***Zgody na użytkowanie urządzeń służbowych poza siedzibą jednostki*** stanowi **załącznik nr 13.**

13.3 W sytuacji, o której mowa w pkt. 13.2 administrator systemu informatycznego jest zobowiązany do zaszyfrowania dysków zainstalowanych w jednostce komputerowej oraz prowadzi ewidencję sprzętu użytkowanego poza siedzibą jednostki przez uprawnionych pracowników.

13.4 Pracownicy wykorzystujący sprzęt poza siedzibą jednostki, są obowiązani do ochrony informacji w nich zapisanych. Ponadto odpowiadają materialnie w pełnej wysokości odpowiadającej wartości odtworzeniowej użytkowanego sprzętu z uwzględnieniem wartości odtworzeniowej zainstalowanego oprogramowania oraz wartości innych wydatków, jakie ewentualnie będzie musiał ponieść Urząd wynikających z utraty informacji, których nośnikiem był utracony sprzęt.

13.5 Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

- ✓ dane osobowe z nośników przenośnych, niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych, powinny być trwale usuwane z tych nośników programem trwale usuwającym pliki lub gdy nie ma takiej możliwości zniszczone (np. płyty CD-ROM);

- ✓ jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów), mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych, nośniki powinny być trwale kasowane lub niszczone;

- ✓ uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie;

- ✓ zabrania się powtórnego używania do sporządzania brudnopisów, pism jednostronnie zadrukowanych jeśli zawierają one dane osobowe;

- ✓ po wykorzystaniu wydruków zawierających dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć je w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku, ani też wynosić poza obszary przetwarzania danych osobowych.

14. Przeglądy okresowe, zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych

14.1 ADO zleca przeprowadzenie raz w roku przeglądu czynności przetwarzania danych osobowych pod kątem celowości i zasadności ich realizacji. Powyższy przegląd może zostać zrealizowany w ramach rocznego przeglądu Polityki Bezpieczeństwa Informacji, którego obowiązek wykonania wynika z Krajowych Ram Interoperacyjności. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza osoby przetwarzające dane osobowe, są obowiązane współpracować z osobą dokonującą przeglądu i wskazywać jej czynności, które powinny zostać usunięte, ze względu na zrealizowanie celu przetwarzania lub brak ich adekwatności do realizowanego celu.

14.2 ADO może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych u administratora danych, jak i każdej innej sytuacji, która w ocenie ADO lub IOD, będzie wymagała przeprowadzenia takiego przeglądu.

15. Udostępnianie danych osobowych

15.1 Udostępnianie danych osobowych policji, sądom oraz pozostałym organom ściganiu lub wymiaru sprawiedliwości, może nastąpić w związku z prowadzonym przez te instytucje postępowaniem.

15.2 Udostępnianie informacji podmiotom, o których mowa w pkt. 15.1 odbywa się według następującej procedury **(Procedura udostępniania danych osobowych – Książka procedur)**:

- ✓ udostępnianie danych osobowych podmiotom, o których mowa w pkt. 15.1 może nastąpić po przedłożeniu przez nie wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

  - oznaczenie wnioskodawcy,
  - wskazanie przepisów uprawniających do dostępu do informacji,
  - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
  - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

15.3 Udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego, może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

15.4 Osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

15.5 Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

16. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

16.1 Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

17. Postanowienia końcowe

17.1 Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
17.2 Dopuszcza się prowadzenie ewidencji i rejestrów stanowiących załączniki do niniejszego dokumentu w wersji elektronicznej.

Załączniki:

Załącznik nr 1 – Struktura organizacyjna jednostki;

Załącznik nr 2 – Rejestr czynnosci przetwarzania danych osobowych;

Załącznik nr 3 – Rejestr ategorii czynnosci przetwarzania;

Załącznik nr 4 – Wzór informacji (z art. 13 oraz art. 14 RODO);

Załącznik nr 5 - Wniosek o nadanie upoważnienia do przetwarzania danych osobowych;

Załącznik nr 6 – Wniosek o odwołanie upoważnienia do przetwarzania danych osobowych;

Załącznik nr 7 – Rejestr wydanych i odwołanych upoważnień;

Załącznik nr 8 - Metodologia analizy ryzyka;

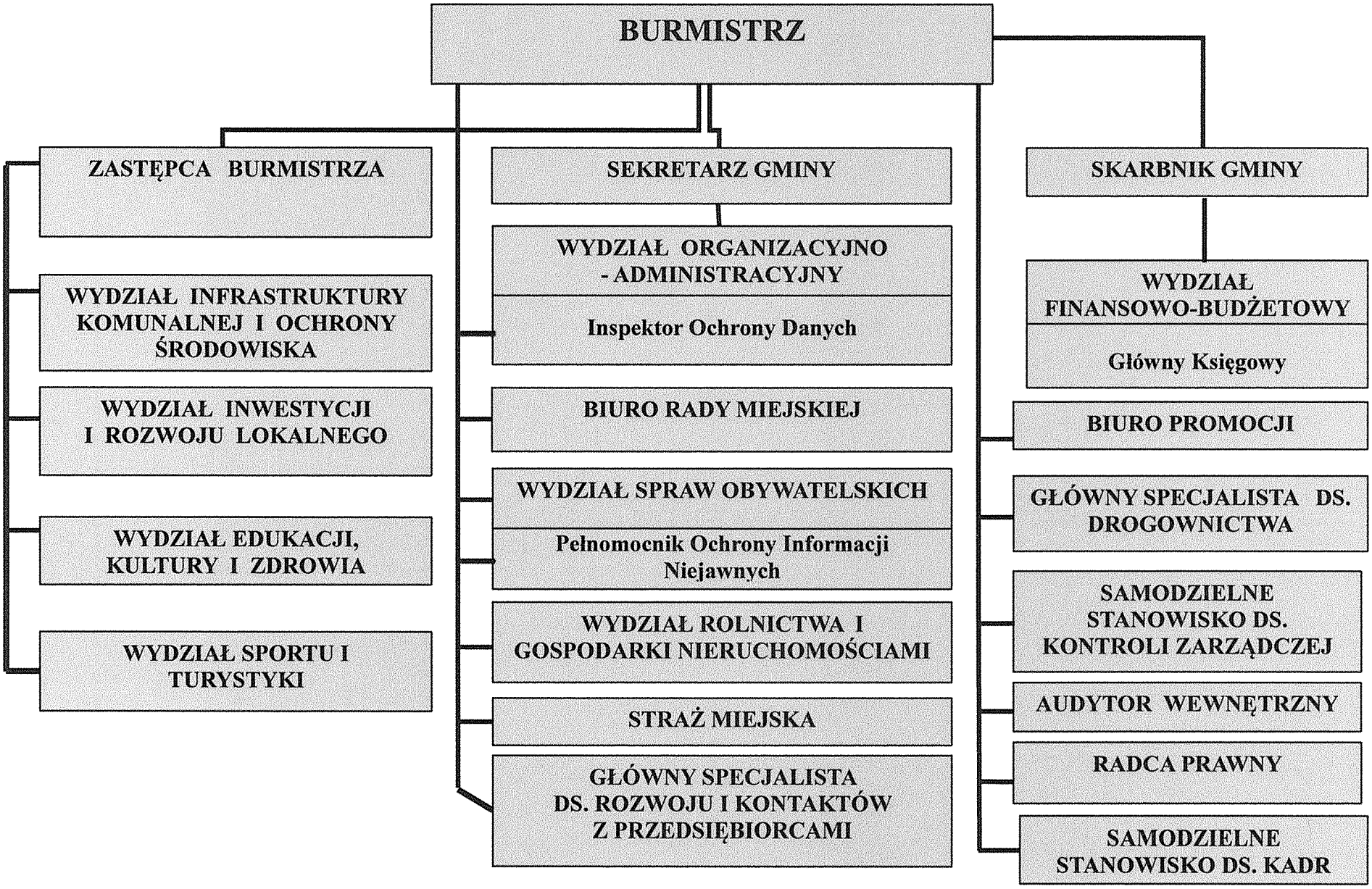
Załącznik nr 9 – Wzór umowy powierzenia danych osobowych do dalszego przetwarzania;

Załącznik nr 10 – Wykaz budynków, pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania;

Załącznik nr 11 - Rejestr zdarzeń nieuprawnionego przetwarzania danych osobowych;

Załącznik nr 12 – Oświadczenie dla osób zatrudnionych na nie urzędniczych stanowiskach pracy;

Załącznik nr 13 – Zgoda na użytkowanie urządzeń służbowych poza siedzibą jednostki;


BURMISTRZ
ZASTĘPCA BURMISTRZA
WYDZIAŁ INFRASTRUKTURY KOMUNALNEJ I OCHRONY ŚRODOWISKA
WYDZIAŁ INWESTYCJI I ROZWOJU LOKALNEGO
WYDZIAŁ EDUKACJI, KULTURY I ZDROWIA
WYDZIAŁ SPORTU I TURYSTYKI
SEKRETARZ GMINY
WYDZIAŁ ORGANIZACYJNO - ADMINISTRACYJNY
Inspektor Ochrony Danych
BIURO RADY MIEJSKIEJ
WYDZIAŁ SPRAW OBYWATELSKICH
Pełnomocnik Ochrony Informacji Niejawnych
WYDZIAŁ ROLNICTWA I GOSPODARKI NIERUCHOMOŚCIAMI
STRAŻ MIEJSKA
GŁÓWNY SPECJALISTA DS. ROZWOJU I KONTAKTÓW Z PRZEDSIĘBIORCAMI
SKARBNIK GMINY
WYDZIAŁ FINANSOWO-BUDŻETOWY
Główny Księgowy
BIURO PROMOCJI
GŁÓWNY SPECJALISTA DS. DROGOWNICTWA
SAMODZIELNE STANOWISKO DS. KONTROLI ZARZĄDCZEJ
AUDYTOR WEWNĘTRZNY
RADCA PRAWNY
SAMODZIELNE STANOWISKO DS. KADR

Nazwa (określenie) czynności przetwarzania danych osobowych	Numer kolejny .....
Rejestr czynności przetwarzania danych osobowych, dla których administratorem jest Burmistrz Łobza z siedzibą: ul. Niepodległosci 13, 73-150 Łobez, tel. 91 39 740 01/02, adres e-mail: lobez@lobez.pl	
Współadministratorzy danych – nazwa, adres siedziby, dane kontaktowe (jeżeli wystepują)	Brak
Dane kontaktowe Inspektora Ochony Danych	
Nazwa, określenie komórki prowadzącej rejestr	
Cel przetwarzania danych osobowych	
Podstawa prawna przetwarzania danychj osobowych	
Opis kategorii osób, których dane osobowe są przetwarzane	
Odbiorcy lub kategorie odbiorców, którym dane zostały lub będą ujawnione	

Kategorie danych osobowych będących przedmiotem przetwarzania	
Informacja o maszynowym przetwarzaniu danych osobowych i profilowaniu	
Wskazanie źródła danych	
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	
Planowany termin usunięcia danych osobowych	
Opis technicznych i organizacyjnych środków bezpieczeństwa	

Nazwa (określenie) kategorii czynności przetwarzania danych osobowych	**Numer kolejny** .....
Rejestr kategorii czynności przetwarzania danych osobowych, dla których przetwarzającym jest Burmistrz Łobza z siedzibą: ul. Niepodległości 13, 73-150 Łobez, tel. 91 39 740 01/02, adres e-mail: lobez@lobez.pl	
Administrator na rzecz, którego przetwarzane są dane osobowe – nazwa, adres siedziby, dane kontaktowe	
Dane kontaktowe Inspektora Ochony Danych	
Nazwa, określenie komórki prowadzącej rejestr	
Kategoria czynności przetwarzania na rzecz administratora	
Informacje o przekazaniu do państwa trzeciego lub organizacji między-narodowej	
Opis technicznych i organizacyjnych środków bezpieczeństwa	Zgodnie z opisem przyjętym w polityce ochrony danych osobowych

Informacja dla osoby udostępniającej dane osobowe

Administratorem Pani/Pana/dziecka danych osobowych jest:
Burmistrz Łobza z siedzibą: ul. Niepodległości 13, 73-150 Łobez. Z administratorem danych można się skontaktować poprzez adres e-mail: lobez@lobez.pl lub telefonicznie pod numerem 91 39 740 01/02 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.
Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iod@lobez.pl lub pisemnie na adres siedziby administratora. Z inspektorem ochrony danych można się kontaktować, w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.

Cele i podstawy przetwarzania.
Podane przez Panią/Pana* dane osobowe będą przetwarzane w celu: .....
Pani/Pana dane są przetwarzane na podstawie: .....
.....

Odbiorcy danych osobowych.
Odbiorcami Pani/Pana* danych osobowych będą: .....

oraz jednostki administracji publicznej uprawnione do sprawowania kontroli i nadzoru nad prawidłowością funkcjonowania Urzędu Gminy w Kołbaskowie lub mogące potwierdzić prawdziwość podanych przez Panią/Pana* informacji.

Okres przechowywania danych.
Pani/Pana* dane będą przechowywane przez okres ..... lat poczynając od 1 stycznia roku następnego, który to wynika z przyjętego w jednostce Jednolitego Rzeczowego Wykazu Akt.

Sposób przetwarzania danych osobowych
Pani/Pana* dane nie będą/ będą* przetwarzane w sposób zautomatyzowany oraz zostaną poddane/ nie zostaną poddane* profilowaniu.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Pani/Panu*:

a) prawo dostępu do swoich danych oraz otrzymania ich kopi,
b) prawo do sprostowania (poprawiania) swoich danych,
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej,
d) prawo do ograniczenia przetwarzania danych,
e) prawo do wniesienia skargi do Prezesa UODO na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa.

Informacja o wymogu podania danych.
Podanie przez Państwa danych jest wymogiem ustawowym/dobrowolnym*.

*niepotrzebne skreślić

Informacja dla osoby, której dane dotyczą, a zostały pozyskane w sposób inny niż od niej bezpośrednio

Administratorem Pani/Pana/dziecka danych osobowych jest:
Burmistrz Gminy Łobez z siedzibą: ul. Niepodległości 13, 73-150 Łobez. Z administratorem danych można się skontaktować poprzez adres e-mail: lobez@lobez.pl lub telefonicznie pod numerem 91 39 740 01/02 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.
Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iod@lobez.pl lub pisemnie na adres siedziby administratora. Z inspektorem ochrony danych można się kontaktować, w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.

Cele i podstawy przetwarzania.
Podane przez Panią/Pana* dane osobowe będą przetwarzane w celu:
.....
Pani/Pana* dane są przetwarzane na podstawie:
.....

Odbiorcy danych osobowych.
Odbiorcami Pani/Pana* danych osobowych będą:
.....
oraz jednostki administracji publicznej uprawnione do sprawowania kontroli i nadzoru nad prawidłowością funkcjonowania Urzędu Gminy Kołbaskowo lub mogące potwierdzić prawdziwość podanych przez Panią/Pana* informacji.

Okres przechowywania danych.
Pani/Pana* dane będą przechowywane przez okres ..... lat poczynając od 1 stycznia roku następnego, który to wynika z przyjętego w jednostce Jednolitego Rzeczowego Wykazu Akt.

Sposób przetwarzania danych osobowych
Pani/Pana* dane nie będą/ będą* przetwarzane w sposób zautomatyzowany oraz zostaną poddane/ nie zostaną poddane* profilowaniu.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Pani/Panu*:

a) prawo dostępu do swoich danych oraz otrzymania ich kopi,
b) prawo do sprostowania (poprawiania) swoich danych,
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej,
d) prawo do ograniczenia przetwarzania danych,
e) prawo do wniesienia skargi do Prezesa UODO na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa.

Informacja o wymogu podania danych.
Podanie przez Państwa danych jest wymogiem ustawowym/dobrowolnym*.

Przetwarzane kategorie danych:
.....

Źródło danych
Źródłem Pani/Pana* danych jest: .....

*niepotrzebne skreślić

Wniosek o nadanie upoważnienia do przetwarzania danych osobowych

Na podstawie pkt. 5.3 *Polityki ochrony danych osobowych* oraz art. 29 RODO w związku z wykonywaniem obowiązków służbowych/zleconych[1] przez Panią/Pana[1] .....

(imię i nazwisko osoby upoważnianej)

wnoszę o nadanie upoważnienia dla wskazanej osoby do nw. czynności przetwarzania[2] danych osobowych zawartych w *Rejestrze czynności przetwarzania danych osobowych* prowadzonym przez:

.....

(określenie nazwy komórki/stanowiska)

1. .....
2. .....
3. .....
4. .....

.....

(data i podpis wnioskodawcy)

Upoważnienie nr ..... z dnia .....

Działając na podstawie pkt. 5.3 Polityki ochrony danych osobowych oraz art. 29 RODO upoważniam **Panią/Pana**[2] ..... do realizacji czynności przetwarzania w zakresie wskazanym we wniosku o nadanie upoważnienia, wyłącznie w związku z wykonywaniem obowiązków służbowych/zleconych*.

Upoważnienie jest udzielone na czas trwania zatrudnienia/realizacji umowy nr ..... z dnia* .....

Upoważnienie wygasa z dniem zakończenia zatrudnienia/realizacji umowy* lub z dniem jego odwołania.

.....

(data i podpis administratora danych osobowych)

1. Niepotrzebne skreślić.
2. Należy podać nazwy czynności przetwarzania określone w *Rejestrze czynności przetwarzania danych osobowych* prowadzonym przez komórkę lub określić je kolejnymi numerami, za jakimi są one ujęte w przedmiotowym rejestrze.

Uprawnienia do systemu informatycznego

W związku z wydanym upoważnieniem do realizacji czynności przetwarzania danych osobowych przyznaję **Pani/Panu**[1].....

(imię i nazwisko, stanowisko)

Login / loginy[1] do niżej wymienionych zasobów informatycznych:

1. .....
2. .....
3. .....

.....

(data i podpis administratora systemu informatycznego)

Pouczenie:

Osoba upoważniona do przetwarzania danych jest zobowiązana zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, w tym także po ustaniu zatrudnienia, odwołaniu upoważnienia lub upływie jego ważności. Nie wywiązanie się z przyjętego zobowiązania skutkować będzie odpowiedzialnością karną wynikającą z art. 266 Kodeksu karnego.

Oświadczenie:

Oświadczam, że zapoznałam/zapoznałem się z obowiązującą *Polityką ochrony danych osobowych* oraz przepisami dotyczącymi ochrony danych osobowych, w szczególności 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) (Dz.U.UE L z dnia 4 maja 2016 r.)* i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach. Jednocześnie zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznam się w trakcie wykonywania powierzonych mi obowiązków oraz sposobów ich zabezpieczenia, zarówno w okresie zatrudnienia/realizacji umowy[1], jak też po jego ustaniu.

.....

(data i podpis upoważnionego)

1. Niepotrzebne skreślić.
2. Należy podać nazwy czynności przetwarzania określone w *Rejestrze czynności przetwarzania danych osobowych* prowadzonym przez komórkę lub określić je kolejnymi numerami, za jakimi są one ujęte w przedmiotowym rejestrze.

Wniosek o odwołanie upoważnienia do przetwarzania danych osobowych

Na podstawie pkt. 5.3 Polityki ochrony danych osobowych wnoszę o odwołanie upoważnienia do czynności przetwarzania danych osobowych, nr .....z dnia .....wydanego dla Pani/Pana .....zawartych w *Rejestrze czynności przetwarzania danych osobowych*

(imię i nazwisko upoważnionego)

prowadzonym przez:

.....

(określenie nazwy komórki/stanowiska)

Jednocześnie wnoszę o wyrejestrowanie ww. osoby, jako użytkownika systemu informatycznego i zablokowanie konta użytkownika. pracującego pod loginem .....
.....

(określenie loginu/loginów jakimi posługiwał się w systemach informatycznych upoważniony)

.....
(podpis wnioskodawcy)

Odwołanie upoważnienia

Działając na podstawie pkt. 5.3 Polityki ochrony danych osobowych oraz art. 29 RODO odwołuję upoważnienie nr ..... z dnia ..... wydane **Pani/Panu*** ....

(imię i nazwisko upoważnionego)

.....
(data i podpis administratora danych osobowych)

Odwołanie uprawnień do systemu informatycznego

Odbieram **Pani/Panu*** .....

(imię i nazwisko, stanowisko)

dostęp do systemu/systemów informatycznych, do których logowanie realizowane było z użyciem

loginu/loginów[1]: .....

(określenie loginu/loginów jakimi posługiwał się w systemach informatycznych upoważniony)

.....

1- niepotrzebne skreślić

(data i podpis administratora systemu informatycznego)

1- niepotrzebne skreślić

Rejestr wydanych i odwołanych upoważnień do przetwarzania danych osobowych

L.p.	Nr Upoważnienia	Nazwisko	Imię	Data nadania	Zakres upoważnienia (wskazanie czynności z nazwy lub podanie jej nr w RCPD)	Data odebrania	Odebrany zakres upoważnienia (w całości/w części – wskazanie nr czynności z RCPD w stosunku, do których odebrano upoważnienie)

Metodologia analizy ryzyka

Proces zarządzania ryzykiem jest integralną częścią działalności Urzędu. Urząd, jako organizacja dysponuje zbiorem zasobów o określonej wartości służących przetwarzaniu informacji, bądź takimi, które same w sobie są ich nośnikiem (np.: dyski komputerów, teczki spraw, przenośne nośniki pamięci itd.). Z tego względu działaniami związanymi z zapewnieniem bezpieczeństwa przetwarzania danych osobowych należy również objąć zasoby, które nie stanowią bezpośrednio informacji i nie są jej nośnikiem, lecz służą jej przetwarzaniu np. system zasilania w energię elektryczną, która jest niezbędna dla pracy systemów komputerowych. Powyższe stanowisko wynika z zapisów ustanowionych przez PN-ISO/IEC 27001:2007, które w tym samym stopniu nakazują chronić zarówno informacje, jak i pozostałe zasoby służące jej przetwarzaniu. Sposoby zabezpieczenia danych osobowych, będących specyficznym rodzajem informacji oraz zasobów wynikają z analizy zagrożeń na jakie są one narażone oraz podatności wynikających z ich indywidualnych cech. Podatność należy rozumieć, jako wady lub luki w strukturze fizycznej, organizacji, procedurach sprzęcie, oprogramowaniu, które mogą być wykorzystane do spowodowania szkód w posiadanych zasobach. Istnienie podatności samo z siebie nie powoduje szkód. Podatność jest jedynie cechą lub ich zestawem, które mogą być świadomie lub nieświadomie wykorzystane do uszkodzenia. Występowanie zagrożeń przy braku podatności nie generuje ryzyka. Przykładowymi podatnościami są:

- niechronione połączenia,
- nieograniczona możliwość stosowania przez użytkowników przenośnych nośników pamięci,
- nieograniczony dostęp użytkowników do zasobów internetowych,
- swoboda i nieograniczony dostęp użytkowników do poczty zewnętrznej,
- nieprzeszkoleni użytkownicy,
- niewłaściwy wybór i użycie haseł,
- brak właściwej kontroli dostępu (logicznej i/lub fizycznej) do zasobów, czy też obszarów przetwarzania,
- brak kopii zapasowych danych lub kopii oprogramowania,
- pojedyncze egzemplarze ważnych urządzeń,
- lokalizacja w obszarze podatnym na wandalizm, zalanie, terroryzm, kradzież.

Podsumowując można przyjąć, że zarządzanie ryzykiem to całkowity proces podzielony na etapy związany z identyfikacją, kontrolowaniem i eliminacją lub minimalizowaniem prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informacyjnego.

Etap 1 Identyfikacja zasobów służących przetwarzaniu informacji

Na tym etapie należy określić posiadane przez Urząd zasoby i aktywa informacyjne mające dla niego wartość wymierną, jak i niewymierną, w stosunku do których należy podjąć działania gwarantujące im szeroko rozumiane bezpieczeństwo, gdyż zapewnienie bezpieczeństwa aktywom zapewnia bezpieczeństwo procesu przetwarzania danych osobowych. Typowe zasoby i aktywa występujące w jednostce w podziale na aktywa wymierne i niewymierne przedstawia tabela 1.

Tabela 1

Zasoby i aktywa wymierne	Zasoby i aktywa niewymierne
Urządzenia systemu komputerowego	Stosunki interpersonalne
Dokumenty w wersji papierowej i elektronicznej zawierające informacje/dane	Zaufanie klientów
Zasilanie	Wizerunek Urzędu
Oprogramowanie aplikacyjne i systemowe	Zaufanie do usług
Zewnętrzne, udostępnione zasoby informatyczne	
Pozostałe oprogramowanie aplikacyjne	
Systemy operacyjne	
Sieć internetowa	

Etap 2 Określenie zagrożeń dla zidentyfikowanych zasobów i ich źródeł

Kolejnym etapem jest identyfikacja zagrożeń, czyli umyślnego lub przypadkowego wykorzystania podatności. Te same zagrożenia mogą mieć różne źródła co ma istotne znaczenie dla prawdopodobieństwa ich zaistnienia. Tworząc katalog potencjalnych zagrożeń posłużono się PN-ISO/IEC 27005, która listuje przykłady typowych zagrożeń i ich źródeł. Zagrożenia określone w przywołanej normie obrazuje tabela 2.

Tabela 2

Lp.	Kategoria, rodzaj zagrożenia	Przyczyna, źródło zagrożenia
1	**Zniszczenie fizyczne nośników danych osobowych (papierowych, elektronicznych)**	Pożar
2		Zalanie
3		Zniszczenie danych
4		Zniszczenie urządzeń lub nośników danych
5		Utrata na skutek zjawisk starzenia się nośników danych (kurz, butwienie itp.)

6	**Zjawiska naturalne lub mające charakter katastroficzny**	Zjawiska pogodowe
7		Powódź
8		Inne zjawiska o charakterze katastroficznym (zawalenie budynku, zapadnięcie ziemi itp.)
9	**Utrata podstawowych usług**	Awaria systemu klimatyzacji
10		Utrata dostaw energii elektrycznej
11		Brak dostaw usług telekomunikacyjnych
12	**Zakłócenia spowodowane promieniowaniem**	Promieniowanie elektromagnetyczne
13		Promieniowanie cieplne
14		Promieniowanie słoneczne
15	**Naruszenie bezpieczeństwa informacji**	Przechwycenie sygnałów wskutek wykorzystania zjawiska interferencji
16		Ujawnione próby pozyskania danych osobowych z wykorzystaniem technik kwalifikowanych, jako szpiegowanie (np. w sieci lub fizyczne na ternie jednostki)
17		Podsłuch
18		Kradzież nośników danych lub dokumentów
19		Składanie wniosków na zasadzie dostępu do informacji publicznej do dokumentów zawierających dane osobowe
20		Kradzież urządzeń służących przetwarzaniu danych (jednostek komputerowych
21		Odtwarzanie danych z nośników przeznaczonych do zniszczenia
22		Używanie nośników nie będących własnością jednostki
23		Niezamierzone ujawnienie danych

24		Powzięcie danych z nieznanych lub niewiarygodnych źródeł
25		Stwierdzenie manipulowania urządzeniami będącymi nośnikami lub przetwarzającymi dane
26		Posługiwanie się nielicencjonowanym,, sfałszowanym oprogramowaniem
27		Próby pozyskiwania informacji przez osoby trzecie o miejscu przechowywania danych
28	**Awarie techniczne**	Awaria urządzenia służącego przetwarzaniu danych (jednostki komputerowe, drukarki, skanery, itp.)
29		Niewłaściwe funkcjonowanie urządzeń służących przetwarzaniu danych (komputery, drukarki, skanery itp.)
3		Przeciążenie systemów informatycznych skutkujące ich zawieszeniem pracy
31		Niewłaściwe funkcjonowanie systemów informatycznych
32		Naruszenie zdolności utrzymania systemu informatycznego (brak przedłużenia licencji, brak dostępu do aktualizacji, brak dostępu do wsparcia serwisowego itp.)
33	**Nieuprawnione działania**	Użycie urządzeń przez nieuprawnionego użytkownika (pracownik nie posiadający uprawnień lub osoba z zewnątrz jednostki)
34		Korzystanie z usług przypadkowych serwisantów
35		Nieuprawnione, nieuzasadnione kopiowanie danych
36		Zniekształcanie, modyfikowanie danych przez osobę nieposiadającą uprawnień
37		Przetwarzanie danych przez osobę nieposiadającą uprawnień

38	**Naruszenie bezpieczeństwa**	Błąd użytkownika – działanie lub próba podjęcia działań niezgodnych z przyjętymi zasadami bezpieczeństwa.
39		Fałszowanie uprawnień, przetwarzanie danych z wykorzystaniem hasła dostępu, loginu innej osoby
40		Brak dostępności personelu posiadającego uprawnienia
41		Brak odebrania uprawnień pracownikom, którzy na skutek odejścia, zmiany wydziału przestali przetwarzać dane.

Etap 3 Określenie prawdopodobieństwa wystąpienia zagrożeń (jego źródeł) wpływających na bezpieczeństwo informacji.

Na tym etapie należy określić w skali od 1 do 3 prawdopodobieństwo wystąpienia określonego zdarzenia w kontekście jego źródeł zakładając, że wartość:

1- oznacza, że zdarzenie na przestrzeni funkcjonowania Urzędu nie wystąpiło, lecz ze względu na swoją powszechność występowania w otoczeniu stwarza przesłanki do jego uwzględnienia - małe prawdopodobieństwo wystąpienia zdarzenia;

2 – oznacza, że zdarzenie nie wystąpiło w okresie 12 miesięcy poprzedzających dzień sporządzenia analizy, lecz miało miejsce w historii funkcjonowania Urzędu – średnie prawdopodobieństwo wystąpienia zdarzenia;

3 - oznacza, że zdarzenie na przestrzeni 12 miesięcy poprzedzających dzień sporządzenia analizy wystąpiło w Urzędzie – duże prawdopodobieństwo wystąpienia zdarzenia.

Etap 4 Określenie wpływu źródeł zdarzenia na czynniki decydujące o bezpieczeństwie informacji

Zgodnie z RODO bezpieczeństwo danych osobowych oparte jest na następujących podstawowych atrybutach: poufność, integralność, dostępność. Wpływ określonego potencjalnego źródła, przyczyny zdarzenia na bezpieczeństwo przetwarzania danych osobowych należy określić na podstawie stopnia jego oddziaływania na poszczególne wymienione atrybuty. Zdarzenie może mieć bardzo negatywny skutek dla jednego z nich, a dla innego nie mieć żadnego, np. pożar. Spalenie teczek osobowych ma katastroficzne znaczenie dla dostępności danych w nich zawartych, lecz jest bez znaczenia dla zachowania ich poufności, wręcz uniemożliwiło jej naruszenie w przyszłości w odniesieniu do konkretnego zasobu, który uległ spopieleniu. Przy określeniu stopnia wpływu przyczyny zdarzenia na bezpieczeństwo danych osobowych należy wziąć pod uwagę „liczebność" lokalizacji zasobów będących jej nośnikiem. Nie bez znaczenia dla bezpieczeństwa informacji w kontekście wszystkich wymienionych wcześniej czynników jest ilość lokalizacji jednostki (rozproszenie w terenie – różne lokalizacje w (terenie). Przy określaniu wpływu źródeł zdarzenia na atrybuty decydujące o bezpieczeństwie danych osobowych przyjęto 3 stopniową skalę, w której wartość:

- 1 oznacza że istnieje możliwość wpływu na atrybut, lecz stopień jego oddziaływania jest nieduży lub dotychczas przyjęte rozwiązania bez poniesienia większych nakładów przywrócą poziom bezpieczeństwa danych, jaki był przed zaistnieniem zdarzenia;

- 2 oznacza, że wystąpienie zagrożenia może mieć wpływ na określony atrybut i stanowić utrudnienie w bezpiecznym przetwarzaniu danych osobowych, a przywrócenie stanu pewności bezpiecznego przetwarzania danych nie wymaga poniesienia istotnych nakładów.

- 3 oznacza istnienie bezpośredniego wpływu na atrybut, którego skutki mają istotne – krytyczne znaczenie dla bezpieczeństwa danych osobowych i wiążą się z utratą możliwości realizowania zadań. Przywrócenie pierwotnego stanu wiąże się z poniesieniem wymiernych nakładów.

Etap 5 Ocena wdrożonych w jednostce poziomów zabezpieczeń

W Urzędzie funkcjonuje szereg zabezpieczeń przed skutkami niepożądanych zdarzeń. Kolejny etap polega na ocenie ich skuteczności zabezpieczenia atrybutów decydujących o bezpieczeństwie przetwarzania danych osobowych przed negatywnym wpływem zidentyfikowanych źródeł zagrożeń. Stosując ocenę jakościową istniejących zabezpieczeń posługujemy się 3 stopniową skalą (od 1 do 3.), gdzie:

- 1 – oznacza brak zabezpieczeń lub ich niewielką skuteczność;

- 2 – występują częściowe zabezpieczenia, które chronią wybrane obszary, lecz nie są w pełni skuteczne;

- 3 – występujące zabezpieczenia chronią skutecznie przed zidentyfikowanymi zagrożeniami.

Etap 6 Szacowanie wartości pierwotnego ryzyka aktywu

Ryzyko pierwotne aktywu jest liczone wg wzoru:

$Rpa = Pwz \times \sum (Wz \times L \times W_L)$, gdzie:

Rpa – ryzyko pierwotne aktywu;
Pwz – prawdopodobieństwo wystąpienia źródła zagrożenia;
$\sum (Wz \times L \times W_L)$ – suma iloczynów dla każdego atrybutu tj. poufności, integralności, dostępności, gdzie:
Wz – wpływ zagrożenia na atrybut;
L – liczebność zasobów;
W_L – wpływ liczebności zasobów

Etap 7 Szacowanie ryzyka szczątkowego po ocenie zabezpieczeń przed zidentyfikowanym zagrożeniem

Ryzyko szczątkowe po wprowadzeniu zabezpieczeń jest liczone wg wzoru:

$Rsz = Pwz \times \sum [(Wz/Pz) \times L \times W_L]$, gdzie:

Rsz – ryzyko szczątkowe po zadziałaniu istniejących zabezpieczeń,

Pz – poziom zabezpieczeń przed wpływem zagrożenia na określony atrybut bezpieczeństwa danych osobowych;
Pozostałe oznaczenia tak, jak w etapie 6.

Etap 8 Określenie poziomu ryzyka dopuszczalnego – akceptowalnego.

Wprowadzanie zabezpieczeń przed zagrożeniami ma pewne granice wynikające z następujących zasad:
- nie istnieją zabezpieczenia idealne gwarantujące 100% bezpieczeństwa;
- zabezpieczenia muszą być adekwatne do zagrożeń;
- zabezpieczenia wprowadza się do momentu, gdy koszt ich funkcjonowania nie przekracza wartości poniesionych strat wynikających ze zmaterializowania się zagrożenia.

Wyznaczenie wartościowe progu akceptowalnego ryzyka polega na wyliczeniu **Rsz** wstawiając maksymalne wartości: prawdopodobieństwa wystąpienia zagrożenia, jego wpływu na czynniki bezpieczeństwa oraz poziomy wdrożonych zabezpieczeń.

Etap 9 Określenie sposobu postępowania w stosunku do sytuacji, w której ryzyko szczątkowe przekracza poziom ryzyka akceptowalnego

Końcowym etapem jest opracowanie planów mających na celu obniżenie ryzyk szczątkowych w odniesieniu do poszczególnych zagrożeń do poziomu ryzyka akceptowalnego. Powyższe działanie dotyczy sytuacji, w której mimo istniejących zabezpieczeń ryzyko szczątkowe przekracza wartością poziom ryzyka akceptowalnego. W pozostałych sytuacjach brak konieczności podejmowania dodatkowych działań.

WZÓR UMOWY POWIERZENIA DANYCH OSOBOWYCH DO DALSZEGO PRZETWARZANIA

zawarta w ..... w ..... pomiędzy:

.....

.....

zwanym dalej Administratorem danych osobowych (Administratorem lub Powierzającym)

a

.....

.....

zwanym dalej Przetwarzającym, zwanymi każdą z osobna w dalszej części Umowy „Stroną", a łącznie „Stronami".

Umowa powierzenia danych osobowych do dalszego przetwarzania jest efektem zawarcia umowy głównej o współprace między stronami z dnia .....w przedmiocie świadczenia przez Przetwarzającego usługi

.....

na rzecz Administratora. Przetwarzający w ramach usługi będącej przedmiotem umowy głównej będzie miał dostęp do danych osobowych w zakresie określonym niniejszą umową. Celem umowy jest określenie warunków, na jakich Przetwarzający będzie wykonywał operacje przetwarzania powierzonych przez Administratora danych osobowych. Strony umowy dążą do takiego uregulowania zasad przetwarzania, aby odpowiadały one w pełni postanowieniom **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 (ogólne rozporządzenie o ochronie danych)** (Dz.U.UE L z dnia 4 maja 2016 r.)

§ 1. Opis przetwarzania

1. Przedmiot. [art. 28 ust. 3 RODO] Na warunkach określonych niniejszą umową i umową główną, Administrator powierza Przetwarzającemu przetwarzanie dalej opisanych danych osobowych (dalej: dane)
2. Czas [art. 28 ust. 3 RODO] Przetwarzanie będzie wykonywane w okresie obowiązywania umowy głównej.
3. Charakter i cel [art. 28 ust. 3 RODO] Charakter i cel przetwarzania wynikają z umowy głównej.
4. Rodzaj danych[art. 28 ust. 3 RODO] Przetwarzanie obejmować będzie następujące rodzaje i kategorie danych osobowych:
   - Dane zwykłe:
     (Przykłady kategorii danych klasyfikowanych, jako zwykłe: imię i nazwisko, nr ewidencyjny PESEL, adres zamieszkania, adres IP, adres e-mail, nr telefonu, data urodzenia, numer NIP, seria i numer dokumentu tożsamości, imiona rodziców, nr rachunku bankowego, płeć.)
   - Dane szczególne i dane karne:
     (Przykłady kategorii danych klasyfikowanych, jako szczególne: wizerunek, stan zdrowia, dokumentacja medyczna, pochodzenie społeczne, wyznanie, poglądy

polityczne, przynależność partyjna, związkowa, sytuacja ekonomiczna, poziom rozwoju intelektualnego.)

- W tym dane dzieci/osób ubezwłasnowolnionych:
  (Należy wymienić te kategorie danych zwykłych i szczególnych, które odnoszą się do dzieci lub osób ubezwłasnowolnionych. W przypadku, gdy dane te nie są przedmiotem powierzenia należy wpisać „brak")

5. Kategorie osób, których dane będą przetwarzane [art. 28 ust. 3 RODO]
   (Przykłady kategorii osób, których dane są przedmiotem powierzenia: pracownicy Administratora, klienci korzystający z usług Administratora, uczniowie, podopieczni)

§ 2. Podpowierzenie

1. Podpowierzenie [art. 28 ust. 2 RODO] Przetwarzający może powierzyć konkretne operacje przetwarzania danych innemu podmiotowi.
2. Podpowierzenie wymaga uzyskania pisemnej zgody Administratora.
3. Umowa podpowierzenia wymaga formy pisemnej.
4. Transfer obowiązków [art. 28 ust. 4 RODO] Dokonując dalszego powierzenia danych, Przetwarzajacy ma obowiązek zobowiązać podmiot, któremu powierza dane do realizacji wszystkich obowiązków wynikających z niniejszej umowy w odniesieniu do obowiązujących przepisów RODO) regulujących proces przetwarzania danych.
5. Zobowiązanie względem Administratora. Przetwarzający ma obowiązek zapewnić, aby podmiot, któremu powierzył dane złożył Administratorowi pisemne zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie (4). Wymóg ten może zostać spełniony jedynie w drodze pisemnego oświadczenia skierowanego na adres Administratora.

§ 3. Obowiązki Przetwarzającego.

1. Udokumentowane polecenia [art. 28 ust. 3 RODO]. Przetwarzający przetwarza dane w związku z dyspozycjami zawartymi w umowie głównej lub na podstawie pisemnych poleceń lub instrukcji Administratora.
2. Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit.a RODO]. Przetwarzający oświadcza, że nie przekazuje danych poza EOG.
3. Tajemnica [art. 28 ust. 3 lit.b RODO] Przetwarzający ma obowiązek uzyskania od osób, które pisemnie upoważni do przetwarzania, pisemnego zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.
4. Bezpieczeństwo [art. 28 ust. 3 lit.c RODO] Przetwarzający zobowiązany jest do zapewnienia ochronę danych, o których mowa w art. 32 RODO zgodnie z dalszymi postanowieniami umowy.
5. Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit.e RODO] Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania praw określonych w Rozdziale III RODO (tzw. „prawa jednostki"). Przetwarzający oświadcza, że zapewnia obsługę praw jednostki w odniesieniu do powierzonych danych.
6. Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit.f RODO]. Przetwarzający współpracuje z Administratorem przy wykonywaniu obowiązków z obszaru ochrony danych

osobowych, o których mowa w art. 32-36 RODO (ochrona, zgłaszanie naruszeń, ocena skutków dla ochrony danych, uprzednie konsultacje z organem nadzorczym).

7. Legalność [art. 28 ust. 3 ak. 2 RODO]. Jeżeli Przetwarzający poweźmie wątpliwości, co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
8. Projektowanie prywatności [art. 24 ust. 1 RODO]. Planując jakiekolwiek zmiany w przetwarzaniu, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności i ma z wyprzedzeniem powiadamiać Administratora o planowanych zmianach w sposób zapewniający Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany zdaniem Administratora zagrażają poziomowi bezpieczeństwa określonego umową lub niosą za sobą zwiększone ryzyko naruszenia praw i wolności osób wskutek przetwarzania ich danych przez Przetwarzającego.
9. Minimalizacja [art. 25 ust. 2 RODO]. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych wyłącznie do osób, których dostęp do danych jest niezbędny dla realizacji umowy głównej i posiadających odpowiednie upoważnienie
10. RCPD [art. 30 ust. 2 RODO]. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru kategorii czynności przetwarzania danych (wymóg art. 30 RODO). Przetwarzający udostępnia na żądanie Administratora prowadzony rejestr kategorii czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych Jego klientów.
11. Profilowanie [art. 13 i 14 RODO]. Jeżeli Przetwarzający wykorzystuje w celu realizacji umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, informuje o tym fakcie Administratora w celu i zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

12. Szkolenie personelu. Przetwarzający zobowiązuje się do zapewnienia odpowiedniego szkolenia z zakresu danych osobowych osobom upoważnionym do przetwarzania danych osobowych będących przedmiotem niniejszej umowy.

§ 4. Obowiązki Administratora

1. Administrator jest zobowiązany do współdziałania z Przetwarzającym w wykonaniu umowy, udzielać przetwarzającemu wyjaśnień w razie wątpliwości, co do legalności poleceń Administratora.

§ 5. Bezpieczeństwo danych

1. Bezpieczeństwo danych [art. 32 RODO]. Przetwarzający jest zobowiązany do przeprowadzenia analizy ryzyka przetwarzania powierzonych danych i udostępnić jej wyniki Administratorowi, co do organizacyjnych i technicznych środków ochrony danych na każde jego żądanie.
2. Przetwarzający zapewnia i zobowiązuje się, że:
   - dokonał oceny przydatności pseudonimizacji i szyfrowania i stosuje te techniki w zakresie, w jakim są potrzebne dla realizacji niniejszej umowy

- posiada zdolność do ciągłego zapewnienia poufności, dostępności i integralności powierzonych danych,
- posiada zdolność do szybkiego przywrócenia dostępności danych w razie jakiegokolwiek incydentu fizycznego lub technicznego,
- regularnie testuje, mierzy i ocenia skuteczność stosowanych organizacyjnych i technicznych środków bezpieczeństwa.

3. Powiadomienie o naruszeniu [art. 33 RODO]. Przetwarzający powiadamia Administratora o każdym stwierdzonym naruszeniu ochrony danych osobowych nie później niż w ciągu 24 h od momentu stwierdzenia naruszenia. W przypadku wystąpienia naruszenia Przetwarzający umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i umożliwia jemu udział w ich prowadzeniu.
4. Przetwarzający przesyła powiadomienie Administratorowi o naruszeniu w terminie wskazanym powyżej (pkt 3) wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku wynikającego z art. 33 RODO.

§ 6. Nadzór

1. Sprawowanie kontroli[art. 28 ust. 3 RODO] Administrator ma pełne prawa do kontroli u Przetwarzającego procesu przetwarzania danych będących przedmiotem powierzenia. Powiadomienie o takiej kontroli Administrator wysyła Przetwarzającemu z minimalnym wyprzedzeniem wynoszącym 72h przed rozpoczęciem planowanych czynności.
2. Przetwarzający w związku z prawem kontroli ze strony Administratora zobowiązuje się do udostępnienia wszelkich informacji niezbędnych do wykazania, że przetwarzający przetwarza dane zgodnie z przepisami RODO.
3. Przetwarzający umożliwi Administratorowi swobodny i nieograniczony dostęp do osób dokonujących u Niego przetwarzania oraz do pomieszczeń, w których dokonuje się przetwarzania powierzonych danych.

§ 7. Oświadczenia stron

1. Oświadczenie Administratora. Administrator oświadcza, że jest Administratorem danych i jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Oświadczenie przetwarzającego [art.28 ust. 1 RODO]. Przetwarzający oświadcza oświadcza, iż posiada niezbędną wiedzę i odpowiednie środki techniczne oraz organizacyjne dające rękojmie przetwarzania powierzonych danych w sposób zgodny z obowiązującymi przepisami.

§ 8. Odpowiedzialność

1. Odpowiedzialność Przetwarzającego [art. 82 ust.3 RODO] Przetwarzający odpowiada w wymiarze finansowym za wszystkie szkody będące skutkiem niezgodnego przetwarzania danych z przepisami prawa obowiązującymi w tej materii lub zapisami niniejszej umowy.

§ 9. Okres obowiązywania umowy

1. Okres obowiązywania umowy [art. 28 ust. 3 RODO]. Umowa zostaje zawarta na czas realizacji umowy głównej z zastrzeżeniem terminu karencji usunięcia powierzonych danych w terminie wskazanym w pkt. kolejnym.
2. Usunięcie danych [art. 28 ust. 3 lit.g RODO]. W chwili rozwiązania, wygaśnięcia umowy niniejszej umowy, Przetwarzający nie ma prawado dalszego przetwarzania danych osobowych i jest zobligowany do:
   - usunięcia danych i pisemnego poinformowania Administratora o tym fakcie przetwarzania, wskazując w szczególności sposób usunięcia danych i datę tej czynności,
   - usunięcia wszelkich kopii danych lub ich zwrotu Administratorowi.
3. Administrator daje przetwarzającemu 90 dni do wykonania czynności wskazanych w pkt. 2, chyba, że poleci jemu uczynić to wcześniej.

§ 10. Postanowienia końcowe.

1. Pierwszeństwo. W razie konfliktu między postanowieniami umowy głównej, a postanowieniami niniejszej umowy w aspekcie przetwarzania danych osobowych, pierwszeństwo mają postanowienia niniejszej umowy.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.
3. W kwestiach nieujętych niniejszą umową zastosowanie mają przepisy RODO i Kodeksu Cywilnego.
4. Wszelkie kwestie sporne strony umowy zobowiązują się rozstrzygać w pierwszej kolejności w oparciu o wzajemne kontakty i wspólnie wypracowane rozwiązania.
5. Wszelkie zmiany postanowień niniejszej umowy wymagają pisemnego aneksu.

Wykaz budynków, pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania

L.p.	**Pomieszczenie** (określenie nr pokoju lub jego nazwy wraz ze wskazaniem piętra)	**Lokalizacja** (wskazanie adresu budynku)	**Dane osobowe** (wskazanie rodzaju czynności przetwarzania danych osobowych lub ich nr za jakimi są ujęte w RCPD)
1			
2			
3			
4			
5			
6			
7			
8			

Rejestr zdarzeń niezamierzonego nieuprawnionego przetwarzania danych osobowych

Lp.	Opis niezamierzonego nieuprawnionego przetwarzania danych osobowych	Kategorie przetworzonych danych	Data wystąpienia zdarzenia	Opis podjętych działań

Oświadczenie dla osób zatrudnionych na nieurzędniczych stanowiskach pracy

Ja niżej podpisana / podpisany* ..... Oświadczam, że znane są mi przepisy i regulacje obowiązujące w jednostce, związane z zasadami przetwarzania i ochrony danych osobowych opisane w Polityce ochrony danych osobowych i wdrożone do stosowania.

Jednocześnie oświadczam, że zobowiązuję się przestrzegać zasad i przepisów z zakresu ochrony danych osobowych wskazanych ww. Polityce ochrony danych osobowych podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

- ✓ dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych;
- ✓ nie podejmowania żadnych działań polegających na przetwarzania danych osobowych w sytuacji braku pisemnego upoważnienia do tego rodzaju czynności;
- ✓ zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, nieuprawnioną zmianą lub zniszczeniem, utratą, uszkodzeniem, kiedy w trakcie realizacji zadań służbowych stwierdzę możliwość wystąpienia takiej sytuacji.
- ✓ niezwłocznego powiadomienia przełożonego w przypadku dokonania niezamierzonego nieuprawnionego przetwarzania danych osobowych w związku z powierzonymi zadaniami do realizacji;
- ✓ zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia w trakcie zatrudnienia, jak również po jego ustaniu.

.....
(data i podpis osoby składającej oświadczenie)

* niepotrzebne skreślić

Łobez, dnia .....

.....

(imię i nazwisko, stanowisko wnioskodawcy)

Zgoda na użytkowanie urządzeń służbowych poza siedzibą jednostki

W związku z .....
(należy wskazać powód np. realizacja obowiązków służbowych poza siedzibą jednostki)

wnioskuję o wyrażenie zgody na użytkowanie nw. sprzętu informatycznego poza siedzibą Urzędu.

Wykorzystywany sprzęt .....

.....
(należy określić rodzaj sprzętu wskazując jego nr fabryczny oraz nr inwentarzowy)

będzie użytkowany poza siedzibą jednostki w okresie zatrudnienia / terminie * od dnia .....

do dnia .....

.....
(data i podpis wnioskodawcy)

Opinia administratora systemu informatycznego

Ww. sprzęt technicznie jest przygotowany do bezpiecznego użytkowania poza siedzibą Urzędu / brak technicznych możliwości bezpiecznego użytkowania sprzętu poza siedzibą Urzędu*. Jednocześnie pozytywnie / negatywnie* odnoszę się do złożonego wniosku.

.....
(data i podpis administratora systemu informatycznego)

Decyzja administratora danych osobowych

Wyrażam / nie wyrażam* zgody na użytkowanie wskazanego sprzętu informatycznego poza siedzibą Urzędu przez w okresie wskazanym we wniosku.

.....
(data i podpis administratora danych osobowych)

* niepotrzebne skreślić

Pouczenie:

Zgodnie z art. 124 Kodeksu Pracy pracownik, któremu powierzono instrumenty lub podobne przedmioty z obowiązkiem zwrotu, odpowiada w pełnej wysokości za szkodę powstałą w tym mieniu.

Oświadczenie:

Ja, niżej podpisana/podpisany*.....
zatrudniona/zatrudniony w Urzędzie Miejskim w Łobzie na stanowisku
.....
oświadczam, że przyjmuję pełną odpowiedzialność materialną za powierzone mi mienie Urzędu Miejskiego w Łobzie z obowiązkiem zwrotu albo do wyliczenia się.

Nie wnoszę zastrzeżeń co do warunków zabezpieczenia przez pracodawcę powierzonego mi mienia.

.....
(data, imię i nazwisko pobierającego sprzęt)

* niepotrzebne skreślić