Zarządzenie Nr SK.0050.112.2019
Wójta Gminy Świerzno
z dnia 23 września 2019 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych, Instrukcji zarządzania systemem informatycznym i Księgi procedur w Urzędzie Gminy w Świerznie

Na podstawie art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE L. 206. 119. 1) zarządza się, co następuje:

§ 1. Wprowadza się prowadzoną Politykę ochrony danych osobowych (zał. nr 1), Instrukcję Zarządzania Systemem Informatycznym (zał. nr 2) i Księgę procedur (zał. nr 3) w Urzędzie Gminy w Świerznie stanowiące integralną część niniejszego zarządzenia.

§ 2. Polityka ochrony danych osobowych, Instrukcja zarządzania systemem informatycznym i Księga procedur mają zastosowanie w Urzędzie Gminy w Świerznie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe.

§ 3. Z treścią Polityki ochrony danych osobowych, Instrukcją zarządzania systemem informatycznym i Księgą procedur zobowiązani są zapoznać się wszyscy pracownicy Urzędu Gminy w Świerznie przetwarzający dane osobowe.

§ 4. Zobowiązuje się wszystkich pracowników Urzędu Gminy w Świerznie do przestrzegania zasad wynikających z Polityki ochrony danych osobowych, Instrukcji zarządzania systemem informatycznym oraz z Księgi Procedur.

§ 5. Administrator Systemu Informatycznego Urzędu Gminy w Świerznie odpowiada za ochronę danych w systemach informatycznych oraz za aktualizację, realizację i przestrzeganie przepisów zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 6. Przypadki naruszeń zasad zawartych w niniejszym zarządzaniu lub zaistnienie pojedynczego rażącego naruszenia zasad bezpieczeństwa w stosunku do ochrony danych osobowych i systemów informatycznych w Urzędzie Gminy w Świerznie zgłaszane są Administratorowi danych i stanowią podstawę wszczęcia postępowania dyscyplinarnego w stosunku do osób winnych naruszeń.

§ 7. Wdrożenie i nadzór nad realizacją zarządzenia powierzam Inspektorowi Ochrony Danych Osobowych (IODO).

§ 8. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Radosław Drozdowicz

Uzasadnienie

Wdrożenie prowadzonej dokumentacji o ochronie danych osobowych i zapewnianie przestrzegania jej zapisów wynika z konieczności stosowania 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), zwanego dalej „Rozporządzeniem".

Rozporządzenie obowiązuje w polskim porządku prawnym bezpośrednio i ma zastosowanie od dnia 25 maja 2018 r., i od tego dnia polskie przepisy muszą zapewniać skuteczne stosowanie przepisów Rozporządzenia, nie powielając jego rozwiązań ani nie będąc z nim sprzecznymi. Przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), przestały z dniem 25 maja 2018 r. obowiązywać. W świetle powyższego konieczne stało się opracowanie i wdrożenie nowej dokumentacji w zakresie ochrony danych osobowych, która odpowiada przepisom i standardom ochrony danych osobowych zawartym w Rozporządzeniu. Zgodnie z Rozporządzeniem od 25 maja 2018 r. osoba pełniąca funkcję Administratora Bezpieczeństwa Informacji stała się Inspektorem Ochrony Danych.

Załącznik nr 1 do zarządzenia Wójta Gminy Świerzno Nr SK.0050.112.2019

Polityka ochrony danych osobowych – dokument główny

ZATWIERDZAM

WÓJT
Radosław Drozdowicz

.....

podpis Wójta

Świerzno 2018 roku

METRYKA

Nazwa jednostki	Urząd Gminy w Świerznie		
Tytuł dokumentu	Polityka ochrony danych osobowych		
Opis	W skład dokumentu wchodzą: Polityka ochrony danych osobowych wraz z załącznikami		
Zastosowanie	Urząd Gminy w Świerznie		
Plik	Polityka ochrony danych osobowych		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia 21. 11. 2018 r.	Liczba stron	24

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	15.08.2018	utworzenie	wszystkie	Krzysztof Rychel	
2.00	19.09.2019	modyfikacja	załącznik nr 1 E	Martyna Danś	

* 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 Gminy w Świerznie (dalej: Urząd, jednostka) jest zbiorem zasad i procedur, obowiązujących przy realizacji wszystkich czynności przetwarzania i wykorzystywania danych osobowych we wszystkich zbiorach danych, administrowanych przez Urząd Gminy. Celem wprowadzenia polityki jest ograniczenie ryzyka naruszenia praw i wolności osób fizycznych, w tym w szczególności mieszkańców gminy, klientów korzystających z usług Urzędu i jego pracowników, jakie może spowodować przetwarzanie ich danych w związku z realizowanymi zadaniami i obowiązkami. Ponadto polityka ma na celu wykazanie realizacji zasady rozliczalności, przez prowadzenie odpowiedniej dokumentacji, opisującej sposoby ochrony danych, na którą składa się niniejsza polityka wraz z załącznikami stanowiącymi jej integralną część. Niniejsze reguły 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 w ramach zbiorów, jak i spoza nich, które mogą być realizowane w sposób ciągły, jak i doraźny. W polityce przyznano wyższy priorytet realizowanym czynnością przetwarzania danych osobowych i ich identyfikacji w odniesieniu do obowiązku identyfikacji zbiorów danych osobowych. Polityka jest polityką ochrony danych osobowych w rozumieniu *rozporządzenia 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 Urzedzie 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 związanych z obszarem ochrony danych osobowych w Urzędzie Gminy Świezno i zawiera:

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

1.5 Integralną częścią dokumentacji niniejszej polityki są:

- ✓ Instrukcja zarządzania systemem informatycznym;
- ✓ Księga procedur

1.6 Odpowiedzialnym za wdrożenie i utrzymanie niniejszej polityki jest najwyższe kierownictwo Urzędu w osobie Wójta Gminy Świerzno.

2. Definicje

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

- ✓ **„administrator danych osobowych"** (dalej:**ADO**) – Urząd Gminy Świerzno reprezentowany przez Wójta;

- ✓ **„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 Gminy Świerzno;
- ✓ **„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 Urzędzie podlegający konkretnej osobie, sprawującej nadzór nad jej działaniami. W jednostce zgodnie z przyjętym schematem organizacyjnym **(załącznik nr 1)** przyjęto zasadę, że każdy pracownik podlega bezpośrednio jednemu przełożonemu.
- ✓ **„kierownik komórki organizacyjnej"** – rozumie się przez to osoby kierujące lub nadzorujące pracę innych osób lub osobę zajmującą samodzielne stanowisko. W Urzędzie przyjęto zasadę, iż bezpośredni nadzór nad pracami pracowników pełni Wójt, Sekretarz bądź Skarbnik;

- ✓ **"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"** 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 i dopuszczona, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym Urzędu przez ASI, jak i poza nim 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);
- ✓ **„rozliczalność danych"** - właściwość pozwalająca przypisać określone działanie związane z przetwarzaniem danych osobowych do osoby, procesu, miejsca oraz umiejscowić je w czasie;
- ✓ **„serwisancie"** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego oraz pozostałych elementów infrastruktury informatycznej;
- ✓ **"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 lub inna osoba w nim zatrudniona na podstawie umowy o pracę, umowy cywilnej, upoważniona do przetwarzania danych osobowych, w tym w sposób tradycyjny, z wykorzystaniem systemu informatycznego, programu komputerowego, aplikacji;
- ✓ **„Urząd" –** Urząd Gminy Świerzno;
- ✓ **„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 w jednostce przetwarza się dane osobowe na podstawie, co najmniej jednej z przesłanek przetwarzania danych osobowych wynikających z art. 6, 9, 10 RODO. Urząd realizuje zadania wynikające ze ustawy z dnia 8 marca o samorządzie gminnym z przyjętym podziałem zadań dla poszczególnych pracowników określonym w Regulaminie Organizacyjnym Urzędu Gminy w Świerznie przyjętym zarządzeniem nr SK.0050.100.2017 Wójta Gminy Świerzno. Przetwarzanie danych osobowych w jednostce odbywa się w głównej mierze w oparciu o przesłanki wskazane art. 6 ust. 1 lit. a, b, c, e. art. 9 oraz art. 10 RODO. Stosowanie ww. norm prawa oznacza stosowanie się do zasady legalizmu i zobowiązuje pracowników Urzędu do identyfikowanie podstawy prawnej w postaci konkretnej normy prawa w odniesieniu do realizowanych czynności przetwarzania danych osobowych, 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 przez Wójta Gminy Świerzno bądź wskazaną przez niego osobę.

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, którym powierzono prowadzenie sprawy lub jej prowadzenie wynika z przyjętego zakresu obowiązków. Za realizację przedmiotowego obowiązku informacyjnego odpowiada pracownik oraz jej bezpośredni przełożony. Sposób realizacji obowiązku informacyjnego określa **Procedura realizacji obowiązku informacyjnego (Księga procedur).**

3.6 Urząd Gminy w Świerznie, jako administrator przetwarza dane osobowe jedynie w celach związanych z realizacją zadań wskazanych w pkt 3.3 oraz zadań zleconych przez jednostki nadrzędne, wynikające z ustawy z dnia 8 marca 1990 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 (RCPD)***.

3.7 Urząd jako podmiot przetwarzający w sytuacji, gdy powierzono jemu dane przez innego administratora i na mocy przyjętego w formie 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*** jest prowadzony na zasadach określonych, jak dla ***Rejestru czynności przetwarzania danych osobowych*** w pkt. 3.4.

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 jednostce 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 jednostce przechowuje się wyłącznie przez okres niezbędności dysponowania dokumentacją dla realizowania zadań lub przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt. 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 i jej zbędność do celów służbowych. Realizacja zasady ograniczenia przechowywania następuje również przez wskazanie planowanych terminów usunięcia 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 danych, które wykonuje w drodze zawartych umów powierzenia danych 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 wskazanych przez Wójta pracowników Urzędu.

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:

- ✓ **obowiązki informacyjne** – Urząd przekazuje informacje właścicielom danych osobowych w formie, 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 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 (w postaci linków) o prawach osób i sposobie korzystania z nich.

4.4 Urząd przestrzega prawnych terminów dotyczących obowiązków informacyjnych względem osób oraz dokumentuje obsługę obowiązków informacyjnych, 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, Wójt 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 Wójt Gminy Świerzno.

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 częstotliwości 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;
- ✓ podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie;
- ✓ organizację administrowania danymi oraz określa właściwe techniki zabezpieczenia danych osobowych;
- ✓ upoważnienie poszczególnych pracowników do czynności przetwarzania danych osobowych w zakresie, odpowiadającym powierzonym czynnościom na danym stanowisku pracy (art. 29 RODO). ADO wydaje upoważnienie sporządzone wg wzoru **załącznik nr** 5 – ***Upoważnienie do przetwarzania danych osobowych.*** Przy wydawaniu upoważnień administrator danych osobowych kieruje się tzw. zasadą wiedzy koniecznej w stosunku do osoby upoważnianej;

- ✓ odwoływanie wydanych upoważnień na podstawie własnej decyzji. Wzór wniosku odwołującego upoważnienie do przetwarzania danych osobowych stanowi **załącznik nr 6 – *Odwołanie upoważnienia do przetwarzania danych osobowych***;
- ✓ przestrzeganie procedury nadawania i odbierania upoważnień określonej w ***Procedurze nadawania i odbierania uprawnień do przetwarzania danych osobowych*** **(Książka procedur)**;
- ✓ prowadzenie ewidencji wydanych i odwołanych upoważnień do przetwarzania danych osobowych ***(wg załącznika nr 7 – Rejestr wydanych i odwołanych upoważnień)*** oraz pozostałą dokumentację 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 jednostce 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);
- ✓ dokonanie oceny skutków przetwarzania danych osobowych dla praw lub wolności osób fizycznych (art. 35 RODO) lub zlecenie IOD przeprowadzenie tej oceny;
- ✓ sprawowanie nadzoru nad przestrzeganiem przyjętych zasad ochrony danych osobowych;
- ✓ sprawowanie bezpośredniego 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***, która stanowi **Załącznik nr 8** do niniejszej polityki, 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;
- ✓ określenie w drodze pisemnego upoważnienia, osób odpowiedzialnych za realizację poszczególnych obowiązków jemu przypisanych, jeżeli którekolwiek z nich powierzy innym pracownikom Urzędu, co jednak nie zwalnia go z odpowiedzialności za sposób ich realizacji;
- ✓ wybór podmiotów przetwarzających dane na rzecz jednostki, określając wymogi w stosunku do przetwarzających, co do warunków przetwarzania, które winny zostać 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 oraz zatwierdza wybór osoby, która będzie administrowała systemami informatycznymi użytkowanymi w jednostce. Niezależnie od sposobu powołania administratora systemu informatycznego (dalej: ASI), Wójt o fakcie tym powiadamia pracowników w drodze stosownego zarządzenia lub w innej formie przyjętej dla tego rodzaju komunikatów.

6.2 Funkcję związaną z administrowaniem systemem informatycznym może pełnić: pracownik jednostki, pracownik lub podmiot zewnętrzny na zasadzie świadczenia usługi. 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 systemem informatycznym, 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 oprogramowania i jego aktualizacją;
- ✓ jest jedyną osobą uprawnioną do instalowania i usuwania oprogramowania systemowego, narzędziowego i jego aktualizacji. 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 jednostce 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 jednostce;
- ✓ przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w tym w szczególności do zasobów, w których przetwarzane są dane osobowe;
- ✓ na wniosek Wójta, określa dla użytkownika dostęp do poszczególnych zasobów informatycznych funkcjonujących w jednostce, przydzielając każdemu użytkownikowi indywidualny login oraz dokonuje ewentualnych modyfikacji uprawnień;
- ✓ prowadzi rejestr przydzielonych poszczególnym pracownikom loginów w odniesieniu do użytkowanych systemów informatycznych oraz pozostałych rejestrów wymienionych 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 ADO;
- ✓ 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 jego skutków;
- ✓ 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 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 przypadku 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 jednostce;
- ✓ 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 jednostki po wcześniejszym ustaleniu tego z ADO;
- ✓ wnioskowania o złożenie pisemnych lub ustnych wyjaśnień przez pracowników jednostki 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 jednostki.

7. Inspektor Ochrony Danych

7.1 Wójt Gminy jako administrator i podmiot przetwarzający jest obowiązany do wyznaczenia inspektora ochrony danych na zasadach określonych w art. 37 RODO.

7.2 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.

7.3 Do zadań IOD należy:

- ✓ informowanie administratora oraz pracowników 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 kątem 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;
- ✓ doradztwo i pomoc w zakresie rozpatrywania wniosków kierowanych do ADO związanych z realizacją praw osób fizycznych, których dane osobowe są przetwarzane.

8. Osoba upoważniona do przetwarzania danych osobowych

8.1 Osoba upoważniona do przetwarzania danych osobowych **(użytkownik),** to każda osoba spełniająca kryteria definicji zawartej w Rozdziale **2. Definicje**.

8.2 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 *11. Pozostałe zasady bezpiecznego przetwarzania danych osobowych.***

8.3 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.

8.4 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.

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

8.6 W przypadku sytuacji niezamierzonego nieuprawnionego przetwarzania danych osobowych (np. na skutek otrzymania pisma z zewnątrz 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.

8.7 Dane osobowe będące przedmiotem niezamierzonego nieuprawnionego przetwarzania, winny bezzwłocznie zostać zanonimizowane (zatarte, zakorektorowane w sposób uniemożliwiający ich odczytanie). W przypadku, kiedy do pisma załączono dokumenty zawierające dane osobowe zbędne dla załatwienia sprawy, dokumenty takie należy niezwłocznie zwrócić nadawcy.

8.8 Wszyscy użytkownicy przetwarzający dane osobowe zobowiązani są do:

- ✓ zapoznania się przepisami Polityki ochrony danych osobowych wraz ze wszystkimi dokumentami wchodzącymi w jej skład (*Instrukcja zarządzania systemem informatycznym, Księga procedur*) 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 wyłącznie w celach służbowych.

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

9.1 Opisane środki techniczne i organizacyjne są stosowane w celu zapewnienia bezpieczeństwa danych osobowych, przetwarzanych w Urzędzie, a tym samym w celu ograniczenia ryzyka naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane.

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

9.3 Na zabezpieczenia o charakterze technicznym składają się:

- ✓ ochrona przed nieuprawnionym dostępem do obszarów przetwarzania realizowana poprzez:
  - ➢ stosowanie systemów alarmowych załączanych po godzinach pracy jednostki, monitorowanych przez zewnętrzną, licencjonowaną firmę z branży ochrony osób i mienia,
  - ➢ stosowanie zamków mechanicznych do pomieszczeń stanowiących miejsca przetwarzania danych osobowych,
  - ➢ 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,

- ✓ 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 w miarę możliwości wszystkich pomieszczeń znajdujących się w wykazie miejsc przetwarzania danych osobowych w mechaniczne niszczarki dokumentów,
  - ➢ okresowe działania o charakterze konserwacyjnym w odniesieniu do infrastruktury technicznej, związanej z przetwarzaniem danych osobowych;

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

- ✓ ochrona przed awariami realizowana jest:
  - ➢ wyposażenie urządzeń serwerowych (jeżeli posiada) 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,
- dbanie o prawidłową wentylację komputerów (kategoryczny zakaz ustawiania jednostek komputerowych w sposób zasłaniający kratki wentylatorów meblami, ścianą),
- niepodłączania do listew, podtrzymujących napięcie, przeznaczonych do zasilania sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejników, czajników, wentylatorów),
- wykonywanie kopii roboczych danych, na których się właśnie pracuje, z częstotliwością zapobiegającą ich utratę,
- 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,
- zamykanie 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 bezpośredniego przełożonego, 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.

9.4 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 zawartych w niniejszym dokumencie i ***Instrukcji zarządzania systemem informatycznym***
- 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, jak i nie urzędnicze) 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:

- niepozostawianie bez kontroli dokumentów i nośników danych, w strefach określanych mianem publicznych, do których zaliczamy ciągi komunikacyjne oraz miejsca w Urzędzie, do których klienci mają swobodny niczym nieograniczony i niekontrolowany dostęp,
- pilne strzeżenia akt i wymiennych nośników pamięci,
- nieużywanie powtórnie dokumentów zadrukowanych jednostronnie,
- niezapisywanie hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,
- powstrzymywanie 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,
- niewynoszenie poza siedzibę Urzędu, na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
- zachowanie tajemnicy danych, w tym także wobec najbliższych,
- przestrzeganie 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,
- kopiowanie tylko jednostkowych danych (pojedyńczych 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.

10. Infrastruktura przetwarzania danych osobowych

10.1 Infrastrukturę przetwarzania danych osobowych tworzą budynki i pomieszczenia, systemy informatycznie oraz pozostałe aktywa będące nośnikami danych wykorzystywane przez jednostkę.

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

10.3 ***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.

10.4 ***Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania*** jest prowadzony w sposób bieżący przez Wójta lub przez osobę przez niego wyznaczoną.

10.5 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.

10.6 W pomieszczeniach, o których mowa w pkt. 10.5 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.

10.7 Zabrania się przetwarzania danych osobowych w pomieszczeniach innych niż wymienione w wykazie, o którym mowa w pkt. 10.3.

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

11. Pozostałe zasady bezpiecznego przetwarzania danych osobowych

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

11.2 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 10**.

11.3 W sytuacji, o której mowa w pkt. 11.2 administrator systemu informatycznego jest zobowiązany do zaszyfrowania dysków zainstalowanych w jednostce komputerowej oraz prowadzi ewidencję sprzętu użytkowanego poza siedzibą jednostki przez uprawnionych pracowników.

11.4 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.

11.5 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 pojedyńczych 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.

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

12.1 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.

12.2 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.

13. Udostępnianie danych osobowych

13.1 Udostępnianie danych osobowych policji i sądom, może nastąpić w związku z prowadzonym przez te instytucje postępowaniem.

13.2 Udostępnianie informacji policji i sądom odbywa się według **Procedury udostępniania danych osobowych – Książka procedur**:

- ✓ udostępnianie danych osobowych funkcjonariuszom policji może nastąpić po przedłożeniu 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 funkcjonariusza upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

13.3 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.

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

13.5 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 jest możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

14. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

14.1 Niezastosowanie się do wprowadzonej 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.

15. Postanowienia końcowe

15.1 Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz do złożenia stosownego oświadczenia, potwierdzającego znajomość jego treści.
15.2 W odniesieniu do załączników mających formę rejestrów dopuszcza się możliwość ich prowadzenia w formie elektronicznej z wykorzystaniem narzędzi użytkowanego w jednostce oprogramowania biurowego.

Załączniki:

Załącznik nr 1 – Struktura organizacyjna jednostki;

Załącznik nr 2 – Rejestr czynnosci przetwarzania danych osobowych;

Załącznik nr 3 – Rejestr kategorii czynności przetwarzania;

Załącznik nr 4 – Klauzule informacyjne (z art. 13 oraz art. 14 RODO);

Załącznik nr 5 - Upoważnienia do przetwarzania danych osobowych;

Załącznik nr 6 – 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;

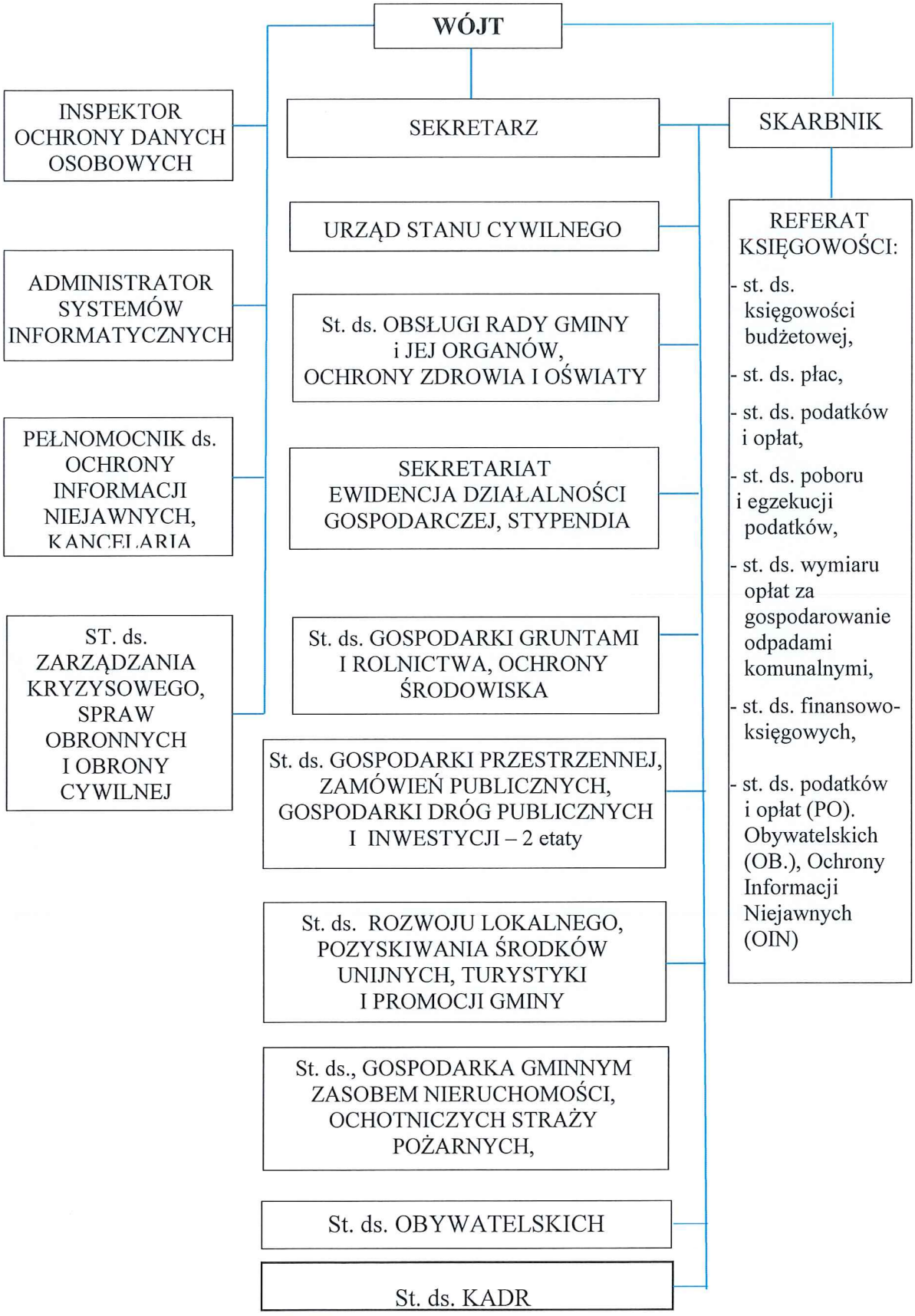
Załącznik nr 10 – Wykaz budynków, pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania;

Załącznik nr 11 - Rejestr zdarzeń nieuprawnionego przetwarzania danych osobowych;

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

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

SCHEMAT ORGANIZACYJNY URZĘDU



Nazwa (określenie) czynności przetwarzania danych osobowych ……	Numer kolejny ……
Rejestr czynności przetwarzania danych osobowych, dla których administratorem jest Urząd Gminy w Świerznie	
Współadministratorzy danych – nazwa, adres siedziby, dane kontaktowe (jeżeli wystepują)	
Dane kontaktowe Inspektora Ochony Danych	Kontakt listowy z administratorem na adres siedziby Urzędu lub e-mail: iodo_swierzno@wp.pl
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	
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	
Planowany termin przetwarzania danych osobowych	
Opis technicznych i organizacyjnych środków bezpieczeństwa	Zgodnie z opisem przyjętym w polityce ochrony danych osobowych

Nazwa (określenie) kategorii przetwarzania danych ……	Nr ……
Rejestr kategorii czynności przetwarzania danych osobowych, dla których przetwarzającym jest: Urząd Gminy w Świerznie	
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* danych osobowych jest:

Urząd Gminy Świerzno z siedzibą: Świerzno 13, 72-405 Świerzno. Z administratorem danych można się skontaktować poprzez adres e-mail: ug@swierzno.pl lub telefonicznie pod numerem 91 383 27 93 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.

Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iodo_swierzno@wp.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 administratora 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 Panią/Pana* 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* danych osobowych jest:

Urząd Gminy Świerzno z siedzibą: Świerzno 13, 72-405 Świerzno. Z administratorem danych można się skontaktować poprzez adres e-mail: ug@swierzno.pl lub telefonicznie pod numerem 91 383 27 93 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.

Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iodo_swierzno@wp.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.

Otrzymane Pani/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 administratora 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.

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.

Przetwarzane kategorie danych:

.....

Źródło danych

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

*niepotrzebne skreślić

Upoważnienie nr ..... z dnia .....

Działając na podstawie pkt. 5.3 Polityki ochrony danych osobowych oraz art. 29 RODO upoważniam **Panią/Pana**[1] ..... do realizacji nw. czynności przetwarzania danych osobowych[2]:

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

w zakresie niezbędnym do wykonywania obowiązków służbowych/zleconych*.

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

Upoważnienie wygasa z dniem zakończenia zatrudnienia/upływu terminu na jaki zostało wydane/realizacji umowy* lub z dniem jego odwołania.

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

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* do niżej wymienionych zasobów informatycznych:

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

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

1. Imię i nazwisko osoby upoważnianej
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

* niepotrzebne skreślić

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*, jak też po jego ustaniu.

.....

(data i podpis upoważnionego)

1. Imię i nazwisko osoby upoważnianej
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

* niepotrzebne skreślić

Odwołanie upoważnienia do przetwarzania danych osobowych

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)

do nw. czynności przetwarzania danych osobowych zawartych w *Rejestrze czynności przetwarzania danych osobowych*:

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

.....
(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. .....
2. .....

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

* niepotrzebne skreślić

Rejestr wydanych i odwołanych upoważnień do przetwarzania danych osobowych

L.p.	Nr Upoważnienia	Nazwisko	Imię	Data nadania	Zakres upoważnienia. Określenie nr czynności zgodnie z rejestrem czynności przetwarzania	Data odebrania	Odebrany zakres upoważnienia (w części/w całości). Określenie nr czynności zgodnie z rejestrem czynności przetwarzania

Metodologia analizy ryzyka

Proces zarządzania ryzykiem jest integralną częścią działalności jednostki. Jednostka 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 jednostkę 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 jednostki
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 jednostki 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 jednostki – średnie prawdopodobieństwo wystąpienia zdarzenia;

3 - oznacza, że zdarzenie na przestrzeni 12 miesięcy poprzedzających dzień sporządzenia analizy wystąpiło w jednostce – 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 jednostce 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:
     - 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:
- wizerunek,
- stan zdrowia,
- dokumentacja medyczna,
- pochodzenie społeczne,
- wyznanie,
- poglądy polityczne, przynależność partyjna, związkowa
- sytuacja ekonomiczna,
- poziom rozwoju intelektualnego,
- informacje o wyrokach i odbytych karach
- .....

➢ W tym dane dzieci/osób ubezwłasnowolnionych:
- imię i nazwisko,
- data urodzenia,
- adres zamieszkania,
- adres szkoły,
- nr legitymacji szkolnej,
- imiona i nazwiska rodziców/opiekunów prawnych,
- dane kontaktowe rodziców//opiekunów prawnych,

5. Kategorie osób, których dane będą przetwarzane [art. 28 ust. 3 RODO]
   - ➢ Pracownicy Administratora,
   - ➢ Klienci korzystający z usług Administratora,
   - ➢ Uczniowie,
   - ➢ Podopieczni,
   - ➢ Osoby, z którymi klient wchodzi w relacje wynikające z przedmiotu i charakteru prowadzonej działalności.

§ 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. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru kategorii 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 [art. 30 ust. 2 RODO].
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 wraz ze wskazaniem piętra)	**Lokalizacja** (wskazanie adresu budynku)	**Dane osobowe** (określenie rodzaju czynności przetwarzania danych osobowych lub ich nr z rejestru – załącznik nr 2)
1			
2			
3			
4			
5			
6			
7			
8			

Rejestr zdarzeń niezamierzonego nieuprawnionego przetwarzania danych osobowych

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

Oświadczenie dla osób zatrudnionych na nie urzędniczych 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

Świerzno, 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 Gminy w Świerznie.

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 jednostki / brak technicznych możliwości bezpiecznego użytkowania sprzętu poza siedzibą jednostki*. 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 jednostki 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 Gminy w Świerznie na stanowisku:

.....

oświadczam, że przyjmuję pełną odpowiedzialność materialną za powierzone mi mienie jednostki 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

Załącznik nr 2 do zarządzenia Wójta Gminy Świerzno Nr SK.0050.112.2019

Instrukcja zarządzania systemem informatycznym

ZATWIERDZAM

WÓJT

Radosław Drozdowicz

.....

podpis Wójta Gminy Świerzno

Świerzno 2018

METRYKA

Nazwa przedsiębiorstwa	Urząd Gminy Świerzno		
Tytuł dokumentu	Instrukcja zarządzania systemem informatycznym		
Opis	W skład dokumentu wchodzą: Instrukcja zarządzania systemem informatycznym wraz z załącznikami		
Zastosowanie	Wszystkie komórki organizacyjne		
Plik	Instrukcja zarządzania systemem informatycznym		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia 21.11. 2018 r.	Liczba stron	25

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	30.07.2018	utworzenie	wszystkie	Krzysztof Rychel	

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

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych w stosunku, do których jednostka pełni funkcję administratora, współadministratora bądź przetwarzającego lub jest odbiorcą danych. Celem opisanych poniżej działań, jest zabezpieczenie danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności odpowiadają wymogom *rozporządzenia 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)* i są zgodne z przyjętą w jednostce *Polityką ochrony danych osobowych*. Niniejszy dokument jest integralną częścią przyjętej Polityki ochrony danych osobowych w jednostce. Wszystkie użyte pojęcia, określenia osób, swoje zdefiniowanie znajdują w Rozdziale 2. Definicje Polityki ochrony danych osobowych.

Instrukcja zarządzania systemem informatycznym stanowi zbiór zasad postępowania w obszarze IT, związanym z przetwarzaniem danych osobowych, za wdrożenie i przestrzeganie, których odpowiada osoba sprawująca funkcję administratora systemu informatycznego (dalej: ASI), niezależnie od sposobu i formy jej zatrudnienia w jednostce.

2. Uprawnienia dostępu do systemów informatycznych, nadawanie i obieranie

2.1 Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, posiada wyłącznie ASI oraz osoba upoważniona do ich przetwarzania i zarejestrowana, jako użytkownik w systemie przez administratora systemu informatycznego.

2.2 Podstawą do nadania uprawnień przez administratora systemu informatycznego do przetwarzania danych osobowych w systemie informatycznym, jest upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych, na formularzu stanowiącym **załącznik nr 5** do *Polityki ochrony danych osobowych.* Przedmiotowy formularz winien określać systemy, do których udziela się użytkownikowi dostęp. Uprawnienia, o których mowa ASI może nadać po nadaniu upoważnienia użytkownikowi do czynności przetwarzania danych, przez administratora danych osobowych.

2.3 Osoby uprawnione do wnioskowania o nadanie uprawnień do systemów informatycznych, w tym do systemów, w których przetwarzane są dane osobowe określa *Polityka ochrony danych osobowych*.

2.4 ASI w związku z nadawaniem uprawnień dostępowych do systemu informatycznego zobowiązuje się do:

- ✓ określenia w formie pisemnej zasad tworzenia loginów do systemów informatycznych o ile twórca systemu lub administrator centralny systemu nie określił zasad ich tworzenia;
- ✓ w przypadku, gdy dana osoba na podstawie wydanego upoważnienia do przetwarzania danych osobowych, otrzymuje uprawnienia dostępowe do systemów informatycznych po raz pierwszy, informuje ją o zasadach bezpieczeństwa związanych z ich użytkowaniem;
- ✓ nadaje osobie upoważnionej, indywidualny login i hasło do pierwszego zalogowania się w systemie i instruuje osobę o konieczności zmiany hasła po zalogowaniu się do systemu, wskazując sposób wykonania tej czynności;
- ✓ powstrzymania się przed nadaniem uprawnień dostępowych w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie zatwierdzonego przez ADO;
- ✓ nadania użytkownikowi unikalnego loginu w systemie informatycznym i nie może być to login, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności loginu odbywa się na podstawie *Rejestru osób upoważnionych do systemów,* którego wzór stanowi **załącznik nr 1** do niniejszej instrukcji;
- ✓ prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych w postaci *Rejestru osób upoważnionych do systemów*;
- ✓ skonfigurowania systemu operacyjnego na jednostce komputerowej użytkownika w sposób zapewniający wymuszenie na nim zmiany hasła okresowo co 30 dni;
- ✓ hasła administracyjne (używane przez ASI) mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to powyżej, jednak nie dłużej niż 6 miesięcy oraz każdorazowo po rozwiązaniu umowy z administratorem systemu informatycznego;
- ✓ skonfigurowania systemu, by hasło dostępu do systemu informatycznego spełniało poniższe warunki:
  - długość co najmniej 12 znaków,
  - zawierało małe i duże litery,
  - zawierało cyfry lub znaki specjalne,
  - w trakcie wpisywania, nie było widoczne na ekranie monitora,
  - nie było jednakowe z loginem użytkownika,

- nie było poprzednio stosowane przez użytkownika – do 4 razy wstecz.

2.5 Login i hasło użytkownika, stanowią podstawowe środki uwierzytelniania dostępu do systemu informatycznego, który służy do przetwarzania danych osobowych.

2.6 W przypadku konieczności odebrania uprawnień, czynność ta jest realizowana również w oparciu o formularz, który stanowi **załącznik nr 6** do *Polityki ochrony danych osobowych.*

2.7 Wyrejestrowanie użytkownika z systemu może mieć charakter stały lub czasowy.

2.8 Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego w ramach, którego zatrudniony był użytkownik, zmiana indywidualnego zakresu czynności. Trwałe wyrejestrowanie użytkownika z systemu jest równoznaczne z wygaśnięciem lub odwołaniem wydanego upoważnienia do przetwarzania danych osobowych.

2.9 Przyczynę czasowego wyrejestrowania użytkownika z systemu informatycznego może stanowić:

- ✓ jego nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych, o której winien poinformować ASI bezpośredni przełożony pracownika;
- ✓ zawieszenie w pełnieniu obowiązków służbowych, o którym administrator systemu informatycznego winien być poinformowany przez bezpośredniego przełożonego pracownika bądź przez komórkę ds. kadr.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

3.1 Przed przystąpieniem do pracy w systemie informatycznym, użytkownik winien zapewnić sobie zorganizowanie stanowiska pracy z wykorzystaniem systemu informatycznego w sposób zgodny z przyjętymi poniżej zasadami bezpiecznego przetwarzania informacji.

3.2 Przed rozpoczęciem przetwarzania danych osobowych w systemach informatycznych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego uszkodzenia sprzętu komputerowego. W przypadku wystąpienia jakichkolwiek nieprawidłowości, powiadamia bezpośredniego przełożonego i administratora systemu informatycznego.

3.3 Rozpoczęcie pracy na stacji roboczej następuje poprzez:

- ✓ uruchomienie komputera;
- ✓ wprowadzenie loginu i hasła lub samego hasła, w zależności od sposobu skonfigurowania jednostki;
- ✓ hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby postronne;
- ✓ w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego loginu i hasła, użytkownik natychmiast powiadamia o tym fakcie bezpośredniego przełożonego i administratora systemu informatycznego;
- ✓ w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe, pracownik natychmiast powiadamia o zaistniałym fakcie bezpośredniego przełożonego i administratora systemu informatycznego oraz powstrzymuje się przed dalszym korzystaniem z aplikacji.

3.4 Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem loginu i hasła dostępu innego użytkownika.

3.5 W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi:

- ✓ dokonać zapisu wprowadzonych danych, wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych lub,
- ✓ zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła [klawisze: windows+L lub klawisze: ctr+alt+delet].

3.6 W przypadku zakończenia pracy użytkownik musi:

- ✓ wylogować się z systemu informatycznego służącym do przetwarzania danych osobowych. Wylogowanie powinno być poprzedzone zapisem wprowadzonych danych, opcjonalnie sporządzeniem w miarę potrzeb kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem nośników danych płyty CD, pendrive i innych, zawierających dane osobowe;
- ✓ zamknąć wszystkie aplikacje uruchomione na stacji roboczej;
- ✓ wyłączyć stację roboczą za pomocą odpowiednich poleceń, zawartych w zainstalowanym na niej systemie operacyjnym. Zabronione jest wyłączanie jednostki za pomocą przycisków „POWER" lub „RESET", (możliwe tylko i wyłącznie na wyraźne polecenie administratora systemu informatycznego);
- ✓ po wyłączeniu stacji roboczej, należy wyłączyć wszystkie pozostałe urządzenia z nią współpracujące, takie jak: monitor, drukarka, skaner, UPS, itp.;
- ✓ pozostawienie włączonych stacji roboczych poza godzinami pracy jednostki, możliwe jest po uzyskaniu zgody przełożonego i poinformowaniu o tym fakcie administratora systemu informatycznego;

- ✓ administrator systemu informatycznego prowadzi rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki. Wzór rejestru stanowi **załącznik nr 2** do Instrukcji - *Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki.*

3.7 Powyżej wskazane zasady obowiązują przy przetwarzaniu danych osobowych również na komputerach przenośnych, w tym również poza siedzibą jednostki z wyjątkiem konieczności powiadamiania administratora systemu informatycznego o użytkowaniu urządzenia poza godzinami pracy jednostki.

3.8 Administrator systemu informatycznego prowadzi *Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą jednostki* wg wzoru zamieszczonego w **załączniku nr 3** do niniejszej instrukcji. W rejestrze należy uwzględnić również tablety oraz smartfony.

3.9 Użytkownicy, którym zostały powierzone komputery przenośne powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Sposób użytkowania komputerów przenośnych określa *Regulamin użytkowania komputerów przenośnych* stanowiący **załącznik nr 4** do niniejszej instrukcji.

3.10 Pliki zawierające dane osobowe przechowywane na komputerach przenośnych muszą być zaszyfrowane i opatrzone hasłem dostępu.

3.11 Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych nawet w postaci zaszyfrowanej.

3.12 Obowiązuje kategoryczny zakaz samodzielnej modernizacji, naprawy, aktualizowania jakiegokolwiek elementu wchodzącego w skład użytkowanego systemu informatycznego. Wszelkie zmiany, mogą być wykonane przez administratora systemu informatycznego lub w jego obecności przez podmiot serwisujący dany system informatyczny lub urządzenie.

4. Zasady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

4.1 Do wykonywania kopii zapasowych całościowych baz danych, plików aplikacji oraz systemów wykorzystywanych do przetwarzania danych osobowych, upoważniony jest jedynie administrator systemu informatycznego.

4.2 Administrator systemu informatycznego prowadzi rejestr kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

4.3 Dla każdego elementu wymienionego w pkt. 4.2 będącego przedmiotem wykonywania kopii zapasowych, administrator systemu informatycznego w porozumieniu z użytkownikiem (grupą użytkowników, komórką organizacyjną użytkującą elementy), określa częstotliwość wykonywania kopii zapasowych. Przedmiotowe ustalenia muszą zostać udokumentowane w postaci przyjętego harmonogramu wykonywania kopii zapasowych. Wzór *Harmonogramu wykonywania kopii zapasowych* stanowi **załącznik nr 5.**

4.4 Administrator systemu informatycznego w odniesieniu do każdego systemu, określi rodzaj wykonywanej kopii wybierając jej wariant z możliwych, o których mowa poniżej tj.

- ✓ standardowa – polega na skopiowaniu każdego wybranego pliku i wyczyszczeniu archiwa. Dzięki czemu przy tworzeniu kolejnej kopi zapiszą się pliki, w których zmieniło się archiwum. Tworzenie tego typu kopi trwa najdłużej. Zazwyczaj jest wykonywane przy tworzeniu pierwszej kopi;
- ✓ przyrostowa – wybór tego typu kopi zapasowej powoduje archiwizacje plików które zostały utworzone lub zmodyfikowane od momentu wykonania ostatniej kopi przyrostowej lub kopi normalnej. Proces odtwarzania danych polega na przywróceniu normalnej kopi zapasowej oraz kopi przyrostowych w kolejności tworzenia. Tworzenie kopi przyrostowej zajmuje mniej miejsca oraz mniej czasu niż w porównaniu z kopią normalną. Jednak odtwarzanie zajmuje więcej czasu;
- ✓ różnicowa – kopiuje tyle te pliki, które zmieniły się od czasu wykonania ostatniej kopii normalnej lub przyrostowej. Kopia różnicowa nie zmienia atrybuty archiwizacji plików. Aby przywrócić dane wystarczy kopia normalna i ostatnia kopia różnicowa. Kopia ta zajmuje więcej miejsca niż kopia przyrostowa, ale nie trzeba każdej wersji przechowywać na dysku, bo wystarczy najnowsza;
- ✓ codzienna – wykonuje kopie tylko tych plików które zostały utworzone lub zmienione w dni wykonania archiwizacji. Podczas wykonywania tej kopi nie jest czyszczony atrybut archiwizacji;
- ✓ kopia (backup) – polega na skopiowaniu zaznaczonych plików bez czyszczenia atrybutów archiwizacji. Opcja ta przydaje się dla osób, które wykonują kopie raz na jakiś czas i nie potrzebują regularnej archiwizacji lub chcą mieć dodatkową kopię pomiędzy cyklem archiwizacji.

4.4 Użytkownik może zapisywać i wykonywać kopie sporządzanych pism i innych dokumentów roboczych wyłącznie wtedy, gdy związane są z prowadzonymi przez niego sprawami i nie stanowią zbiorów danych osobowych lub częściowych wyciągów z nich.

4.5 Za dopuszczalne można uznać zapisywanie kopii, o których mowa w pkt. 4.4 na nośniku zewnętrznym pod warunkiem, że nośnik taki pod koniec każdego dnia pracy, będzie przekazywany do przechowania bezpośredniemu przełożonemu użytkownika.

4.6 Po upływie okresu użyteczności lub przechowywania, kopie zapasowe, a w szczególności zawierające dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

4.7 Nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika w sposób uniemożliwiający odczytanie zapisanych na nich danych.

4.8 W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych, służących do przetwarzania danych osobowych, należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający ich odczyt. Z powyższych czynności likwidacji nośników należy sporządzić protokół.

5. Zasady postepowania z elektronicznymi nośnikami danych osobowych

5.1 Nie należy przechowywać zbędnych nośników zawierających dane osobowe oraz nieprzydatnych kopii zapasowych zawierających dane osobowe.

5.2 W jednostce dopuszcza się użytkowanie tylko i wyłącznie nośników wydanych przez administratora systemu informatycznego, który odpowiada za ich ewidencjonowanie. Ewidencja jest prowadzona wg wzoru stanowiącego **załącznik nr 7** do niniejszej instrukcji.

5.3 Elektroniczne nośniki informacji zawierające dane osobowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w załączniku nr 10 do *Polityki ochrony danych osobowych.* Jedynym wyjątkiem jest sytuacja, gdzie kopie zapasowe ze względów bezpieczeństwa i zapewnienie możliwości przywrócenia lub odtworzenia działania są przechowywane poza siedzibą jednostki oraz sytuacje wymagające przeniesienia danych między różnymi lokalizacjami.

5.4 Elektroniczne nośniki informacji, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, celem zabezpieczenia ich przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

5.5 Nośniki zawierające kopie zapasowe, których celem jest zapewnienie możliwości przywrócenia działania i odtworzenia danych po awarii lub innym zdarzeniu o charakterze katastroficznym, winny być przechowywane w innych lokalizacjach, niż lokalizacja jednostek komputerowych, z których dokonano kopii zapasowych, przy jednoczesnym spełnieniu wszystkich zasad bezpiecznego

przechowywania, dających gwarancję ich zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem oraz gwarancję pełnej dostępności na wypadek konieczności ich wykorzystania w celu przywrócenia lub odtworzenia działań jednostki.

5.6 Okres przechowywania nośników informacji zawierających kopie zapasowe dla poszczególnych systemów informatycznych służących przetwarzaniu danych osobowych określa **załącznik nr 5** do Instrukcji – *Harmonogram wykonywania kopii zapasowych.* Po upływie tego okresu nośniki danych są niszczone lub dane na nich zawarte trwale usuwane.

5.7 Dopuszcza się powierzenie niszczenia nośników (szczególnie papierowych) danych osobowych, wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

- ✓ zawarcia umowy powierzenia danych osobowych do dalszego przetwarzania z tym podmiotem;
- ✓ zagwarantowania poufności danych przez usługodawcę;
- ✓ umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD lub upoważnionego przez niego pracownika jednostki;
- ✓ udokumentowania faktu przekazania nośników do zniszczenia protokołem.

5.8 W przypadku wycofania sprzętu komputerowego z użycia, dane osobowe na nim zapisane są kasowane przez administratora systemu informatycznego przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk takiego urządzenia podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada administrator systemu informatycznego. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez administratora systemu informatycznego.

5.9 W przypadku przekazania sprzętu komputerowego do podmiotu zewnętrznego, celem jego naprawy, należy usunąć z niego wszystkie zapisy zawierające dane osobowe, jeżeli jest to niemożliwe naprawa/serwisowanie takiego sprzętu, może być realizowana jedynie w obecności administratora systemu informatycznego.

5.10 Przekazanie sprzętu komputerowego do podmiotu zewnętrznego musi być potwierdzone protokołem przekazania, a jego odbiór również winien być zaprotokołowany.

6. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

6.1 W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

- ✓ uruchamiania użytkownikowi jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w jednostce;
- ✓ samowolnego korzystania z nośników przenośnych innych niż wydane przez administratora systemu informatycznego;
- ✓ otwierania poczty elektronicznej, której tytuł (temat) nie sugeruje związku z pełnionymi obowiązkami służbowymi lub adres nadawcy budzi obawy. W przypadkach wątpliwych należy skonsultować się z administratorem systemu informatycznego;
- ✓ korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
- ✓ podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.

6.2 W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania, użytkownik zobowiązany jest powiadomić swojego przełożonego i administratora systemu informatycznego. Do objawów powyższych można zaliczyć:

- ✓ istotne spowolnienie działania systemu informatycznego;
- ✓ nietypowe działanie aplikacji;
- ✓ nietypowe komunikaty;
- ✓ utratę danych lub modyfikację danych.

6.3 System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

- ✓ oprogramowanie antywirusowe;
- ✓ zaporę sieciową;
- ✓ wykorzystywanie wyłącznie oprogramowania systemowego posiadającego wsparcie techniczne;
- ✓ automatyczną aktualizację oprogramowania systemowego oraz antywirusowego;
- ✓ konfigurację oprogramowania, o którym mowa powyżej w sposób minimalizujący ryzyko naruszenia bezpieczeństwa (ciągła praca w tle i wykrywanie zagrożeń w czasie rzeczywistym);
- ✓ monitoring ruchu sieciowego;

- ✓ zainstalowanie ww. oprogramowania na każdej stacji roboczej i jednostce komputerowej.
- ✓ stałe blokowanie dostępu do stron internetowych sklasyfikowanych jako potencjalnie niebezpieczne (np.: portale randkowe i erotyczne),

6.4 Za nadzór nad powyższymi zabezpieczeniami jest odpowiedzialny administrator systemu informatycznego, a w szczególności za:

- ✓ weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
- ✓ weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
- ✓ przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
- ✓ weryfikację poprawności aktualizacji oprogramowania systemowego.

7. Wykonywanie przeglądów i konserwacji systemów informatycznych oraz urządzeń służących do ich funkcjonowania

7.1 Konserwacja sprzętu i urządzeń pracujących w systemach informatycznych jednostki ma na celu, zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzeniu lub naruszenia bezpieczeństwa.

7.2 Przeglądy i konserwacje urządzeń wchodzących w skład użytkowanych systemów informatycznych, są dokonywane przez administratora systemu informatycznego, wyznaczone przez niego osoby lub przez podmioty zewnętrzne w oparciu o zawarte umowy serwisowe.

7.3 W odniesieniu do użytkowanej w jednostce infrastruktury informatycznej realizowane są okresowe czynności konserwacyjne w sposób zapewniający, iż każdy jej element (jednostki robocze, drukarki, skanery, monitory itd.), zostanie objęty czynnościami, o których mowa minimum raz w roku. Harmonogram prac z tym związanych sporządza administrator systemu informatycznego wg **załącznika nr 6** do niniejszej instrukcji – *Harmonogram przeglądów i konserwacji urządzeń*. Przy tworzeniu harmonogramu należy uwzględnić zalecenia producenta urządzenia.

7.4 Prace serwisowe wykonywane na terenie jednostki przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi administratora systemu informatycznego lub osoby przez niego wyznaczonej.

7.5 Wszelkie prace serwisowe oraz prace, o których mowa w pkt. 5.9 niniejszej instrukcji wymagają sporządzenia protokołu zawierającego co najmniej następujące informacje:

- ✓ wskazanie osoby przeprowadzającej prace serwisowe lub przyjmującej sprzęt do serwisowania oraz podmiotu, którego osoba ta jest pracownikiem;
- ✓ wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie jednostki);
- ✓ przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu, w przypadku oprogramowania określenie systemu będącego przedmiotem serwisu);
- ✓ zakres prac serwisowych i ich wynik;
- ✓ czas przeprowadzania prac serwisowych.

7.6 Zabronione jest wykonywanie czynności związanych z konserwacją i naprawą urządzeń wchodzących w skład systemów informatycznych samodzielnie przez ich użytkowników.

7.7 Powierzenie sprzętu użytkownikowi, nieodłącznie wiąże się z przekazaniem jemu instrukcji obsługi opracowanej przez producenta lub innego dokumentu, zawierającego zasady bezpiecznego użytkowania powierzonego sprzętu.

8. Kontrola licencjonowanego oprogramowania

8.1 Administrator systemu informatycznego celem uzyskania zapewnienia, iż jednostka wykorzystuje jednie legalne oprogramowanie, prowadzi spis użytkowanych w jednostce systemów, programów i aplikacji zawierający:

- ✓ informację o nośniku instalacyjnym (jeżeli występuje) i miejscu jego przechowywania;
- ✓ określenie licencji (np.: wersja jedno, wielostanowiskowa, z ograniczeniami, bez ograniczeń itp.) ze wskazaniem okresu jej ważności;
- ✓ określenie miejsca zainstalowania (ze wskazaniem nr inwentarzowego jednostki komputerowej lub jej nazwy, komórki organizacyjnej, nr pomieszczenia),

8.2 IOD niezależnie od innych osób posiada prawo do kontroli spisu licencjonowanego oprogramowania ze względu na charakter realizowanych działań.

8.3 Kontrole IOD licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym po uprzednim poinformowaniu kierownika jednostki.

8.4 Do przesłanek uruchamiających proces kontroli doraźnej w szczególności można zaliczyć:

- ✓ informację o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika, na żądanie, jego przełożonego lub innej osoby posiadającej wiedzę o takim zdarzeniu;

- ✓ otrzymanie zgłoszenia lub innej informacji o pojawieniu się lub podejrzeniu pojawienia się w systemie informatycznym nieautoryzowanego oprogramowania, aplikacji,

8.5 Nie rzadziej niż raz na dwa lata ASI w porozumieniu z IOD przeprowadza planową kontrolę spisu użytkowanego w jednostce oprogramowania.

8.6 Okresowo, nie rzadziej niż raz w roku, wszystkie komputery przenośne użytkowane poza lokalizacjami jednostki są sprawdzane przez administratora systemu informatycznego pod kątem obecności nieautoryzowanego oprogramowania.

8.7 W terminie do 20 stycznia każdego roku obrachunkowego celem zatwierdzenia, administrator systemu informatycznego przedstawia kierownikowi jednostki aktualne zestawienie przenośnych jednostek komputerowych, o których mowa w pkt. 8.6 wraz z harmonogramem ich przeglądu.

8.8 Do przeprowadzenia kontroli zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, mogą zostać zastosowane narzędzia programistyczne umożliwiające m.in.:

- ✓ automatyczne sprawdzanie stacji roboczych i serwerów,
- ✓ centralne zarządzanie spisem licencjonowanego oprogramowania,
- ✓ automatyczne ostrzeganie przed przekroczeniem liczby licencji.

8.9 Administrator systemu informatycznego odpowiada za niezwłoczne usunięcie nielicencjonowanego oprogramowania, a informacja o przypadkach używania nieautoryzowanego oprogramowania jest przedstawiana kierownikowi jednostki.

9. Zarządzanie poprawkami technicznymi

9.1 Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów informatycznych, programów.

9.2 Administrator systemu informatycznego zobowiązany jest do bieżącego i ciągłego monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych, programów i aplikacji wykorzystywanych w jednostce.

9.3 Administrator systemu informatycznego obowiązany jest do wprowadzania poprawek w oparciu o informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych, programów i aplikacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.

9.4 Poprawki techniczne, w zależności od ich krytyczności i istotności są testowane w środowisku

testowym, zanim zostaną wprowadzone do środowiska produkcyjnego. Administrator bezpieczeństwa informacji prowadzi rejestr dokonywanych zmian. Nie dotyczy to systemów, które samodzielnie rejestrują wprowadzone poprawki techniczne.

9.5 Wprowadzanie krytycznych i istotnych poprawek bezpośrednio do środowiska produkcyjnego przez ASI, może być wykonane wyłącznie po skonsultowaniu takiego stanu rzeczy z użytkownikami zasobu obsługiwanego przez system, program, aplikację, którego dotyczy poprawka.

10. Bezpieczeństwo systemów operacyjnych

10.1 W jednostce stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:

- ✓ uwierzytelnianie użytkowników, zgodnie z przyjętymi zasadami kontroli dostępu;
- ✓ rejestrowanie nieudanych prób dostępu do systemu;
- ✓ rejestrowanie użytkowników systemów operacyjnych;
- ✓ generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu;
- ✓ blokowanie dostępu po 10 minutach braku aktywności w sesji.

10.2 Systemy operacyjne użytkowane w jednostce muszą mieć włączone mechanizmy bezpiecznego logowania zapewniające (w zależności od możliwości technicznych):

- ✓ ujawnianie minimum informacji o systemie;
- ✓ wyświetlanie ostrzeżenia, że dostęp do systemu jest dozwolony jedynie dla uprawnionych użytkowników;
- ✓ unikanie wyświetlania komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi przy nieautoryzowanych próbach dostępu;
- ✓ unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania;
- ✓ ograniczenie liczby nieudanych prób logowania się do systemu do 3, a następnie blokowanie konta po 3 następujących po sobie nieudanych próbach logowania;
- ✓ wykonywanie zapisu każdego nieudanego logowania w logach zdarzeń;
- ✓ ograniczenie możliwości zalogowania się do systemu w określonych przedziałach czasowych („oknach logowania") w godzinach np. 6-18;
- ✓ blokowanie wyświetlania hasła w trakcie jego wprowadzania;
- ✓ szyfrowanie przesyłanych haseł.

10.3 Wszyscy użytkownicy systemów muszą posiadać unikalne identyfikatory użytkownika (loginy, identyfikatory ID użytkownika) do swojego wyłącznego użytku.

10.4 Dostęp do systemu dla użytkownika, który trzykrotnie pod rząd podał błędne hasło jest blokowany. Odblokowania dokonuje ręcznie administrator systemu informatycznego na pisemny wniosek bezpośredniego przełożonego pracownika.

11. Zarządzanie zmianami w systemach informatycznych

11.1 Kryteria odbioru systemu informatycznego obejmują dostarczenie przez dostawcę:

- ✓ w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika;
- ✓ w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury;

11.2 Ponadto, kryteria odbioru obejmują:

- ✓ sprawdzenie wymagań wydajnościowych i pojemnościowych systemu informatycznego,
- ✓ dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia;
- ✓ dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji, a w szczególności przetwarzanych danych osobowych został uwzględniony;
- ✓ szkolenia z zakresu posługiwania się i działania nowych systemów;

11.3 Odbiór nowo instalowanych systemów informatycznych lub oprogramowania systemowego obejmuje następujące główne elementy:

- ✓ wykonanie instalacji oprogramowania;
- ✓ wykonanie testowania systemu zakończone stosownym dokumentem potwierdzającym prawidłowość testów;
- ✓ odbiór oprogramowania potwierdzony stosownym dokumentem;
- ✓ odrzucenie oprogramowania potwierdzone stosownym dokumentem w przypadku negatywnych wyników testów;
- ✓ w przypadku wystąpienia jakichkolwiek rozbieżności, co do jakości produktu, może zostać zlecony zewnętrzny audyt mający na celu wyjaśnienie przyczyn rozbieżności.

11.4 Każdorazowo, w odniesieniu do systemów operacyjnych oraz użytkowanych aplikacji, wszelkie ich

zmiany na nowsze wersje administrator systemu informatycznego winien odnotować odrębnym dokumentem sporządzonym w dowolnej formie (notatka, protokół):

- ✓ wykaz dokonanych zmian w systemie (oprogramowaniu) w stosunku do poprzedniej wersji wraz z ich opisem;
- ✓ uaktualnienie dokumentacji opisującej system (oprogramowanie) uwzględniające zmiany dokonane.

11.5 Mechanizmy opisane w pkt. od 11.1 do 11.4 mają na celu zapewnianie poprawnego i bezpiecznego działania systemów informatycznych pracujących w jednostce.

11.6 Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i oceną ryzyka w związku ze zmianami dokonywanymi w systemach informatycznych jednostki.

11.7 Każda zmiana w systemie informatycznym dotycząca jego kluczowych elementów musi być udokumentowana.

11.8 Zasady wskazane w niniejszym rozdziale odnoszą się do:

- ✓ zmian infrastruktury technicznej systemu informatycznego, sprowadzających się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędu w infrastrukturze, przy czym:

  - zmiana infrastruktury regularna – oznacza zmianę, która nie wymaga natychmiastowego wdrożenia,

  - zmiana infrastruktury awaryjna - stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny, z pominięciem lub uproszczeniem niektórych etapów (np. testów) przy założonym ryzyku,

  - zmiana infrastruktury rutynowa - zaakceptowane wcześniej działanie związane z relatywnie prostymi czynnościami np. wymiana drukarki lub monitora.

- ✓ zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, zmiany aplikacyjne są klasyfikowane, jako:

  - zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,

  - zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania, aplikacji,

11.9 Za proces zarządzania zmianami odpowiedzialny jest administrator systemu informatycznego i kierownik komórki organizacyjnej, w której dokonuje się zmian.

11.10 Każda zmiana regularna jest poprzedzona udokumentowanym:

- ✓ opisem zmiany;
- ✓ opisem przyczyny zmiany wraz z podaniem aktów prawnych uzasadniających zmianę;
- ✓ opisem rodzaju wymaganych działań;
- ✓ szacowaniem ryzyka potencjalnego wpływu zmian;
- ✓ wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń;
- ✓ przetestowaniem zmian.

11.11 Za realizację działań wskazanych w pkt. 11.10 odpowiada kierownik komórki organizacyjnej, w której realizowane są zmiany wspólnie z administratorem systemu informatycznego

11.12 Jeżeli zmiana ma charakter awaryjny, dokumentacja, o której mowa w pkt. 11.10 może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.

11.13 Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności jednostki, wymaga zgody kierownika jednostki.

12. Bezpieczeństwo dokumentacji systemu

12.1 Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemów podlegają ochronie i nie powinna stanowić informacji o charakterze publicznym.

12.2 Osobą odpowiedzialną za aktualność i kompletność dokumentacji, o której mowa w niniejszym rozdziale jest administrator systemu informatycznego.

11.3 Nieograniczony dostęp do przedmiotowej dokumentacji posiada administrator systemu informatycznego, pozostałym osobom (użytkownikom) jest ona udostępniana na zasadzie „wiedzy koniecznej".

13. Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

13.1 System bezpieczeństwa poczty elektronicznej winien zapewniać:

ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej,

- ✓ ochronę antywirusową załączników przesyłanych w poczcie elektronicznej;

- ✓ ochronę antyspamową;
- ✓ możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej;
- ✓ monitorowanie i rejestrowanie poczty elektronicznej.

13.2 Zasoby poczty elektronicznej podlegają sporządzaniu kopii zapasowej. Kopia zapasowa sporządzana jest zgodnie z harmonogramem dla właściwego serwera pocztowego.

13.3 System poczty elektronicznej nakłada ograniczenia, co do rozmiaru pojedynczej skrzynki pocztowej oraz wielkości przesyłanej wiadomości.

13.4 Ruch HTTP między klientem poczty w Internecie, a serwerem poczty powinien być zabezpieczony za pomocą protokołu szyfrującego SSL.

13.5 Uwierzytelnienie dostępu użytkownika do poczty internetowej realizowane jest za pomocą certyfikatu lub identyfikatora i hasła.

13.6 Administrator systemu informatycznego jest odpowiedzialny za ochronę kluczy w trakcie ich użytkowania, a w szczególności za ochronę klucza prywatnego przed ujawnieniem lub nieautoryzowanym użyciem. W przypadku zaistnienia faktu (lub uzasadnionego podejrzenia), naruszenia ochrony klucza prywatnego, należy niezwłocznie przeprowadzić proces unieważniania certyfikatu.

13.7 Odnowienie certyfikatu klucza publicznego musi nastąpić przed końcem okresu jego ważności.

13.8 Po zakończeniu użytkowania certyfikatu klucza publicznego, w przypadku stosowania go wyłącznie do zabezpieczenia komunikacji w protokole SSL, należy parę kluczy zniszczyć w sposób nieodwracalny.

14. Zasady przechowywania haseł przez administratora systemu informatycznego

14.1 Administrator systemu informatycznego zobowiązany jest do zachowania wszystkich haseł dostępu wykorzystywanych przy administrowaniu systemem informatycznym jednostki.

14.2 Utrzymywanie w poufności przedmiotowych haseł, przez administratora systemu informatycznego nie może stanowić samo w sobie zagrożenia w sytuacji zaistnienia nagłej konieczności ich użycia w trakcie czasowej lub trwałej jego nieobecności.

14.3 W celu zapewnienia ciągłości działania jednostki na wypadek nieprzewidzianych zdarzeń o charakterze losowym wprowadza się zasady postępowania w odniesieniu do haseł dostępowych użytkowanych przez osobę lub podmiot pełniący funkcję administratora systemu informatycznego w odniesieniu do wszystkich elementów infrastruktury informatycznej jednostki.

- ✓ administrator systemu informatycznego jest zobowiązany do prowadzenia tzw. wykazu haseł w systemie kopertowym;

- ✓ każde hasło użytkowane przez administratora systemu informatycznego musi zostać zapisane i umieszczone w zaklejonej kopercie z opisem czego dotyczy;
- ✓ koperty zawierające hasła winny być przechowywane przez administratora danych osobowych w sposób gwarantujący wyłącznie jemu dostęp do zarchiwizowanych haseł;
- ✓ w przypadku nagłej konieczności ADO może udostępnić hasło osobie zastępującej administratora systemu informatycznego, która po wykorzystaniu hasła nadaje nowe, które również zapisuje i w zaklejonej kopercie powierza administratorowi systemu informatycznego;
- ✓ każdy przypadek wykorzystania „systemu kopert" winien być zgłoszony przez osobę wykorzystującą hasło z koperty wraz z uzasadnieniem IOD.

15. Pozostałe zasady ochrony systemu informatycznego służącego przetwarzaniu danych osobowych

15.1 Administrator danych osobowych, administrator bezpieczeństwa informacji oraz inspektor ochrony danych osobowych mają prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

15.2 Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją.

15.3 Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych będzie uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym.

15.4 Wraz z niniejszą instrukcją przyjmuje się nw. standardy do stosowania:

- standard bezpiecznego przetwarzania danych osobowych,
- standard bezpiecznego rozmieszczenia urządzeń infrastruktury informatycznej,
- standard bezpiecznego okablowania.

16. Standard bezpiecznego przetwarzania danych osobowych

Standard bezpiecznego przetwarzania informacji wynika z przestrzegania niżej wymienionych zasad:

16.1 Zasada przywilejów koniecznych – polegająca na tym, że każdy użytkownik systemu informatycznego, posiada prawa dostępu do danych ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych zadań i wynikających z otrzymanego upoważnienia.

16.2 Zasada wiedzy koniecznej – polegająca na tym, że poszczególni pracownicy mają dostęp do danych ograniczony wyłącznie do tych, których znajomość jest konieczna do realizacji powierzonych im zadań.

16.3 Zasada usług koniecznych – polegająca na tym, że zakres dostępnych użytkownikowi usług systemu informatycznego jest ograniczony tylko do tych usług, które są konieczne do prawidłowego realizowania obowiązków służbowych.

16.4 Zasada asekuracji zabezpieczeń – polegająca na tym, że wszyscy użytkownicy systemu informatycznego są świadomi konieczności ochrony wykorzystywanych zasobów.

16.5 Zasada indywidualnej odpowiedzialności – polegająca na tym, że za utrzymywanie właściwego poziomu bezpieczeństwa poszczególnych elementów systemu informatycznego, odpowiadają konkretne osoby, które mają świadomość tego, za co są odpowiedzialne i jakie konsekwencje poniosą, jeżeli zaniedbają swoje obowiązki.

16.6 Zasada obecności koniecznej – polegająca na tym, że prawo przebywania w określonych pomieszczeniach mają wyłącznie osoby, które są do tego upoważnione.

16.7 Zasada najsłabszego ogniwa łańcucha – polegająca na tym, że poziom bezpieczeństwa systemu informatycznego wyznacza najsłabszy element tego systemu (najczęściej jest to człowiek).

16.8 Zasada separacji obowiązków – polegająca na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa systemu informatycznego nie mogą być realizowane przez jedną osobę.

16.9 Zasada wykorzystywania udostępnionego przez pracownikowi sprzętu, aplikacji programowych, konta poczty elektronicznej tylko i wyłącznie dla realizacji obowiązków służbowych. W praktyce oznacza to całkowity zakaz wykorzystywania powierzonych urządzeń i konta poczty elektronicznej dla potrzeb prywatnych.

16.10 Zasada niepozostawiania danych o charakterze poufnym na automatycznych sekretarkach oraz przesyłania drogą faksową.

16.11 Zasada czystego biurka dla dokumentów papierowych oraz zasada czystego ekranu.

17. Standard bezpiecznego rozmieszczenia i ochrony sprzętu

Sprzęt wykorzystywany do przetwarzania danych osobowych (jednostki komputerowe, monitory, klawiatury, drukarki, skanery itp.) powinien być tak rozlokowany i tak chroniony, aby redukować ryzyko

wynikające z zagrożeń środowiskowych (zalanie przez nieszczelne okno, kradzież) oraz nieautoryzowanego dostępu. W tym celu należy przestrzegać nw. reguł;

17.1 Każdy sprzęt musi posiadać nr inwentarzowy i być przypisany do konkretnego użytkownika odpowiedzialnego materialnie za jego stan.

17.2 Sprzęt należy rozmieszczać w sposób zapewniający sprawowanie nad nim nadzoru przez osobę materialnie odpowiedzialną za jego stan.

17.3 W miejscu lokalizacji sprzętu winna się znajdować instrukcja jego obsługi opracowana przez producenta.

17.4 Niedopuszczalne jest usytuowanie sprzętu poza obszarami przetwarzania tj.: korytarze i inne ciągi komunikacyjne oraz pomieszczenia lub ich części, do których mają nieograniczony dostęp klienci jednostki.

17.5 Celem zapobieżenia uszkodzeniu urządzeń na skutek zalania pomieszczenia, ułatwienia czynności sprzątania pomieszczenia, nie należy umieszczać jego bezpośrednio na podłodze, lecz na stabilnych podstawach (biurko, półki, stoliki itp.),

17.6 Ponadto przy rozmieszczaniu sprzętu należy przestrzegać następujących zasad:

- ✓ nie należy umieszczać sprzętów w bezpośrednim sąsiedztwie źródeł ciepła (grzejniki, inne urządzenia grzewcze) oraz na parapetach okiennych;
- ✓ w pomieszczeniach na niskich kondygnacjach sprzęt nie powinien być rozmieszczany w bezpośrednim sąsiedztwie okien;
- ✓ urządzenia wchodzące w skład systemu informatycznego winny być podpięte do sieci elektrycznej za pośrednictwem listew antyprzepięciowych, które po zakończeniu pracy są wyłączane;
- ✓ niedopuszczalne jest podpinanie do listew antyprzepięciowych dodatkowo jakichkolwiek innych urządzeń elektrycznych nie będących częścią systemu informatycznego.

17.7 W bezpośrednim sąsiedztwie urządzeń wchodzących w skład systemu informatycznego obowiązuje kategoryczny zakaz spożywania posiłków, napojów i palenia tytoniu.

17.8 Wszystkie pomieszczenia wchodzące w skład obszarów przetwarzania winny posiadać instalację alarmową i znajdować się w budynku wyposażonym w instalację odgromową.

18.Standard bezpiecznego okablowania

Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne powinno być chronione przed przejęciem (wykorzystaniem do nieautoryzowanego przetwarzania danych) lub uszkodzeniem. W odniesieniu do bezpieczeństwa okablowania należy przestrzegać następujących zasad:

18.1 Tam, gdzie to możliwe, linie zasilające i telekomunikacyjne należy prowadzić pod ziemią, tynkiem lub zabezpieczyć je w inny stosowny sposób adekwatny do zagrożeń.

18.2 Należy chronić okablowanie sieciowe przed nieautoryzowanym dostępem i przejęciem za pomocą rur, korytek kablowych unikając w mirę możliwości ich prowadzenia przez obszary wchodzące w skład strefy publicznej (ogólnodostępnej dla klientów jednostki).

18.3 Należy oddzielać okablowanie zasilające od okablowania komunikacyjnego celem uniknięcia zjawiska interferencji.

18.4 Należy używać jednoznacznego oznakowania umożliwiającego identyfikację kabli i sprzętu w celu zmniejszenia ryzyka takich błędów, jak nieumyślne połączenie nieodpowiedniego kabla sieciowego.

18.5 Niedopuszczalne jest prowadzenie przewodów zasilających i komunikacyjnych w sposób narażający je na deptanie, rozjeżdżanie fotelami i tym podobne zagrożenia.

18.6 Należy prowadzić dokumentację połączeń elektrycznych i komunikacyjnych w celu zmniejszenia prawdopodobieństwa błędów.

18.7 W odniesieniu do części systemów o znaczeniu krytycznym lub wrażliwym dodatkowo należy wprowadzić zabezpieczenia w postaci:

- ✓ zbrojonych rur lub koryt kablowych, zamknięć pomieszczeń w miejscach zakończeń sieci i instalacji o podwyższonym standardzie bezpieczeństwa;
- ✓ alternatywnego systemu zasilania (UPS) i transmisji (sieć bezprzewodowa) zapewniającego ciągłość działalności;
- ✓ ekranów elektromagnetycznych do ochrony kabli;
- ✓ systemu kontroli dostępu do pomieszczeń, jeżeli znajdują się w nich panele połączeniowe lub inna infrastruktura techniczna o podobnym znaczeniu;
- ✓ systematycznych przeglądów pod kątem możliwości podłączenia nieautoryzowanych urządzeń.

Załączniki:

Załącznik nr 1 - Rejestr osób upoważnionych do systemów

Załącznik nr 2 – Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki

Załącznik nr 3 – Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą

Załącznik nr 4 – Regulamin użytkowania komputerów przenośnych

Załącznik nr 5 – Harmonogram wykonywania kopii zapasowych

Załącznik nr 6 – Harmonogram przeglądów i konserwacji urządzeń

Rejestr osób upoważnionych do systemów

L.p.	Nazwisko	Imię	Login	Data nadania	Obsługiwane systemy informatyczne ze wskazaniem dostępu lub jego braku do poczty zewnętrznej	Data odebrania

Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki

L.p.	Nazwisko	Imię	Login	Przedział czasowy wykorzystywania systemów informatycznych ze wskazaniem dni i godzin	Wykorzystywane systemy informatyczne

Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą jednostki

L.p.	Określenie jednostki komputerowej (nazwa nr seryjny, nr inwentarzowy)	Imię i nazwisko użytkownika	Nazwa komórki organizacyjnej	Podpis osoby przyjmującej urządzenie do użytkowania	Data wydania urządzenia do użytkowania	Data zwrotu urządzenia	Podpis osoby przyjmującej zwrot urządzenia

Regulamin użytkowania komputerów przenośnych

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą zapoznać się z Regulaminem użytkowania komputera przenośnego i zobowiązują do jego przestrzegania.

2. Dane osobowe lub dane poufne muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).

3. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.

4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem przełożonemu i administratorowi systemu informatycznego.

5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:

   ✓ zaleca się przenoszenie komputera przenośnego w przeznaczonej do tego celu torbie;

   ✓ zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej;

   ✓ zabrania się pozostawiania komputera przenośnego w miejscach typu przechowalnie bagażu,

6. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych w sposób uzgodniony z administratorem systemu informatycznego.

7. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych oraz powstrzymania się od korzystania z internetu z wykorzystaniem publicznej sieci wi-fi.

8. Użytkownik komputera przenośnego zobowiązuje się do nie udostępniania jego innym osobą w jakimkolwiek celu.

9. Użytkownik komputera przenośnego nie może dokonywać samodzielnie jakichkolwiek jego napraw, modernizacji i innych czynności związanych z ingerencją w parametry konfiguracyjne jednostki.

Harmonogram wykonywania kopii zapasowych

L.p.	Określenie zasobów informacyjnych podlegających kopiowaniu	Określenie częstotliwości wykonywania kopii	Określenie metody wykonywania kopii	Określenie miejsca przechowywania nośników kopii	Określenie terminu przechowywania nośników kopii

Harmonogram przeglądów i konserwacji urządzeń

L.p.	Określenie urządzenia stanowiącego element systemu informatycznego	Miejsce użytkowania	Opis działań związanych z wykonywanymi czynnościami konserwacji lub przeglądu	Częstotliwość wykonywania przeglądów lub konserwacji	Określenie podmiotu wykonującego przegląd lub konserwację

Rejestr wydanych nośników pamięci

L.p.	Określenie nośnika	Data przyjęcia do użytkowania	Określenie pracownika korzystającego z nośnika	Data udostępnienia nośnika pracownikowi	Data zwrotu nośnika przez pracownika

Załącznik nr 3 do zarządzenia Wójta Gminy Świerzno Nr SK.0050.112.2019

Księga procedur
Wersja dokumentu 1.00 z dnia

ZATWIERDZAM

WÓJT

.....

Radosław Drozdowicz

podpis Wójta

Świerzno 2018

METRYKA

Nazwa jednostki	Urząd Gminy w Świerznie		
Tytuł dokumentu	Księga Procedur		
Opis	W skład dokumentu wchodzą: Księga procedur wraz z załącznikami		
Zastosowanie	Urząd Gminy w Świerznie		
Plik	Księga procedur		
Status	Dokument zatwierdzony, obowiązujący do stosowania od ...21. 11. ..... 2018 r.	Liczba stron	16

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	15.08.2018	utworzenie	wszystkie	Krzysztof Rychel	

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

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Procedura realizacji obowiązku informacyjnego.

Prawo do wiedzy o tym, co się dzieje z danymi osobowymi jest jednym z podstawowych praw właściciela danych osobowych. Obowiązek informowania właściciela danych osobowych występuje w czterech podstawowych sytuacjach:

a) jeżeli dane są zbierane bezpośrednio od osoby (art. 13 RODO);
b) gdy dane osobowe są zbierane z innego źródła niż właściciel danych (art. 14 RODO);
c) zmieniając cel przetwarzania lub dodając nowy (art. 13 ust. 3 i art. 14 ust. 4 RODO);
d) w wykonaniu żądania dostępu do danych.

Wszystkie ww. sytuacje mogą wystąpić w następujących okolicznościach:

a) wpływ pisma do jednostki,
b) przekazanie pisma, sprawy przez inną komórkę w ramach jednostki,
c) bezpośrednia wizyta petenta w jednostce i rozpoczęcie sprawy na jego wniosek,
d) rozpoczęcie procedowania sprawy „z urzędu".

Postępowanie:

1. Rozpoczęcie przetwarzania danych osobowych może być efektem sytuacji wymienionych w pkt. od a) do d).

2. W momencie bezpośredniej wizyty petenta i zainicjowania sprawy, istnieje możliwość natychmiastowego spełnienia obowiązku informacyjnego lub w przypadku, kiedy nie jesteśmy do tego przygotowani ustalenia z nim sposobu jego spełnienia w najbliższej przyszłości.

3. W przypadku innym niż bezpośrednia wizyta petenta należy ustalić, czy wobec niego został spełniony obowiązek informacyjny np. przez stanowisko merytoryczne przekazujące nam jego sprawę. Uwaga! Za stanowisko merytoryczne nie uważa się stanowiska odpowiadającego za obsługę procesu przyjmowania korespondencji w jednostce (kancelaria, biuro podawcze, sekretariat). Za pierwsze stanowisko merytoryczne zobowiązane do spełnienia obowiązku informacyjnego uznaje się stanowisko wszczynające postępowanie w sprawie, niezależnie od sposobu jej realizacji. Jeżeli przedmiotowy obowiązek informacyjny został spełniony przez stanowisko rozpoczynające procedowanie sprawy, a my jedynie ją kontynuujemy, jedynym obowiązkiem jest zweryfikowanie czy czynność przetwarzania danych osobowych w związku z rozpoczętymi działaniami znajduje swoje odzwierciedlenie w *Rejestrze czynności przetwarzania danych osobowych* lub w *Rejestrze kategorii czynności przetwarzania,* które są przypisane do naszego stanowiska.

4. Jeżeli obowiązek informacyjny wobec petenta nie został spełniony przez stanowisko wcześniej procedujące w tej sprawie lub nasze stanowisko jest rozpoczynającym załatwianie sprawy, należy zweryfikować, czy czynności przetwarzania związane z podejmowanymi działaniami są ujęte w rejestrach, o których mowa w pkt. 3, przypisanych do naszego stanowiska. Jeżeli czynności przetwarzania danych osobowych, jakie będą realizowane przy procedowaniu sprawy, nie zostały ujęte w rejestrach, o których mowa w pkt. 3, to w pierwszej kolejności należy uzupełnić zapisy stosownego rejestru o nowo zdefiniowane czynności przetwarzania danych, w szczególności definiując wobec nich: cel przetwarzania, podstawę prawną przetwarzania, okres przechowywania dokumentacji, wykaz odbiorców danych, a następnie uzupełnić właściwy rejestr o zdefiniowane

informacje. Szczegółowe elementy przedmiotowego rejestru określa załącznik nr 2 do *Polityki ochrony danych osobowych*.

5. Jeżeli czynności przetwarzania danych osobowych, jakie będą realizowane w związku z procedowaniem sprawy są ujęte w jednym z dwóch rejestrów, o których mowa w pkt. 3, to na podstawie zawartych w nich zapisów można przystąpić do przygotowania klauzuli informacyjnej, w wariancie uzależnionym od osoby przekazującej dane. W przypadku, kiedy procedowanie sprawy jest wynikiem inicjatywy osoby przekazującej dane stosowany jest wzór klauzuli informacyjnej z art. 13 RODO, natomiast jeżeli inicjatorem procedowania sprawy nie jest petent, lecz inny podmiot, zastosowanie ma wzór klauzuli informacyjnej z art. 14 RODO. Uwaga w przypadku, kiedy petent w związku ze sprawą wskazuje inne strony postępowania lub na skutek procedowania sprawy, sami ujawnimy strony postępowania, to wobec tak ujawnionych osób fizycznych, będących stronami postępowania, również istnieje konieczność spełnienia obowiązku informacyjnego przy zastosowaniu wzoru klauzuli informacyjnej z art. 14. Wzory wymienionych klauzul informacyjnych z art. 13 oraz art. 14 stanowią załącznik nr 4 do *Polityki ochrony danych osobowych*.

6. Kolejny krokiem postępowania jest ustalenie czy osoba, wobec której istnieje obowiązek informacyjny (wynikający z art.13 bądź 14 RODO), będzie w związku z procedowaną sprawą miała z nami kontakt osobisty, czy też nie. W przypadku założenia, że będzie istniała możliwość kontaktu osobistego (petent w związku ze sprawą pojawi się w jednostce), obowiązek informacyjny może zostać spełniony w dowolnej formie w trakcie wizyty petenta w związku ze sprawą. W przypadku, kiedy nie ma takiej konieczności lub przewidujemy, że petent nie pojawi się w związku z procedowaną sprawą, obowiązek informacyjny realizujemy w formie załączenia odpowiedniej klauzuli informacyjnej do pierwszej korespondencji skierowanej do petenta. Uwaga niezależnie od przewidywań czas, jaki ustala się na spełnienie obowiązku informacyjnego wynosi 30 dni kalendarzowych liczonych od daty rozpoczęcia procesu załatwiania sprawy (wpływu, złożenia wniosku, podania, prośby). Jeżeli więc przewidywany pierwszy kontakt z petentem wystąpi po upływie wskazanego 30 dniowego okresu, jesteśmy zobowiązani do przyjęcia innej formy spełnienia obowiązku informacyjnego np. załączając klauzulę informacyjną do pierwszej korespondencji prowadzonej z petentem.

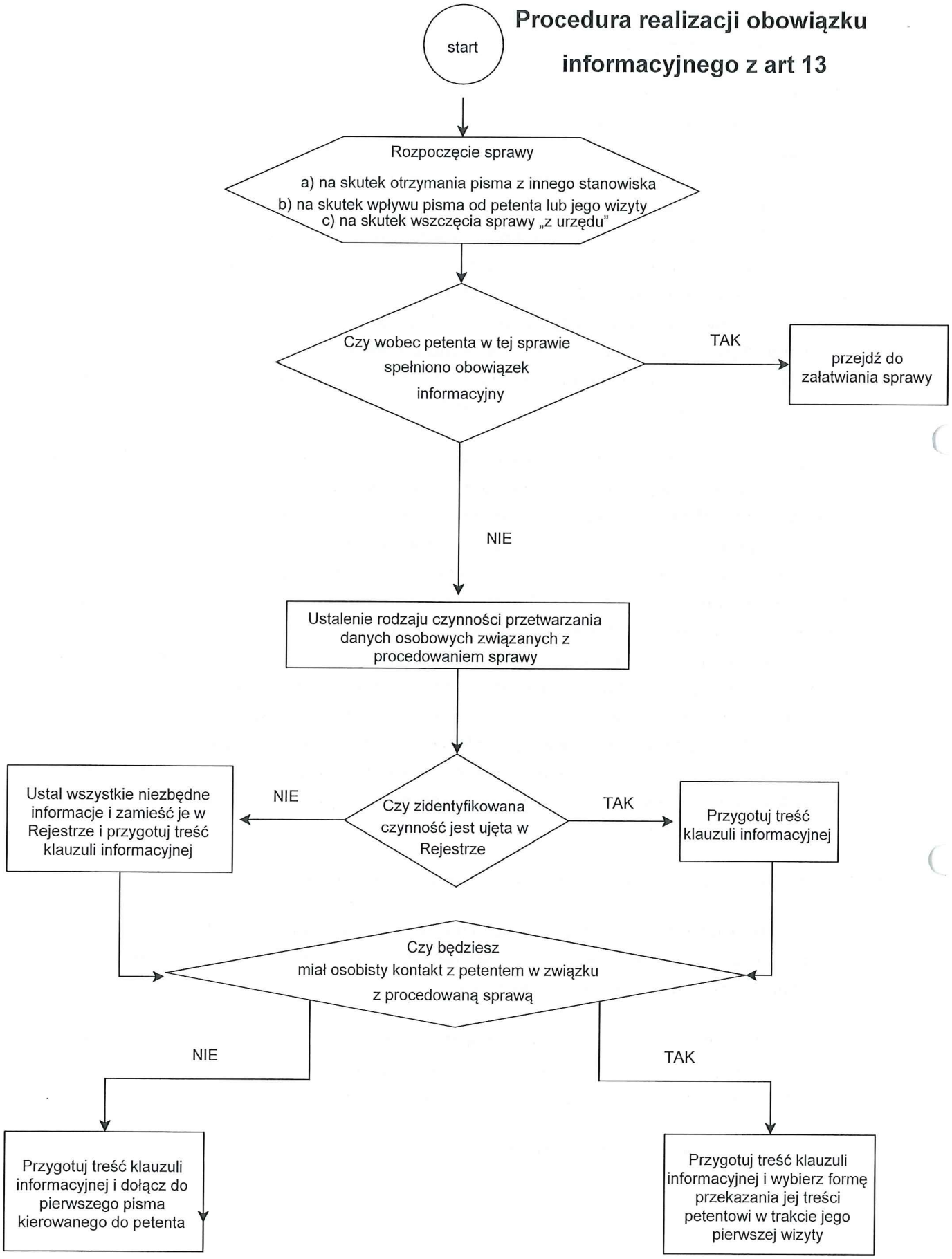
7. Powyższa procedura nie ma zastosowania w następujących sytuacjach:

   a) jeżeli treść klauzuli informacyjnej stanowi integralną część umowy, wniosku, pisma wg wzoru opracowanego przez jednostkę, czy też decyzji, która zostanie wydana przed upływem 30 dniowego okresu, o którym mowa w pkt. 6,

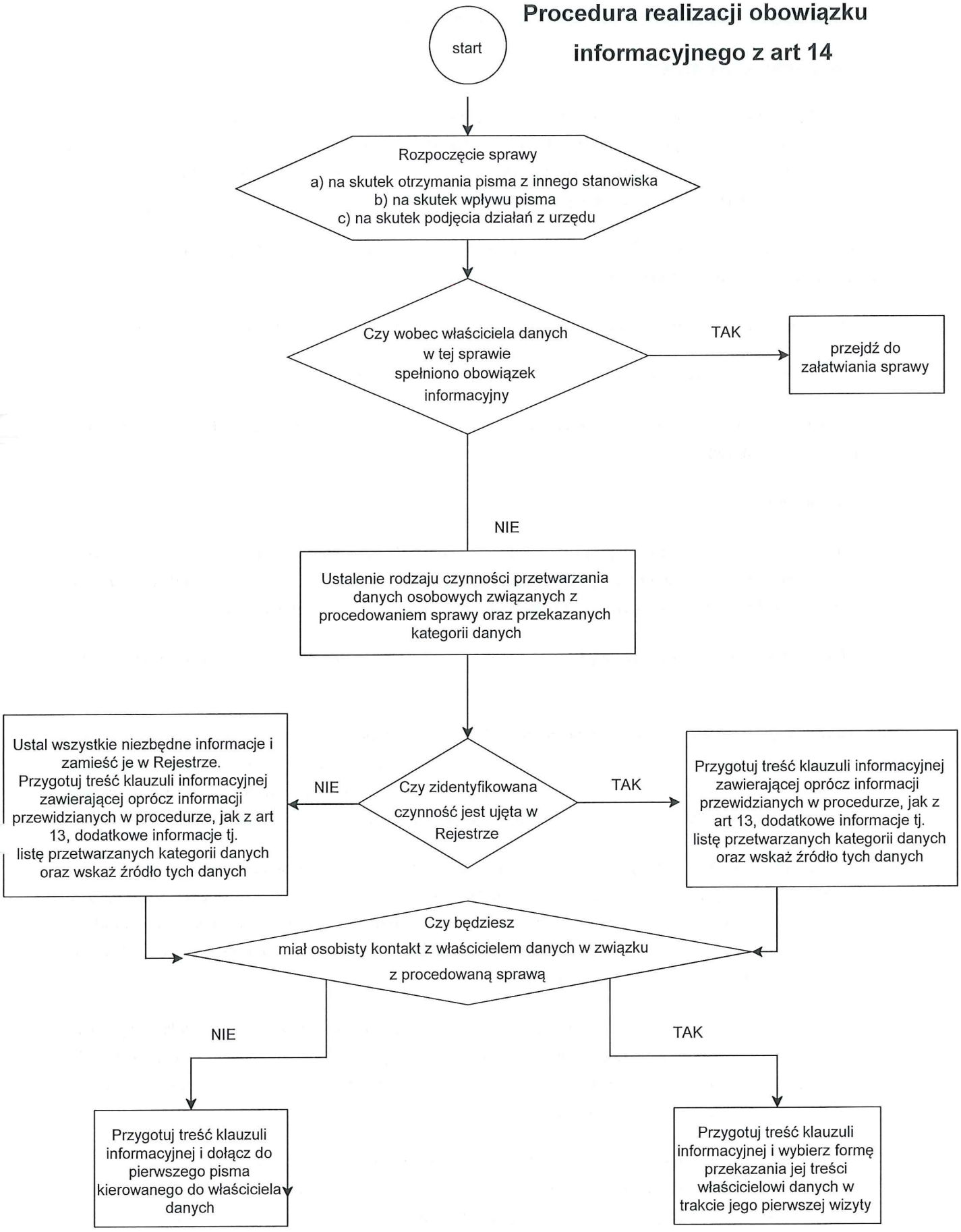
   b) jeżeli dane osobowe są przetwarzane w oparciu o zgodę ich właściciela, stanowiącą **załącznik nr 1** do niniejszego dokumentu, która zawiera w swojej treści wszystkie elementy niezbędnych informacji dla właściciela danych osobowych określone w art. 13 RODO.

Przebieg procesów spełnienia obowiązku informacyjnego w formie graficznej zaprezentowano poniżej.

Procedura realizacji obowiązku informacyjnego z art 13



Procedura realizacji obowiązku informacyjnego z art 14



2. Procedura nadawania i odbierania uprawnień

2.1 Nadanie upoważnienia

Od każdej osoby zatrudnionej w jednostce, niezależnie od formy zatrudnienia, przed przystąpieniem do realizacji czynności przetwarzania danych osobowych wymagane jest posiadanie właściwego upoważnienia, umocowującego tą osobę do ich przetwarzania w sposób zgodny z zasadami określonymi w RODO i *Polityce ochrony danych osobowych*.

Obowiązek nadania właściwych uprawnień (upoważnienia) do przetwarzania danych osobowych może wystąpić w następujących sytuacjach:

a) zatrudnienie przez jednostkę nowej osoby w oparciu o umowę o pracę lub umowę cywilną,

b) zmiana miejsca zatrudnienia (komórki), niezależnie od przyczyny zmiany,

c) zmiana zakresu powierzonych obowiązków niezależnie od przyczyny zmiany (np. zastępowanie innych pracowników)

Postępowanie:

1. Upoważnienie jest wydawane przez administratora danych osobowych (ADO) lub osobę przez niego upoważnionej do nadawania upoważnień. Funkcję ADO definiuje i wskazuje *Polityka ochrony danych osobowych*, która również w załączniku nr 5 określa wzór upoważnienia.

2. Upoważnienie jest sporządzane przez ADO, osobę przez niego upoważnioną, bądź pracownika ds. kadr.

3. W przypadku przygotowania upoważnienia należy kierować się tzw. „zasadą wiedzy koniecznej", co oznacza, że pracownik może zostać upoważniony do czynności przetwarzania danych osobowych w zakresie wynikającym z powierzonego indywidualnego zakresu czynności, który to winien również zawierać czynności wynikające z przyjętego w jednostce systemu zastępstw.

4. Pierwszym krokiem w przygotowaniu upoważnienia jest konfrontacja czynności przetwarzania danych osobowych, jakie będą przedmiotem upoważnienia z zakresem obowiązków osoby upoważnianej oraz zweryfikowanie czy czynności z zakresu powierzonych obowiązków znajdują odzwierciedlenie w *Rejestrze czynności przetwarzania danych osobowych* prowadzonym w jednostce/komórce/na stanowisku pracy.

5. Na jednym formularzu można nadać upoważnienie (w zależności od potrzeb), do kilku czynności przetwarzania danych osobowych, określając je w treści upoważnienia nazwą pod jaką występują w rejestrze, o którym mowa w pkt. 4 lub w przypadku większej ich liczby numerami, za którymi występują w przedmiotowym rejestrze.

6. Wypełnione upoważnienie zatwierdza ADO lub osoba przez niego upoważniona. Ze względu na możliwość nieobecności spowodowanej urlopem, chorobą, za zasadne należy uznać rekomendowanie rozwiązania, polegającego na pisemnym umocowaniu odpowiedniej w hierarchii stanowisk, osoby do czynności związanych z wydawaniem i ewidencjonowaniem upoważnień.

7. Po zatwierdzeniu przez ADO lub umocowaną przez niego osobę upoważnienia, formularz należy przekazać osobie pełniącej funkcję administratora systemu informatycznego (ASI). Funkcję ASI definiuje *Polityka ochrony danych osobowych*.

8. Zadaniem ASI jest weryfikacja czynności przetwarzania danych osobowych dla realizacji, których będzie wykorzystywany określony system informatyczny. W przypadku pojawienia się sytuacji związanej z koniecznością wykorzystania określonych systemów informatycznych, ASI dla każdego z nich, określa indywidualny i niepowtarzalny login dla upoważnionego.

9. ASI po nadaniu loginu/loginów, dokonuje jego/ich zapisu w treści upoważnienia oraz instruuje użytkownika odnośnie pierwszego uruchomienia systemu/systemów i zasad ich funkcjonowania, a następnie dokonuje właściwej konfiguracji jednostki komputerowej przypisanej do stanowiska pracy upoważnionego, w sposób zgodny z zasadami określonymi w *Polityce ochrony danych osobowych.* ASI dokonuje zapisów przydzielonych loginów w prowadzonym rejestrze stanowiącym załącznik nr 1 do *Instrukcji zarządzania systemem informatycznym*.

10. Użytkownik po zapoznaniu się z przyjętą w jednostce dokumentacją określającą zasady funkcjonowania obszaru danych osobowych oraz treścią pouczenia zawartego w upoważnieniu, składa swój podpis pod treścią zamieszczonego w nim oświadczenia i przekazuje dokument ADO oraz archiwizuje jego kopię na swoim stanowisku pracy.

11. Okres archiwizacji wydanych upoważnień jest określony okresem realizacji czynności przetwarzania danych osobowych, będących przedmiotem upoważnienia, powiększonym o okres kolejnych 5 lat po okresie zakończenia określonych czynności przetwarzania na stanowisku pracy.

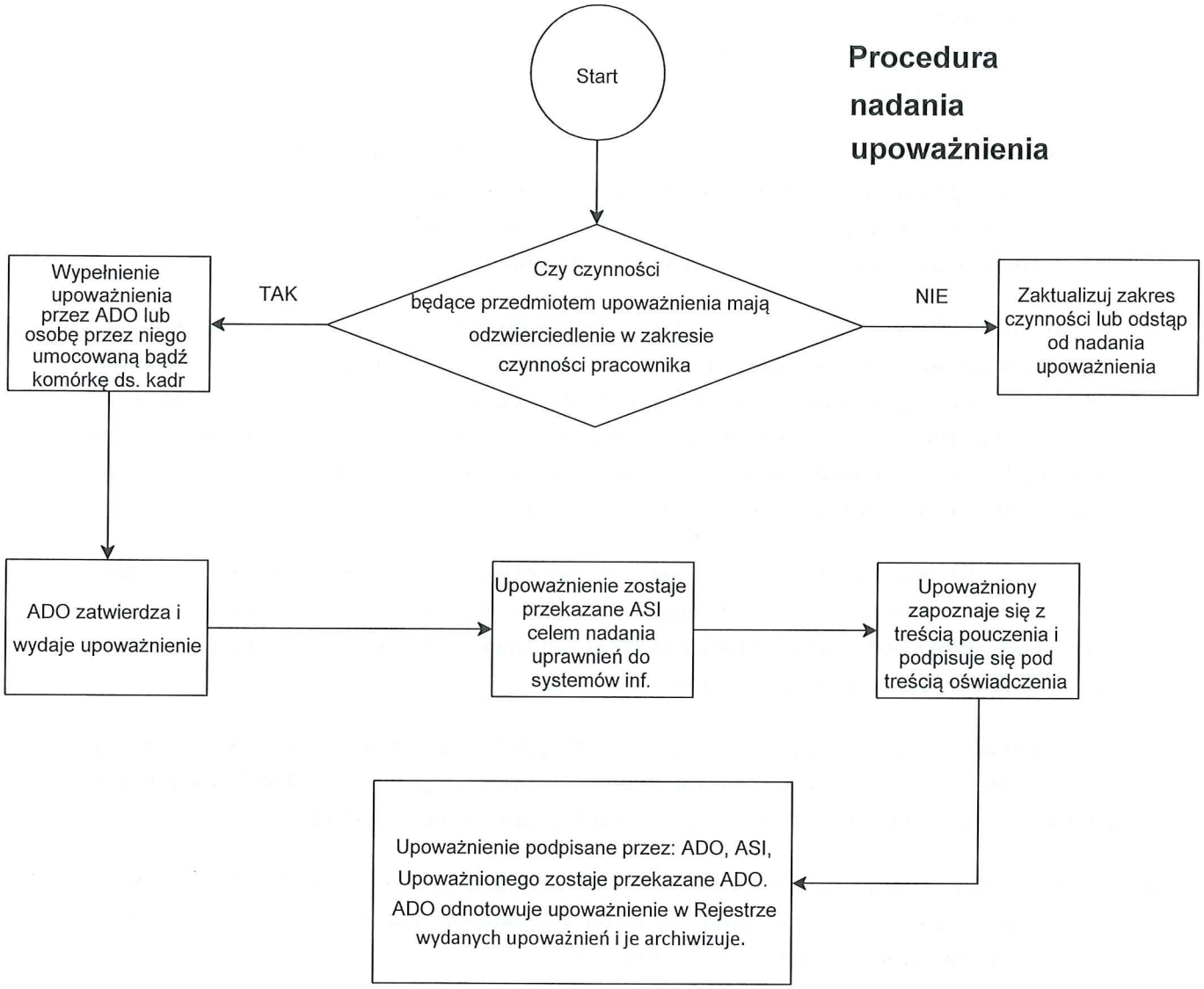
12. Jeżeli upoważnienie jest wydane dla kilku rodzajów czynności przetwarzania danych osobowych, okres 5 lat liczony jest od momentu zaprzestania realizowania ostatniego rodzaju czynności wymienionych we wniosku o nadanie upoważnienia.

13. Każdorazowa zmiana polegająca na dodaniu dodatkowych uprawnień użytkownikowi związanych z przetwarzaniem danych osobowych, wymaga powtórzenia całej procedury.

14. Ostatnim etapem jest odnotowanie wydanego upoważnienia w *Rejestrze wydanych i odwołanych upoważnień*, o którym mowa w Polityce ochrony danych osobowych.

Poniżej zaprezentowano schemat procesu nadawania upoważnienia.

Procedura nadania upoważnienia



2.2 Odebranie upoważnienia

Wydane upoważnienie do czynności przetwarzania danych osobowych może zostać odebrane w każdej chwili. Odebranie upoważnienia do przetwarzania danych osobowych mieści się wyłącznie w zakresie kompetencji kierownika jednostki. Odwołanie wydanego upoważnienia do przetwarzania danych osobowych może zaistnieć w następujących okolicznościach:

a) braku potrzeby dalszego wykonywania określonych czynności przetwarzania danych osobowych np.: na skutek zmiany zakresu czynności, zmiany stanowiska itp.,

b) wygaśnięcia bądź rozwiązania stosunku pracy przez pracownika,

c) wygaśnięcia lub zakończenia realizacji zawartej umowy cywilnej,

d) uzasadnione podejrzenie wobec osoby upoważnionej o braku zachowania należytej staranności przy procesie przetwarzania danych osobowych wynikającej z zasad określonych w *Polityce ochrony danych osobowych.*

Postępowanie:
1. Każda sytuacja zidentyfikowana jako spełniająca przesłanki wymienione w pkt. od a) do d) stanowi bezpośrednią implikację do podjęcia działań związanych z odebraniem nadanego wcześniej upoważnienia.

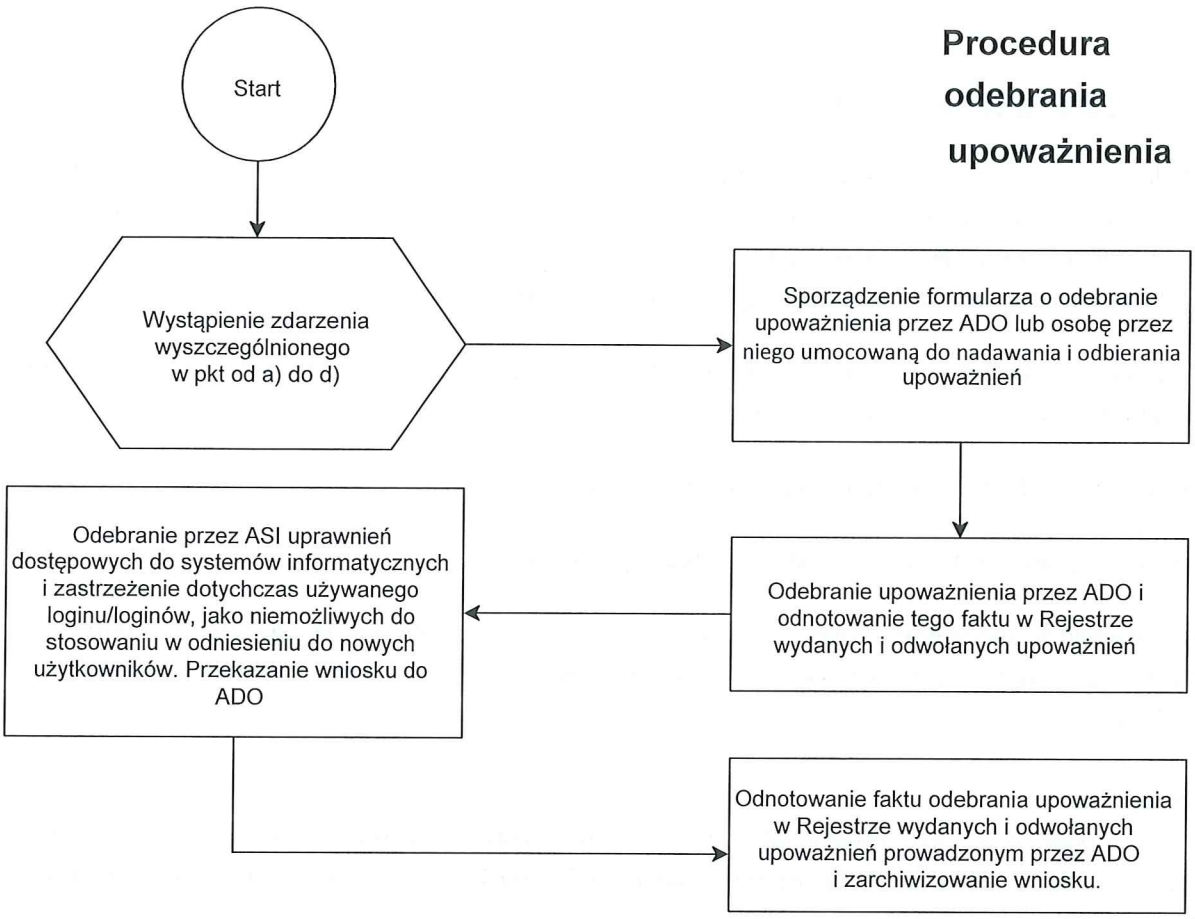
2. Kierownik jednostki jako osoba sprawująca nadzór nad upoważnionym pracownikiem, przygotowuje formularz odebrania nadanego upoważnienia wg załącznika nr 6 do *Polityki ochrony danych osobowych.*

3. ADO lub osoba przez niego umocowana, dokonuje czynności odebrania upoważnienia odnotowując ten fakt w *Rejestrze wydanych i odwołanych upoważnień*. ADO z racji zajmowanego stanowiska samodzielnie podejmuje inicjatywę odebrania upoważnienia.

4. Następnie formularz odwołania upoważnienia trafia do ASI, a ten w stosunku do użytkownika, któremu odbierane są określone upoważnienia, odbiera prawa dostępowe do właściwych systemów informatycznych. Należy podkreślić, że wcześniej przypisany użytkownikowi login, który w momencie cofnięcia posiadanych uprawnień dostępowych przestaje być aktywny, nie może nigdy w przyszłości zostać nadany kolejnemu, nowemu użytkownikowi.

5. Po zakończeniu procedury przez ASI, potwierdzone przez niego odwołanie upoważnienia trafia do ADO celem jego archiwizacji i odnotowania faktu odebrania upoważnienia w *Rejestrze wydanych i odwołanych upoważnień.*

Poniżej zaprezentowano schemat postępowania przy realizacji wniosku o odebranie upoważnienia.



3. Procedura reakcji na ujawnione naruszenie

Zgodnie z przyjętą w Polityce ochrony danych osobowych definicją, przez naruszenie ochrony danych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

a) zniszczenia (utrata atrybutu dostępności),

b) utracenia (utrata atrybutu dostępności i integralności),

c) zmodyfikowania (utrata atrybutu integralności),

d) nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (utrata atrybutu poufności).

Postępowanie:

W przypadku wystąpienia jakiegokolwiek zdarzenia, zjawiska, które będzie charakteryzowało się znamionami określonymi w pkt od a) do d), należy wszcząć procedurę reakcji na ujawnione naruszenie.

1. Ujawnienia naruszenia przetwarzania danych osobowych może dokonać każdy, niezależnie od faktu, czy jest pracownikiem, klientem jednostki lub w żaden sposób nie musi być powiązany z jednostką. Ujawnienie naruszenia mogą również dokonać media.

2. Za moment ujawnienia naruszenia uważa się czas, w którym ktokolwiek z wymienionych tj. pracownik administratora, administrator, inspektor ochrony danych powziął informacje o wystąpieniu naruszenia lub informacja taka został opublikowana w mediach. Nie ma znaczenia sposób powzięcia informacji np. zgłoszenie mailowo, telefonicznie, osobiste stwierdzenie naruszenia, komunikat prasowy itd.

3. Należy pamiętać, iż od momentu powzięcia informacji o naruszeniu w terminie 72 h, należy powiadomić organ nadzorczy o jego wystąpieniu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.

4. Ktokolwiek będąc pracownikiem jednostki powziąwszy informacje o naruszeniu ochrony danych osobowych, winien dokonać natychmiastowej oceny, czy swoim działaniem może ograniczyć naruszenie lub je powstrzymać (np. zdejmując z tablicy ogłoszeń zamieszczony wykaz zawierający dane osobowe, wyłączając jednostkę komputerową, na której doszło do nieupoważnionego dostępu do danych, odebrania dokumentacji zawierającej dane osobowe od osób, które przypadkowo weszły w jej posiadanie - znalazły itp. działania).

5. W przypadku braku możliwości ograniczenia lub powstrzymania naruszenia osoba, która powzięła o tym fakcie wiedzę, jest zobowiązana do powiadomienia administratora danych osobowych oraz inspektora ochrony danych.

6. Administrator wspólnie z IOD, wykorzystując wszelkie dostępne im środki, podejmują działania mające na celu wyeliminowanie zjawiska naruszenia lub jego maksymalne ograniczenie.

7. IOD dokonuje ustaleń mających na celu:

- zidentyfikowanie przyczyny naruszenia,

- określenie kategorii i liczby osób, których prawa i wolności mogą ucierpieć w efekcie naruszenia,

- oszacowanie możliwych do zastosowania środków w celu zminimalizowania negatywnych skutków naruszenia w stosunku do właścicieli danych osobowych.

Z dokonanych ustaleń IOD sporządza protokół i przedkłada go do zatwierdzenia administratorowi.

8. Administrator wspólnie z IOD dokonują analizy ryzyka stopnia naruszenia praw i wolności właścicieli danych osobowych w stosunku, do których doszło do naruszenia danych.

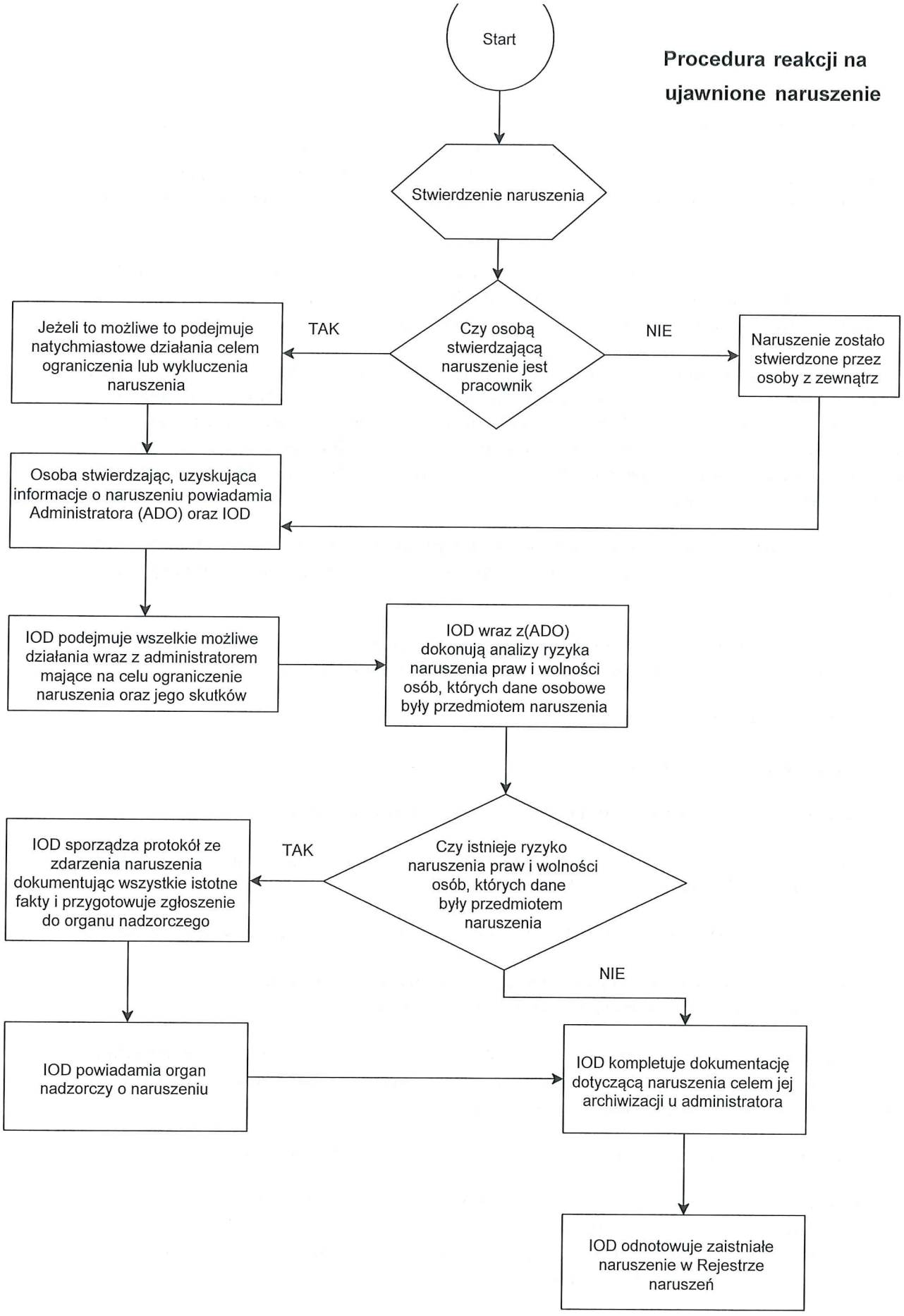
9. Na podstawie wyników przeprowadzonej analizy, o której mowa w pkt. 8 administrator w porozumieniu z IOD podejmuje decyzję o zgłoszeniu naruszenia organowi nadzorczemu lub braku wystarczających przesłanek do jego powiadamiania o naruszeniu.

10. Jeżeli istnieje taka konieczność IOD powiadamia organ nadzorczy o wystąpieniu naruszenia.

11. W przypadku, jeżeli naruszenie ma wpływ na prawa i wolności osób fizycznych należy podjąć działania związane z poinformowaniem tych osób o wystąpieniu naruszenia w stosunku do dotyczących ich danych osobowych i w razie konieczności poinformować o działaniach, które mogą podjąć, by chronić się przed konsekwencjami naruszenia.

12. IOD kompletuje dokumentację dotyczącą naruszenia i zgłoszenia do organu nadzorczego oraz odnotowuje jego wystąpienie w *Rejestrze naruszeń* stanowiącym załącznik nr 2 do niniejszego dokumentu.

Procedura reakcji na ujawnione naruszenie



4. Procedura udostępniania danych osobowych

Możliwe jest ujawnienie danych osobowych (udostępnienie), bez jakiejkolwiek umowy powierzenia danych do dalszego przetwarzania kategorii odbiorców tj.: organom publicznym, które mogą wykorzystywać dane wyłącznie dla potrzeb sprawowanych funkcji publicznych i są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym, zgodnie z obowiązującym prawem. Ponieważ prawo do ochrony danych osobowych nie jest prawem bezwzględnym, przetwarzane dane możemy ujawnić (udostępnić) następującym organom:

a) podatkowym,
b) celnym,
c) policji, prokuraturze, sądom,
d) Straży Granicznej,
e) CBA, CBŚ, ABW

Żądanie ujawnienia danych osobowych, z którymi występują takie organy publiczne, powinno mieć zawsze formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych.

Postępowanie:

1. Jeżeli do jednostki wpłynie wniosek o ujawnienie „udostępnienie" danych osobowych w odniesieniu do osoby / osób, które zostały w jakiś sposób we wniosku określone z jednoczesnym wskazaniem kategorii danych mających być przedmiotem ujawnienia i wniosek ten złoży organ zawarty w katalogu od lit. a) do lit. e), to jednostka jest zobowiązana do ujawnienia danych będących przedmiotem wniosku.

2. Co do zasady wniosek taki winien mieć formę pisemną i wskazywać precyzyjnie organ żądający ujawnienia oraz podstawę prawną, sankcjonującą takie żądanie. Dopuszcza się sytuacje związane z ujawnieniem danych osobowych w związku z ustnym żądaniem funkcjonariusza publicznego, zatrudnionego przez organ w przypadku stanu wyższej konieczności (np. pościg za przestępcą, ratowanie życia ludzkiego lub mienia).

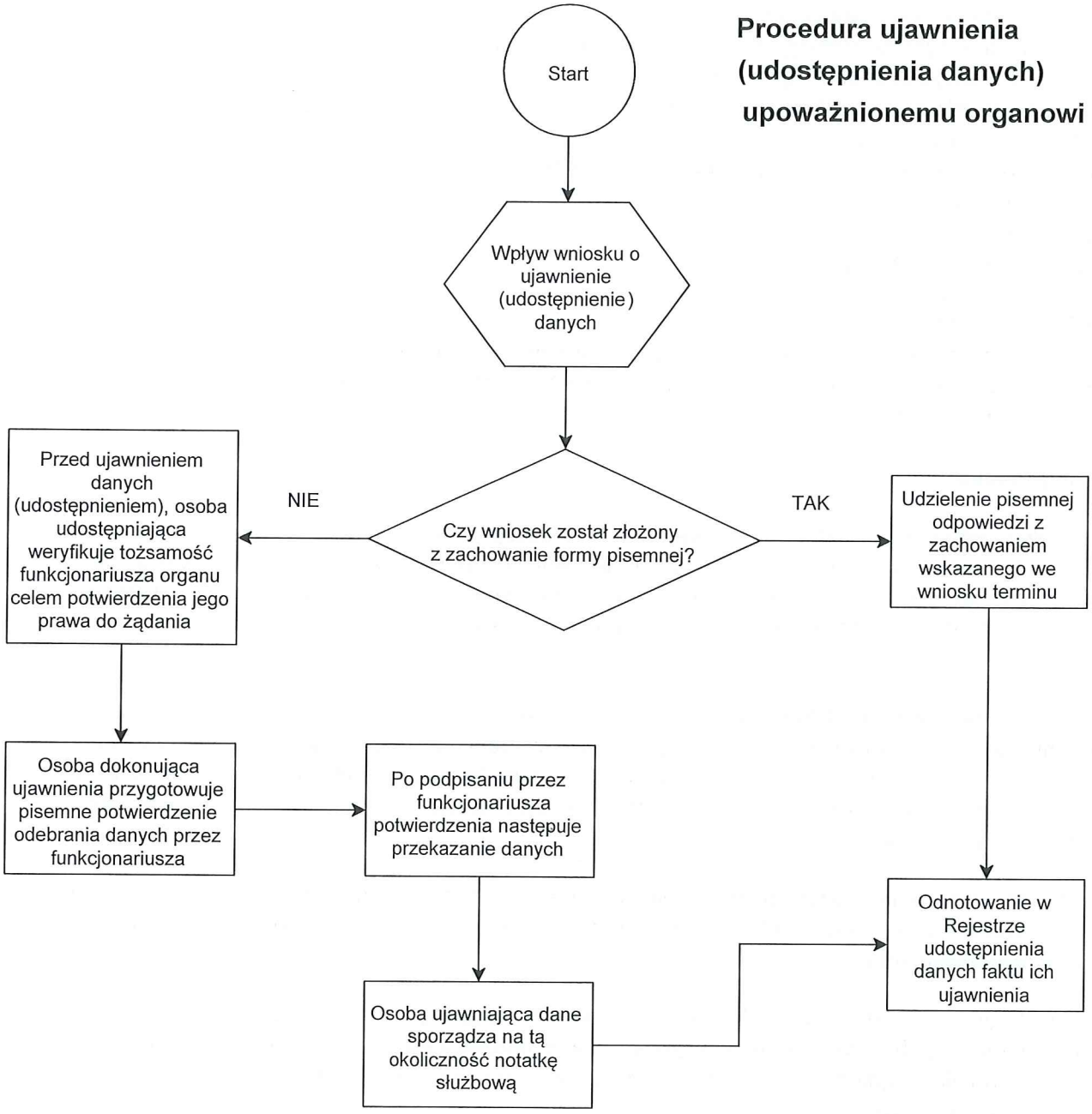
3. Każde ujawnienie (udostępnienie) danych, musi zostać zaewidencjonowane w *Rejestrze udostępnienia danych osobowych* prowadzonym przez ADO. Wzór rejestru stanowi załącznik nr 3 do niniejszego dokumentu.

4. W przypadku ujawnienia (udostępnienia) danych osobowych, na skutek ustnego żądania funkcjonariusza publicznego zatrudnionego w organie, których katalog został określony we wstępie, osoba ujawniająca żąda pisemnego potwierdzenia przekazania danych od funkcjonariusza, któremu dane są przekazywane.

5. Potwierdzenie powinno zawierać następujące informacje:
- miejsce i datę ujawnienia (udostępnienia) danych osobowych,
- precyzyjne określenie organu wraz ze wskazaniem jego siedziby,
- imię i nazwisko oraz stopień funkcjonariusza lub inne dane zawarte w posiadanej przez niego legitymacji służbowej, umożliwiające jego jednoznaczną identyfikację,
- określenie kategorii osób, których dane były przedmiotem ujawnienia, wraz ze wskazaniem kategorii ujawnionych danych.

6. W przypadku ujawnienia (udostępnienia) danych na ustne żądanie funkcjonariusza uprawnionego organu, osoba dokonująca ujawnienia (udostępnienia), sporządza notatkę służbową opisującą przebieg zdarzenia.

Procedura ujawnienia (udostępnienia danych) upoważnionemu organowi



Załączniki:

Załącznik nr 1 – Wzór zgody na przetwarzanie danych osobowych

Załącznik nr 2 – Rejestr naruszeń

Załącznik nr 3 – Rejestr udostępnienia danych osobowych

Zgoda na przetwarzanie danych osobowych

Ja ..... niżej podpisana/y,
(imię i nazwisko upoważniającego)

wyrażam wyraźną i dobrowolną zgodę na przetwarzanie przez Urząd Gminy w Świerznie nw. kategorii moich danych osobowych/oraz mojego dziecka* tj. .....
(imię i nazwisko dziecka)

1. .....
(kategoria danych)

2. .....
(kategoria danych)

3. .....
(kategoria danych)

w zakresie niezbędnym dla realizacji nw. celu/celów*. Jednocześnie oświadczam, że zapytanie o zgodę zostało mi przedstawione w wyraźnej i zrozumiałej dla mnie formie i zrozumiałam (em) treść udzielonej mi informacji odnoszącej się do przetwarzania moich/dziecka* danych osobowych.

1. .....

.....

Data i czytelny podpis osoby wyrażającej zgodę

2. .....

.....

Data i czytelny podpis osoby wyrażającej zgodę

3. .....

.....

Data i czytelny podpis osoby wyrażającej zgodę

Uwaga! *Przetwarzanie danych dla różnych celów wymaga odrębnej zgody dla każdego z celów. W przypadku jednoczesnego pozyskiwania danych dla różnych celów, wszystkie cele przetwarzania należy określić w informacji dla osoby wyrażającej zgodę.*

**niepotrzebne skreślić*

Informacja dla osoby wyrażającej zgodę

Administratorem danych osobowych jest:

Urząd Gminy Świerzno z siedzibą: Świerzno 13, 72-405 Świerzno. Z administratorem danych można się skontaktować poprzez adres e-mail: ug@swierzno.pl lub telefonicznie pod numerem 91 383 27 93 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.

Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iodo_swierzno@wp.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 dla celów:.....

.....

Podane dane są przetwarzane na podstawie art.6 ust. 1 lit. a *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 „RODO")*, (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), czyli Pani/Pana* zgody

Odbiorcy danych osobowych.

Odbiorcami danych osobowych będą: .....

.....

jednostki administracji publicznej uprawnione do sprawowania kontroli i nadzoru nad prawidłowością funkcjonowania administratora oraz jednostki i organy administracji publicznej mogące potwierdzić prawdziwość podanych przez Panią/Pana* informacji.

Okres przechowywania danych.

Dane będą przechowywane przez okres ..... lat poczynając od 1 stycznia roku następnego po roku, w którym nastąpiło wyrażenie zgody.

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 wycofania zgody
f) 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 Panią/Pana* danych jest dobrowolne, jednakże odmowa ich podania uniemożliwi .....

niepotrzebne skreślić

Rejestr naruszeń danych osobowych

Lp.	Opis naruszenia ze wskazaniem daty powstania i jego ujawnienia	Przyczyny naruszenia	Przebieg naruszenia	Kategorie osób oraz kategorie danych będące przedmiotem naruszenia	Zgłoszono / nie zgłoszono do UODO naruszenia. Powody niezgłoszenia

Rejestr udostępnienia danych osobowych

Lp.	Wskazanie daty udostępnienia oraz organu, któremu dane zostały udostępnione	Forma żądania udostępnienia pisemny wniosek/ustne żądanie	Wskazanie osoby udostępniającej oraz osoby odbierającej dane osobowe	Kategorie osób których dane były przedmiotem udostępnienia	Kategorie udostępnionych danych osobowych