Burmistrz Miasta Świeradów-Zdrój
ul. 11 Listopada 35
59-850 Świeradów-Zdrój

Zarządzenie Nr 14/2020
Burmistrza Miasta Świeradów-Zdrój
z dnia 19 lutego 2020 roku

w sprawie wprowadzenia polityki ochrony danych osobowych w Urzędzie Miasta Świeradów-Zdrój

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE.L.2016.119.1) zarządza się co następuje:

§ 1

Wdraża się w Urzędzie Miasta Świeradów-Zdrój politykę ochrony danych osobowych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2

Zobowiązuje się pracowników Urzędu Miasta Świeradów-Zdrój do stosowania zasad określonych w polityce ochrony danych osobowych.

§3

Tracą moc Zarządzenie Nr 70/18 Burmistrza Miasta Świeradów-Zdrój z dnia 12.06.2018 roku.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Roland Karciniak

LEŚNY & WSPÓLNICY
KANCELARIA PRAWNA

POLITYKA OCHRONY DANYCH OSOBOWYCH

URZĄD MIASTA ŚWIERADÓW-ZDRÓJ, UL. 11 LISTOPADA 35, 59-850 ŚWIERADÓW-ZDRÓJ

00-682 Warszawa, ul. Hoża 86/ 410; 62-200 Gniezno ul. Platanowa nr 15
61-806 Poznań, ul. Święty Marcin 29/8; konto nr 45 1940 1076 3105 0557 0000 0000
KRS 0000 406 825; NIP: 784-248-78-16; Regon: 302 011 576
www.lesny.com.pl; kancelaria@lesny.com.pl

ROZDZIAŁ I
Postanowienia ogólne

§ 1
Wstęp

1. Polityka ochrony danych zwana dalej „Polityką", jest dokumentem określającym środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu, a także ma za zadanie usprawnienie i usystematyzowanie organizacji pracy Administratora.

2. Polityka została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) i ma na celu wykazanie, że przetwarzanie danych odbywa się zgodnie z tym rozporządzeniem.

§ 2
Definicje

Ilekroć w Polityce jest mowa o:

1. **Administratorze Danych/Administratorze** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w ramach niniejszego dokumentu jest to Burmistrz Miasta Świeradów-Zdrój;

2. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 s. 1);

3. **Dane osobowe** – to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej;

4. **Zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony na funkcje;

5. **Przetwarzaniu danych** – rozumie się przez to to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;

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

7. **Kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, decyzji, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierający dane osobowe;

8. **Inspektorze Ochrony Danych Osobowych (IOD)** – to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego;

9. **Administratorze Systemów Informatycznych (ASI)** – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację wyznaczonego przez Administratora Danych;

10. **Użytkowniku** – rozumie się osobę upoważnioną przez Administratora danych Osobowych do przetwarzania danych osobowych w systemie informatycznym oraz w kartotekach;

11. **Pomieszczeniach** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 3

Cele

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenie fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz poprzez użytkowników.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,

   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 4

Sposoby realizacji celów

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1. wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych oraz ich odpowiedzialność za ochronę tych danych;
2. przeszkolenie pracowników w zakresie bezpieczeństwa i ochrony danych osobowych;
3. upoważnienie użytkowników do przetwarzania danych osobowych oraz przypisanie użytkownikom określonych atrybutów umożliwiających wykonywanie ustalonych operacji na różnych poziomach zbiorów danych osobowych – stosowanie do indywidualnego zakresu upoważnienia, zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień,
4. podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń;
5. okresowe sprawdzenie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
6. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;
7. śledzenie osiągnięć w dziedzinie zabezpieczenia systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrożenie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

Naruszenie ochrony danych osobowych

Za naruszenie ochrony danych osobowych uważa się w szczególności:

1. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
2. naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jak błąd w działaniu osoby uprawnionej (np. zmianę zawartości, danych, utratę całości lub części danych),
3. naruszenie lub próby naruszenia integralności systemu,
4. zmianę lub utratę danych zapisanych na kopii zapasowych,
5. naruszenie lub próby naruszenia poufności danych lub ich części,
6. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu)
7. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
8. zniszczenie, uszkodzenie lub wszelkie próby integracji nieuprawnionej w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodny z przeznaczeniem) danych zawartych w systemie informatycznym lub kartotekach,
9. inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,

Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

Analiza ryzyka

Procedura szacowania ryzyka, na którą składają się analiza i ocena ryzyka jest niezbędnym elementem prawidłowego zrealizowania ciążącego na Administratorze obowiązku wdrożenia odpowiednich środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Ogólna analiza ryzyka stanowi załącznik nr 1, do niniejszej polityki.

§ 7

Zapewnienie zgodności z przepisami RODO

Administrator zobowiązany jest do spełnienia obowiązków prawnych wynikających z RODO. Należy przede wszystkim zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas – zasada ograniczonego czasu,
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. opracowano klauzule informacyjne dla powyższych osób,

6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

§ 8

Ocena skutków

Ocena skutków jest formalną, wymaganą w określonych w art. 35 RODO przypadkach procedurą, za wykonanie, której odpowiada Administrator. W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem oraz po wyrażeniu przez niego opinii.

§ 9

Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

§ 10

Szkolenia

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

2. Za przeprowadzenie szkolenia odpowiada Administrator, który może zlecić jego przeprowadzenie Inspektorowi Ochrony Danych lub podmiotowi zewnętrznemu, posiadającemu odpowiednią wiedzę i doświadczenie do jego przeprowadzenia.

3. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (zmiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.

§ 11
Upoważnienia

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.

2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia

5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Wzór ewidencji stanowi załącznik nr 3 do Polityki.

§ 12
Postępowanie upoważnionych użytkowników

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.
2. W tym celu należy:
   1) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,
   2) przestrzegać procedur związanych z otwieranych i zamykaniem pomieszczeń, a także z wejściem do obszarów przestrzegania danych osobowych lub osób nieupoważnionych,
   3) informować Administratora, Inspektora Danych Osobowych lub pracowników ochrony o podejrzanych osobach tj.:
      a) osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;
      b) osobach przebywających w obiekcie bez wyraźnego celu;
      c) osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;
      d) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.

3. Administrator, a także osoby na stanowiskach samodzielnych oraz użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Inspektorowi Danych Osobowych projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 13

Dostęp do pomieszczeń

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności co najmniej jednego użytkownika lub za zgodą Administratora Danych.
3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.

§ 14

Polityka kluczy

1. Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.
2. Klucze wydawane są wyłącznie osobom do tego uprawnionym, prowadzona jest ewidencja odbioru kluczy.
3. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.

§ 15

Stosowane zabezpieczenia mające wpływ na ochronę danych osobowych

Administrator wdraża następujące środki mające na celu zapewnienie ochrony danych osobowych:

1. **Środki organizacyjne:**

   a) opracowano i wdrożono politykę ochrony danych osobowych;

   b) opracowano i wdrożono instrukcję zarządzania systemem informatycznym;

   c) powołano Inspektora Ochrony Danych;

   d) powołano Administratora Systemu Informatycznego;

   e) do przetwarzania danych dopuszczono wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych;

   f) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;

   g) osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych;

   h) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;

   i) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

   j) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco;

   k) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

l) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

m) stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe. Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 4 do Polityki. Administrator prowadzi rejestr umów powierzenia przetwarzania danych osobowych, który stanowi załącznik nr 5 do Polityki;

n) w podmiocie prowadzi się politykę czystego biurka i ekranu;

o) w czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe;

p) klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym;

q) przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

2. **Środki ochrony fizycznej danych:**
   a) zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi, posiadającymi zamykane zamki, chyba, że z przepisów prawa wynika obowiązek stosowania drzwi spełniających dodatkowe wymagania techniczne np. drzwiami o podwyższonej odporności ogniowej >= 30 min, o podwyższonej odporności na włamanie - drzwi klasy C;
   b) zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna jeśli zlokalizowane na parterze zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
   c) pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;
   d) dostęp do budynku, w którym znajdują się pomieszczenia, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony;
   e) co do zasady zbiór danych osobowych w formie papierowej, prowadzony w formie kartoteki jest przechowywany w zamkniętej niemetalowej szafie, do których dostęp mają wyłącznie użytkownicy. W przypadku gdy wymaga tego przepis prawa zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej metalowej szafie, bądź w zamkniętym sejfie lub kasie pancernej;
   f) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętym sejfie lub kasie pancernej;
   g) gdy wymaga tego szczegółowy przepis prawa, zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach;
   h) pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;

i) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. W przypadku kartotek, po upływie okresu ich niezbędnej archiwizacji, wynikającego z instrukcji kancelaryjnej są niszczone przez podmiot zewnętrzny spełniający warunki prawidłowego wykonania usługi.

3. **Opis zabezpieczeń infrastruktury informatycznej, w tym środki w ramach narzędzi programowych i baz danych zawiera instrukcja zarządzania systemami informatycznymi stanowiąca załącznik nr 6, do niniejszej polityki.**

ROZDZIAŁ II

Przetwarzanie danych osobowych

§ 16

Miejsce i zasady przetwarzania danych

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, pomieszczeniach na terenie siedziby Administratora Danych.

2. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych, wyłącznie za zgodą Administratora Danych.

3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe zawiera załącznik nr 7 do Polityki.

4. Przetwarzanie, w tym udostępnianie danych osobowych, jest prawnie dopuszczalne, jeżeli jest to niezbędne dla realizowania uprawnienia lub spełniania obowiązku wynikającego z przepisu prawa.

5. Podmiot występujący o udostępnienie danych osobowych powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żą-

dania ich udostępniania. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne, i czy nie będzie ono stanowić naruszenia zasad ochrony danych osobowych.

6. Przetwarzanie, w tym udostępnianie danych osobowych, w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach naukowych, dydaktycznych, historycznych lub statystycznych.

7. Udostępnienie danych osobowych może nastąpić jedynie za zgodą Administratora Danych lub osoby przez niego upoważnionej.

§ 17

Zabezpieczenie pomieszczeń

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić aby:

1. drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby;

2. budynek był chroniony przez wszystkie dni w roku. Ochronie powinny podlegać wyznaczone pomieszczenia w stopniu adekwatnym do ich przeznaczenia;

3. pomieszczenia, w których znajdują się serwery, były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej;

4. pracownicy Administratora Danych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe;

5. przebywanie użytkowanie po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych;

6. w trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.

§ 18

Inspektor Ochrony Danych Osobowych

1. Inspektor Danych Osobowych nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. W celu sprawnego wykonywania swoich zadań Inspektor Ochrony Danych Osobowych jest uprawniony do wnioskowania do Administratora Danych w celu wyznaczania użytkownikom wykonywania określonych zadań.
3. Użytkownicy zobowiązani są do ścisłej współpracy z Inspektorem Danych Osobowych.

§ 19

Zakres przetwarzanych danych osobowych

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi Załącznik nr 8 do Polityki.
3. Administrator Danych prowadzi:
   - 3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
   - 3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:
   - 4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,

4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,

4.3. imię i nazwisko oraz dane kontaktowe IOD,

4.4. cele przetwarzania,

4.5. opis kategorii osób, których dane dotyczą,

4.6. opis kategorii danych osobowych,

4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:

5.1. nazwę oraz dane kontaktowe Administratora Danych,

5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,

5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,

5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,

5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator Danych prowadzi rejestry, o których mowa w pkt 3 w formie elektronicznej. Wzory rejestrów, o których mowa w pkt 3 stanowią załączniki do polityki.

7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

ROZDZIAŁ IV

Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 20

Kontrola przestrzegania zasad ochrony danych osobowych

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.

2. Inspektor Danych Osobowych sprawuje nadzór nad przestrzeganiem zasad ochrony przetwarzania danych osobowych.

3. W przypadku nieobecności Inspektora Danych Osobowych, osobę zastępującą wyznacza Administrator Danych.

4. Inspektor Danych Osobowych lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.

5. Inspektor Danych Osobowych prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.

6. Z kontroli, o których mowa w ust. 3 należy sporządzić dokument, które przechowuje Administrator Danych.

ROZDZIAŁ V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 21

Czynności poprzedzające przystąpienie do pracy

1. Przed przystąpieniem do pracy użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora oraz Inspektora Ochrony Danych.

3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych.

4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.

§ 22

Czynności podjęte po stwierdzeniu naruszenia

1. Do czasu przybycia Administratora lub Inspektora Ochrony Danych osobowych, zgłaszający:

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

   2) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez umożliwienie dostępu do nich osobom nieupoważnionym,

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

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych.

§ 23

Wstępne czynności po stwierdzeniu naruszenia

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Inspektor Ochrony Danych Osobowych, po przybyciu na miejsce:

1. ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,

2. wysłuchuje relacji osoby, która dokonała powiadomienia,

3. podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia danych osobowych. W uzasadnionych przypadkach niezwłoczne powiadamia Administratora Danych.

§ 24

Raport z przebiegu zdarzenia

1. Inspektor Ochrony Danych Osobowych sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
   1) Dacie i godzinie powiadomienia,
   2) Rodzaj naruszenia,
   3) Obowiązek zawiadomienia osoby, której dane dotyczą,
   4) Okoliczności naruszenia,
   5) Skutki naruszenia,
   6) Podjęte działania zaradcze,
2. Inspektor Ochrony Danych Osobowych sporządzony raport przekazuje do organu nadzorczego.

§ 25

Podjęcie czynności zmierzających likwidację naruszenia

1. Inspektor Ochrony Danych Osobowych podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
   2) relacjonuje Administratorowi Danych przedsięwzięte czynności,
   3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób dopuszczonych do przetwarzania danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Inspektor Danych Osobowych wnioskuje do Administratora Danych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/sprawców.

§ 26

Kontynuacja pracy

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia Inspektora Ochrony Danych Osobowych.

§ 27

Postępowanie w przypadku kradzieży

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Inspektora Ochrony Danych Osobowych, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

2. W sytuacji, o której mowa w ust. 1 Inspektor Ochrony Danych Osobowych podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt oraz powiadamia Administratora Danych.

§ 28

Odpowiedzialność

Osoba dopuszczona do przetwarzania danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki ponosi odpowiedzialność przewidzianą w przepisach aktów wewnętrznych Administratora Danych oraz na podstawie innych, odrębnych przepisów prawa.

§ 29

Zgłoszenie incydentu do UODO i obowiązek prowadzenia rejestru

1. Administrator przy współpracy z Inspektorem Ochrony Danych Osobowych jest zobowiązany zidentyfikować, ocenić i zgłosić naruszenie ochrony danych osobowych do Urzędu Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia.
2. Administrator prowadzi wewnętrzny rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO. Wzór rejestru stanowi załącznik nr 9 do Polityki. Rejestr prowadzony jest w wersji elektronicznej.

ROZDZIAŁ VI

Postępowanie w przypadku klęski żywiołowej

§ 30

Definicja

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 31

Zasady postępowania w przypadku ewakuacji

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 32

Obowiązek informacyjny

1. O zagrożeniu, jego skali i podjętych krokach zaradczych użytkownik zobowiązany jest niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych w każdy możliwy

sposób. w razie niemożności skontaktowania się z nim pracownik zawiadamia, co najmniej jedną z niżej wymienionych osób:

1) osobę wyznaczoną przez Administratora Danych,

2) Administratora Danych.

2. Numery telefonów Inspektora Danych Osobowych i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane użytkownikom.

§ 33

Prawo wejścia do pomieszczeń

Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełnienia obowiązku, o którym mowa w § 13 ust. 2 Polityki.

§ 34

Czynności poprzedzające opuszczenie pomieszczeń

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1) zamknięcia systemu informatycznego,

2) zabezpieczenia danych gromadzonych w kartotekach.

§ 35

Zabezpieczenie danych

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Inspektor Danych Osobowej oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieupoważnionym do nich dostępem.

2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych , obecnych przy akcji ratunkowej.

ROZDZIAŁ VI
Postanowienia końcowe

§ 36
Poufność zapisów polityki

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§ 37
Oświadczenie o dochowaniu poufności

1. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami Rozporządzeniu Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania oraz dochowania poufności.

2. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania oraz dochowania poufności, stanowi załącznik nr 10 do polityki.

3. Oświadczenia przechowywane są w aktach osobowych.

4. Ponadto załącznik do niniejszej polityki stanowi wzór ogólnej klauzuli informacyjna – załącznik nr 11.

§ 38

Odpowiednie stosowanie innych przepisów

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych.

2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w przypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

.....
(podpis Administratora Danych)

ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM ZAGROŻEŃ I RYZYKA

zwana dalej:

ANALIZĄ ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

§ 1

Administrator Danych ze względu na ciążące na nim obowiązki wynikające z ustawy o ochronie danych osobowych, a dokładnie art. 32 rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.) tej ustawy, zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych, w świetle adekwatnych zagrożeń, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 2

W związku z § 1 niniejszego dokumentu Administrator Danych wprowadza dokument „Analiza zagrożeń i ryzyka" w podmiocie o nazwie: **Urząd Miasta Świeradów-Zdrój** w celu badania i obserwowania istniejącego środowiska przetwarzania danych osobowych.

Ilekroć w „Analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych" jest mowa o:

1. **ANALIZIE RYZYKA** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;

2. **SZACOWANIU RYZYKA** – proces oceny i analizy ryzyka;

3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;

4. **POSTĘPOWANIU Z RYZYKIEM** – wdrażanie środków modyfikujących ryzyko;

5. **ZARZĄDZANIU RYZYKIEM** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;

6. **RYZYKU SZCZĄTKOWYM** – ryzyko pozostające po procesie postępowania z ryzykiem;

7. **AKCEPTOWANIU RYZYKA** – decyzja, aby zaakceptować ryzyko;

8. **BEZPIECZEŃSTWIE INFORMACJI** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Ochrony Danych, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;

11. **AKTYWACH** – wszystko, co ma wartość dla organizacji;

12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

13. **DOSTĘPNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;

15. **INFORMATYCZNYM NOŚNIKU DANYCH** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

16. **INTEGRALNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

17. **OPROGRAMOWANIU ZŁOŚLIWYM** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;

18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;

19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;

20. **POUFNOŚCI** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

21. **PRZEKAZYWANIU INFORMACJI** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;

22. **TESTACH BEZPIECZEŃSTWA** — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;

23. **ZABEZPIECZENIU** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;

24. **ZAGROŻENIU** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;

25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

§ 4

Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora Danych systemów ochrony. Analiza zagrożeń i ryzyka, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 5

Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych, wprowadzone przez Administratora Danych określa załącznik nr 1.

§ 6

Możliwe zagrożenia występujące w systemach informatycznych, określa załącznik nr 2.

§ 7

Podatność systemu na zagrożenia, określa załącznik nr 3.

§ 8

Analizę zagrożeń i ryzyka, określa załącznik nr 4.

§ 9

Wnioski i działania naprawcze, określa załącznik nr 5.

§ 10

Wzór klauzuli poufności, określa załącznik nr 6.

§ 11

Przebieg przykładowej kontroli podatności systemu, określa załącznik nr 7.

§ 12

Rekomendacja odpowiedniej postawy upoważnionego do przetwarzania danych osobowych, określa załącznik nr 8.

§ 13

Tabela szacowania ryzyka została określona w załączniku nr 9.

.....

(Podpis Administratora Danych Osobowych)

WYMOGI OGÓLNE BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH, WPROWADZONE PRZEZ ADMINISTRATORA DANYCH W:

Urząd Miasta Świeradów-Zdrój, Administrator Danych Osobowych – Burmistrz Miasta Świeradów-Zdrój

§ 1

W czasie przetwarzania danych osobowych informacje mogą występować w postaci:

1. plików lub informacji przechowywanych na dysku twardym komputera;
2. plików lub informacji zapisanych na nośnikach komputerowych;
3. wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

§ 2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:

1. zapewnienia ochrony fizycznej pomieszczeń, stanowiska, jak i infrastruktury komputerowej przed nieuprawnionym dostępem;
2. ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
4. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
5. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
6. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

.....

(Podpis Administratora Danych Osobowych)

ZAGROŻENIA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

§ 1

W myśl ustawy o ochronie danych osobowych, każdy Administrator Danych Osobowych powinien zapewnić takie warunki pracy w systemie, aby cechował się on poufnością, integralnością i rozliczalnością.

§ 2

Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone Administratorowi Danych Osobowych bądź wyznaczonemu Inspektorowi Ochrony Danych.

§ 3

1. Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.
2. Zapewnienie poufności danych osobowych wynika z obowiązku wypełnienia nakładanych na Administratora Danych Osobowych zadań, wynikających z ustaw, wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.
3. Strategiczną częścią zabezpieczania danych osobowych przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do informacji.
4. Na Inspektorze Ochrony Danych spoczywa obowiązek zapoznania osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz konsekwencjami prawnymi z nich wynikającymi.
5. Utrata poufności informacji o zasadach funkcjonowania systemu ochrony danych osobowych jest niezwykle ważna oraz wymaga położenia nacisku na przestrzeganie procedur przez osoby sprawujące opiekę nad systemami i siecią.

§ 4

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności przy przetwarzaniu danych osobowych:

1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;
2. ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;
3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
4. utrata nośnika zawierającego dane osobowe;
5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;
6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku papierowym;
7. udostępnianie danych osobowych osobom nieupoważnionym;

8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną;
9. pokonanie zabezpieczeń fizycznych lub programowych;
10. niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych;
11. niedyskrecja osób uprawnionych do przetwarzania danych osobowych;
12. nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.);
13. niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych;
14. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;
15. podsłuch lub podgląd danych osobowych;
16. elektromagnetyczna emisja ujawniająca;
17. podsłuch akustyczny i podsłuch emisji ujawniającego promieniowania elektromagnetycznego;
18. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;
19. zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 5

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	Całkowita utrata poufności

§ 6

1. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w dokumentacji papierowej stanowiącej część zbioru danych osobowych, w systemie informatycznym, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań użytkowników systemu.
2. Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.
3. Integralność danych dotyczy przede wszystkim wartości informacyjnych przetwarzanych w postaci elektronicznej. Dlatego tak ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci.

4. Administrator Danych powinien objąć procedurami weryfikacji i rozliczania pracowników sprawujących opiekę nad systemami i siecią oraz wprowadzić bieżącą, regularną detekcję prób ingerencji do systemu informatycznego oraz wszelkie próby naruszenia jego struktury, ponieważ skutkiem takich działań jest uszkodzenie bazy danych i w rezultacie naruszenie zapisów ustawy.

§ 7

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przy przetwarzaniu danych osobowych:

1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;
2. błędy, pomyłki;
3. brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
4. wadliwe działanie systemu operacyjnego;
5. brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.
6. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;
7. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
8. działanie złośliwego oprogramowania (wirusy);
9. pożar, zalanie, ekstremalna temperatura, itp.;
10. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

§ 8

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

§ 9

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

§ 10

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu ochrony danych osobowych:

1. brak kontroli nad dokumentami wykorzystywanymi do bieżącej pracy w zakresie ich kopiowania i drukowania;
2. wyparcie się pracy na stanowisku, gdzie przetwarza się dane osobowe;
3. wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
4. błędy oprogramowania lub sprzętu;
5. nieprzydzielenie użytkownikom indywidualnych identyfikatorów;
6. niewłaściwa administracja systemem informatycznym;
7. niewłaściwa konfiguracja systemu informatycznego;
8. zniszczenie lub sfałszowanie logów systemowych;
9. brak rejestracji udostępnienia danych osobowych;
10. podszywanie się pod innego użytkownika;
11. niespełnienie przez system wymagań ustawowych.

§ 11

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności
< 10 >	Absolutny skutek utraty rozliczalności

§ 12

Dla ochrony danych osobowych szczególnie niebezpieczne są występujące zagrożenia miejsc, w których przetwarza się dane osobowe, które występują przeważnie ze względu na ingerencję:

1. **SIŁY NATURY** (to zdarzenia niewynikające z działalności człowieka), mogą to być:
   - **a)** uderzenie pioruna;
   - **b)** pożar będący konsekwencją ww. uderzenia pioruna;
   - **c)** starzenie się sprzętu;
   - **d)** starzenie się nośników pamięci;
   - **e)** smog, kurz;
   - **f)** katastrofy budowlane;
   - **g)** ulewny deszcz;

h) huragan;
i) ekstremalne temperatury, wilgotność;

j) epidemia.

2. **LUDZI** (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy), mogą to być:

a) błędy i pomyłki użytkowników;
b) błędy i pomyłki administratorów;
c) błędy utrzymania systemu w poufności, integralności i rozliczalności;
d) zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu;
e) zagubienie nośnika zawierającego dane osobowe;
f) niewłaściwe zniszczenie nośnika;
g) nielegalne użycie oprogramowania;
h) choroba ważnych osób i nieuprawnione zastępstwo;
i) epidemia kadry i brak osób upoważnionych do dostępu;
j) podpalenie obiektu;
k) zalanie wodą;
l) katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka;
m) zakłócenia elektromagnetyczne, radiotechniczne;
n) podłożenie i wybuch bomby, ładunku wybuchowego;
o) użycie broni;
p) zmiany napięcia w sieci;
q) utrata prądu;
r) zbieranie się ładunków elektrostatycznych;
s) utrata kluczowych pracowników;
t) niedobór pracowników;
u) defekty oprogramowania;
v) szpiegostwo;
w) terroryzm;
x) wandalizm;
y) destrukcja zbiorów i programów impulsem elektromagnetycznym;
z) kradzież;
aa) włamanie do systemu;
bb) wyłudzenie, fałszowanie dokumentów;
cc) podszycie się pod uprawnionego użytkownika;
dd) podsłuch;
ee) użycie złośliwego oprogramowania;
ff) wykorzystanie promieniowania ujawniającego.

.....
(Podpis Administratora Danych Osobowych)

PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

§ 1

Podatność systemu na zagrożenia stanowi pewnego rodzaju słabość. Obecnie, szczególnie trudno jest obronić się przed zagrożeniami w zakresie teleinformatycznym, co związane jest z coraz to bardziej wyrafinowaną cyberprzestępczością. Wraz z coraz to większą ilością dostępnych w środowisku internetowym usług, nasilają się działania przestępcze. Chroniąc placówkę przed takowym działaniem, należy wdrożyć odpowiednie procedury.

§ 2

Podatność systemu na zagrożenia może wynikać z:

1. **Dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę, jak obsługiwać system.**

   Fizyczna ochrona danych osobowych to jeden z podstawowych obszarów w zakresie przetwarzania danych osobowych. Osoba przetwarzająca dane osobowe bardzo często nie zdaje sobie sprawy, jak ważne jest przestrzeganie chociażby „zasady czystego biurka", która bardzo często jest marginalizowana i zwyczajnie nieprzestrzegana. Bardzo często nieświadomość pracowników w tej materii wiąże się z negatywnymi konsekwencjami dla placówki, np. kwestia złożenia skargi, której przedmiotem jest niedochowywanie należytej staranności w zakresie fizycznej ochrony danych osobowych. Proces wdrażania w placówce „kodeksu dobrych praktyk" w kontekście ochrony danych osobowych jest procesem długoletnim i dynamicznym, ale bezsprzecznie powinno się w pierwszej kolejności uwrażliwiać na fizyczną ochronę danych osobowych. Ponadto, tylko i wyłącznie osoby upoważnione do przetwarzania danych osobowych powinny posiadać wiedzę o tym, w jaki sposób obsługiwać system informatyczny, będący integralnym elementem placówki.

2. **Dostępności informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych.**

   System informatyczny w placówce powinien być odpowiednio zabezpieczony, również jeśli dostęp do niego jest możliwy za pośrednictwem połączeń zewnętrznych. Niezależnie od zastosowanych rozwiązań teletransmisyjnych, system ten powinien być „szczelny", to znaczy wystarczająco odporny na wszelkiego rodzaju zewnętrzne zagrożenia.

3. **Możliwości celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych.**

   Możność nieuprawnionego działania na sprzęcie, czy oprogramowaniu może być wynikiem zastosowanej manipulacji, podsłuchu czy podstawienia. Podsłuch polega na tym, że charakter poufności przekazywanych treści zostaje naruszony. Manipulacja z kolei, będzie działaniem, które ukierunkowane jest na uzyskanie dostępu do treści danych i nieuprawnioną ingerencję w nie. Natomiast podstawienie, polega między innymi na wprowadzeniu drugiej strony w błąd, co do swojej tożsamości, po to tylko, by uzyskać konkretne informacje. Kadra powinna być odpowiednio uwrażliwiona na otrzymywanie korespondencji mailowej, co do której zaistnieje podejrzenie, że została przesłana w celu wprowadzenia wirusa komputerowego.

4. **Możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję.**

   Sprzęt informatyczny powinien być cyklicznie odpowiednio serwisowany, tak by wyeliminować zagrożenia. Należy zaznaczyć, iż z firmą informatyczną zewnętrzną, nie podpisujemy upoważnienia do przetwarzania danych osobowych, ale przynajmniej klauzulę poufności informacji w kontekście przetwarzanych danych osobowych. Wzór klauzuli poufności stanowi załącznik nr 7.

5. **Przesyłania informacji przez niezabezpieczone łącza telekomunikacyjne.**

   Brak zabezpieczeń kryptograficznych łącza telekomunikacyjnego czy nieefektywność fizycznych zabezpieczeń, również stanowi zagrożenie utraty poufności danych osobowych.

§ 3

1. Podatność systemu na zagrożenia została ograniczona poprzez:
   a) ochronę fizyczną obiektu, w tym stanowisk komputerowych;
   b) kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;
   c) wydzielenie stref ochronnych;
   d) ograniczenie liczby personelu, mającego potencjalnie dostęp do pomieszczeń, w których znajdują się dane osobowe;
   e) zbudowanie stabilnej sieci zasilającej;
   f) przeglądy okresowe nośników;
   g) kontrolę zmian konfiguracji;
   h) testowanie oprogramowania;
   i) audyt;
   j) zabezpieczanie haseł;
   k) użycie oprogramowania antywirusowego;
   l) backupy.
2. By maksymalnie wyeliminować zagrożenie dla całego systemu ochrony danych osobowych, należy wdrożyć procedury kontrolne, które nie będą zorientowane tylko i wyłącznie na jeden obszar przetwarzania danych osobowych, np. środowisko komputerowe. Warunkiem wyeliminowania działań cyberprzestępców, jest pełne współdziałanie wszystkich obszarów przetwarzania danych osobowych:
   a) prowadzenie odpowiedniej dokumentacji;
   b) fizyczna ochrona danych osobowych;
   c) środowisko komputerowe;
   d) „kodeks dobrych praktyk" wdrożony przez Inspektora Ochrony Danych, o ile jest powołany lub Administratora Danych Osobowych.
3. Przebieg przykładowej kontroli tych obszarów stanowi załącznik nr 8.

§ 4

W celu wdrażania systemu ochrony danych osobowych w taki sposób, by uniemożliwić działanie nieuprawnione na danych osobowych, Administrator Danych Osobowych zobowiązuje pracowników podmiotu o nazwie **Urząd Miasta Świeradów-Zdrój** do stosownego zachowania w trakcie przetwarzania danych osobowych, czego aprobatę wyraził w swojej rekomendacji, która stanowi załącznik nr 9.

§ 5

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych w jednostce, wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów. Analiza ryzyka musi być wykonywana okresowo przez Inspektora Ochrony Danych i Administratora Systemu Informatycznego - raz do roku na tej podstawie aktualizowana jest tabela ryzyka znajdująca poniżej - § 6.

§ 6

Identyfikacja podatności systemu informatycznego na określone zagrożenia.

WARTOŚĆ	SKUTKI
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

.....

(Podpis Administratora Danych Osobowych)

ANALIZA ZAGROŻEŃ I SZACOWANIE RYZYKA

§ 1

Administrator Danych Osobowych, aby poprawnie przeprowadzić analizę ryzyka, powinien określić:

1. **ZASOBY** - które będzie chronić:
   a) sprzęt komputerowy przechowujący dane - dysk twardy,
   b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
   c) aplikacje, w których przetwarzane są dane osobowe,
   d) pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2. **ZAGROŻENIA** - czynnik, który może powodować wystąpienie incydentu;
3. **PODATNOŚĆ** - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie;
4. **SKUTKI** - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

§ 2

Administrator Danych Osobowych bądź Inspektor Ochrony Danych, aby dokonać skutecznego zarządzania bezpieczeństwem informacji w podmiocie, dokonuje dokładnej analizy zagrożeń w związku z reagowaniem na zmieniające się warunki otoczenia mające wpływ na ryzyko w organizacji. Tak stworzony efektywny system zarządzania daje możliwość podjęcia działań redukujących wartość ryzyka do akceptowanego poziomu.

§ 3

Poniższy schemat obrazuje prawidłowy tok szacowania i postępowania z ryzykiem, jakie podejmuje Administrator Danych Osobowych.

§ 4

1. Analiza ryzyka jest częścią szacowania ryzyka. Jest ona pojęciem węższym niż szacowanie ryzyka, nie zawiera bowiem oceny ryzyka.
2. Ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można zaakceptować.
3. Szacowanie ryzyka obejmuje analizę ryzyka i ocenę ryzyka.

§ 5

1. Administrator Danych Osobowych szacuje wynik ryzyka. Poprzez określenie poziomu ryzyka akceptowalnego i kończy etap szacowania ryzyka.
2. Administrator Danych osobowych wyciąga wnioski oraz podejmuje działania naprawcze, mające na celu obniżenie wartości ryzyka akceptowalnego.
3. Tabela szacowania ryzyka stanowi załącznik nr 10.

§ 6

1. Administrator Danych Osobowych określa poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie średnim w podmiocie o nazwie **Urząd Miasta Świeradów-Zdrój** przy uwzględnieniu ryzyka ogólnego przy wartości **31,6**

   RYZYKO = wartość skutków x podatność zasobów systemu

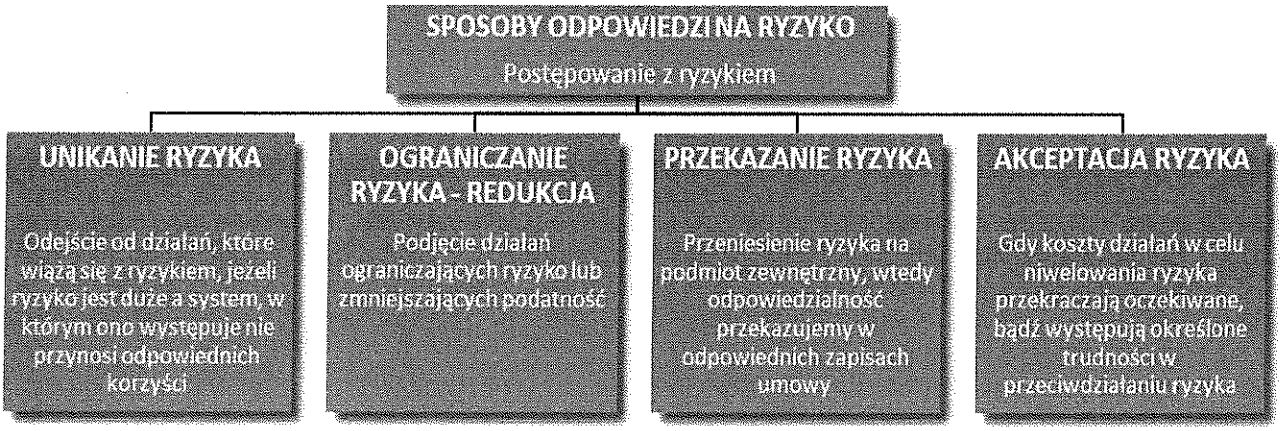
   (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
<1-20>	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

2. Poziomy ryzyka utraty bezpieczeństwa danych osobowych:
   a) **NISKI** – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;
   c) **WYSOKI** – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;
   d) **MAKSYMALNY** – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

§ 7

Administrator Danych Osobowych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem. Koniecznym jest podjęcie działania, które będzie odpowiedzią podmiotu na oszacowany poziom występującego ryzyka. W ramach postępowania z ryzykiem możemy podjąć cztery różne działania.



§ 8

Proces zarządzania ryzykiem związany z bezpieczeństwem informacji zapewnia:

1. identyfikowanie zagrożeń dla przetwarzanych informacji;
2. oszacowanie ryzyka w kategoriach konsekwencji dla funkcjonowania biznesowego oraz prawdopodobieństwa wystąpienia zagrożeń;
3. odpowiednie przedstawienie oraz zrozumienie prawdopodobieństwa oraz konsekwencji materializacji ryzyka;
4. ustanowienie priorytetów dotyczących postępowania z ryzykiem;
5. wprowadzanie priorytetowych działań mających na celu redukcję ryzyka;
6. zaangażowanie kierownictwa podczas podejmowania decyzji związanych z zarządzaniem ryzykiem oraz bieżące informowanie go o postępach realizowanych działań minimalizujących;
7. monitorowanie i regularne przeglądanie ryzyka oraz procesu zarządzania nimi;
8. kształcenie pracowników w zakresie ryzyka oraz działań mających na celu obniżenie poziomu prawdopodobieństwa ich wystąpienia.

.....

(Podpis Administratora Danych Osobowych)

WNIOSKI I DZIAŁANIA NAPRAWCZE
W ZWIĄZKU Z PRZEPROWADZONĄ „ANALIZĄ RYZYKA I ZAGROŻEŃ PRZY PRZETWARZANIU DANYCH OSOBOWYCH"

§ 1

1. Administrator Danych Osobowych w placówce o nazwie: **Urząd Miasta Świeradów-Zdrój**, przeprowadził analizę dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.
2. Administrator Danych Osobowych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona analiza.
3. Zmiany związane z pkt 2 należy wprowadzić do aktualnej Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

§ 2

W wyniku przeprowadzonej analizy w placówce o nazwie: **Urząd Miasta Świeradów-Zdrój**, Administrator Danych Osobowych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

- **ODCIĘCIE ZASILANIA,**
- **KRADZIEŻ,**
- **AWARIA SPRZĘTU,**

§ 3

W celu zmniejszenia zagrożeń, wymienionych w § 2 przez Administratora Danych Osobowych, należy zwrócić uwagę w szczególności na:

- **PRZEGLĄD BATERII W UPS-ach,**
- **ZABEZPIECZENIA PLACÓWKI W ZAKRESIE TECHNICZNYM,**
- **STAN TECHNICZNY SPRZĘTU,**

§ 4

Administrator Danych Osobowych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje działania naprawcze, polegające w szczególności na:

- **Kontakt z autoryzowanym serwisem celem modernizacja lub wymiany modułu zasilania,**
- **Zwiększenie kontroli doraźnych oraz interwału sporządzania raportu dziennego/miesięcznego,**
- **Starania w zakresie powiększenia gospodarki magazynowej z zakresu części zamiennych .**

.....

(Podpis Administratora Danych Osobowych)

WZÓR KLAUZULI POUFNOŚCI INFORMACJI [1]

§ 1

Strony umowy zobowiązują się wzajemnie do niewykorzystywania, nieujawniania oraz nieprzekazywania informacji, które stanowią tajemnicę przedsiębiorstwa drugiej strony niniejszej umowy.

§ 2

Strony powinny zachować poufność informacji, które zdobędą na każdym etapie jakiejkolwiek wzajemnej współpracy.

§ 3

Klauzula poufności danych obowiązuje strony przez okres trwania umowy, a także bezwzględnie po jej zakończeniu przez okres 2 lat.

§ 4

Strony odpowiadają za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzyły.

§ 5

Strony umowy zobowiązują się do wykorzystywania przetwarzanych przez nie danych osobowych, w ramach realizacji niniejszej umowy, wyłącznie w celach określonych w umowie.

§ 6

Stronom umowy przysługuje w każdym czasie i bez ograniczenia - kontrola procesu przetwarzania i ochrony danych osobowych.

§ 7

Strony, dopełniając czynności wynikających z niniejszej umowy, zobowiązują się do przestrzegania przepisów 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.

§ 8

W przypadku niedochowania warunków umowy, strony zastrzegają sobie prawo rozwiązania niniejszej umowy w trybie natychmiastowym, w każdym czasie.

1 **UWAGA:** Niniejszy dokument może być zastosowany:

- jako osobny (niezależny) dokument celem zobowiązania drugiej strony do zachowania poufności informacji,
- jako dodatkowe zapisy (paragrafy) do umowy lub innego dokumentu wiążącego strony wzajemną współpracą.

PRZEBIEG PRZYKŁADOWEJ KONTROLI PODATNOŚCI SYSTEMU

L.P.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.
3.	DOKUMENTACJA	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, ale nie przetwarzają tych danych, posiadają zgody na przebywanie w obszarze przetwarzania.
4.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka".
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).
7.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w programie komputerowym bazodanowym (czyli dotyczącym baz danych) logują się za pomocą WŁASNEGO identyfikatora i hasła.
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.
13.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
14.	ZBIORY DANYCH OSOBOWYCH	Kontrolowanie, czy opracowano prawidłowy rejestr czynności przetwarzania danych, który jest na bieżąco uzupełniany.
15.	ZBIORY DANYCH OSOBOWYCH	Sprawdzenie, czy wszystkie zbiory, które prowadzi się w placówce, znajdują się w rejestrze czynności przetwarzania.
16.	ZBIORY DANYCH OSOBOWYCH	Przeprowadzenie wywiadu, którego celem jest ustalenie, czy pracownik przetwarza zbiór danych osobowych, który nie figuruje w rejestrze czynności przetwarzania (szczególnie ma się na względzie projekty prowadzone przez referaty).
17.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: • próby nieuprawnionego dostępu do danych osobowych; • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; • próba nieuprawnionej interwencji przy sprzęcie komputerowym; • wynoszenie niezabezpieczonych pamięci z miejsca pracy; • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

REKOMENDACJA ODPOWIEDNIEJ POSTAWY OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Przepisy kodeksu pracy zobowiązują pracownika do sumiennego wykonywania swoich obowiązków. Pracownik powinien odpowiednio przestrzegać czasu pracy, co w konsekwencji oznacza, że nie powinien on w godzinach pracy zajmować się prywatnymi sprawami, chociażby prywatną korespondencją.

§ 2

Pracodawca wyposaża pracowników w konkretne narzędzia pracy, jak telefon czy komputer i nie musi godzić się na wykorzystywanie ich do prywatnych celów.

§ 3

Pracodawca może kontrolować pracownika w ramach stosownego wykorzystywania narzędzi, które powinny służyć tylko do celów służbowych. Za interesem pracodawcy przemawia fakt, że musi on chronić tajemnicę przedsiębiorstwa oraz zabezpieczać odpowiednio placówkę pod względem systemu ochrony danych osobowych.

§ 4

Należy przypomnieć niniejszym dokumentem, iż w placówce wdrożono postanowienia Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym, co w konsekwencji oznacza, iż dobrych praktyk powinno się przestrzegać.

§ 5

Jeśli pracodawca podczas kontroli stwierdzi, iż zakaz nie jest respektowany, może wobec pracownika wyciągnąć konsekwencje służbowe.

§ 6

Pracodawca może ustalić, że na służbowych komputerach nie można instalować aplikacji oraz używania portali społecznościowych. Ponadto, pracodawca może zakazać wnoszenia prywatnych nośników danych tj. nośników: optycznych (płyty CD, DVD itp.), półprzewodnikowych (układy scalone), magnetycznych (w tym pamięci ferrytowe), magnetooptycznych, polimerowych (np. Millipede), papierowych (np. karty dziurkowane), z linią opóźniającą (np. pamięci rtęciowe).

§ 7

Pracodawca niniejszym dokumentem informuje pracowników, iż kontrola w danym zakresie będzie miała miejsce, a pracownicy przyjmują ten fakt do wiadomości.

.....

(Podpis Administratora Danych Osobowych)

TABELA SZACOWANIA RYZYKA

SZACOWANIE RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI																			
RYZYKO ŚREDNIE [2]:				29			35			33			29			32	31,6
ZAGROŻENIA			ZASOBY SZACOWANE	SPRZĘT			LUDZIE			APLIKACJA			POMIESZCZENIA			DODATKOWE ZABEZPIECZENIA			RYZYKO OGÓLNE [3]:
			SZACOWANIE	SKUTKI	PODATNOŚĆ	RYZYKO [4]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	
INTEGRALNOŚĆ		AWARIA SPRZĘTU		5	5	25	8	5	40	8	5	40	8	4	32	8	5	40	
		ODCIĘCIE ZASILANIA		6	5	30	6	5	30	8	6	48	7	6	42	7	5	35	
		POŻAR		5	2	10	7	6	42	7	5	35	8	4	32	6	6	36	
		ATAK WIRUSA		6	3	18	7	5	30	8	5	40	5	5	25	5	4	20	
		KRADZIEŻ		8	4	32	8	6	48	6	5	30	7	4	28	6	4	24	
		NIEUPRAWNIONY DOSTĘP		8	5	40	5	4	20	7	6	42	7	5	35	6	5	30	
ROZLICZALNOŚĆ		AWARIA SPRZĘTU		9	5	45	7	5	35	5	5	25	6	5	30	6	5	30	
		ODCIĘCIE ZASILANIA		7	5	35	6	6	36	7	5	35	8	6	48	9	5	45	
		POŻAR		8	4	32	7	4	28	5	4	20	7	4	28	6	5	30	
		ATAK WIRUSA		6	5	30	6	5	30	5	5	25	5	4	20	5	5	25	
		KRADZIEŻ		7	4	28	7	3	21	6	5	30	6	4	24	6	5	30	
		NIEUPRAWNIONY DOSTĘP		6	4	24	8	3	24	7	5	35	8	3	18	8	5	40	
POUFNOŚĆ		AWARIA SPRZĘTU		5	4	20	8	5	40	4	4	16	5	4	20	7	6	42	
		ODCIĘCIE ZASILANIA		4	5	20	7	5	35	6	6	36	7	5	35	5	5	25	
		POŻAR		7	3	21	7	6	42	7	6	42	8	3	24	6	5	30	
		ATAK WIRUSA		6	5	30	7	5	35	7	5	35	5	4	20	6	5	30	
		KRADZIEŻ		8	6	48	8	5	40	7	4	28	8	4	32	5	5	25	
		NIEUPRAWNIONY DOSTĘP		7	5	35	8	6	48	7	5	35	7	4	28	7	4	28	

Skala poziomu ryzyka:

2 **RYZYKO ŚREDNIE** = suma ryzyka każdego z sześciu zakresów poufności, rozliczalności i integralności dzielona przez 18

3 **RYZYKO OGÓLNE** = suma ryzyka średniego z zasobów: sprzęt, ludzie, aplikacja, pomieszczenia, zabezpieczenia dodatkowe, dzielona przez 5

4 **RYZYKO** = wartość skutków x podatność zasobów systemu (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
1-20	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
21-60	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
61-80	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
81-100	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

PODSUMOWANIE

W podmiocie o nazwie: **Urząd Miasta Świeradów-Zdrój** po przeprowadzeniu analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, zwanej dalej: analizą zagrożeń i ryzyka przy przetwarzaniu danych osobowych wartość i poziom ryzyka przedstawia się następująco:

Ryzyko ogólne wynosi: **31,6 / 100.**

Powyższa wartość ryzyka określa **Średnie** ryzyko utraty bezpieczeństwa danych osobowych.

.....

(Data i Podpis Administratora Danych Osobowych)

LEŚNY & WSPÓLNICY
KANCELARIA PRAWNA

....., dnia ..... 2020 r.

Załącznik nr 2 do Polityki ochrony danych osobowych

Administrator Danych Osobowych
Burmistrz Miasta Świeradów-Zdrój

Upoważnienie
do przetwarzania danych osobowych
nr .....

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

§1

Niniejszym jako Administrator Danych Osobowych upoważniam do przetwarzania danych osobowych Pana/Panią ..... zatrudnionego w Urzędzie Miasta Świeradów-Zdrój na stanowisku/ pełniącego/ą funkcję ..... w zakresie wskazanym poniżej.

§2

Przetwarzanie danych osobowych następuje wyłącznie na podstawie udzielonego upoważnienia i w zakresie w nim wskazanym.

§3

Niniejsze upoważnienie przyznaje Pani/Panu prawo do przetwarzania w zakresie następujących czynności (należy wskazać w jakich czynnościach bierze udział pracownik):

a) .....

b) .....

c) .....

(W przypadku gdy była utworzona wcześniej polityka bezpieczeństwa, można skorzystać z tego co było już do tej pory określone. Jeśli był rejestr zbiorów to można wykorzystać zbiory tam znajdujące w celu określenia do jakich posiada uprawnienia konkretny pracownik. W przypadku braku, należy określić do jakich zbiorów danych, lub czynności przetwarzania przysługuje upoważnienie np. akta obecnych i byłych pracowników).

§4

1. Przetwarzanie danych osobowych w zakresie wskazanych wyżej zbiorów obejmuje przetwarzanie

a) w formie papierowej: ..... (np. kartoteki, wyciągi, skorowidze, wykazy i inne zbiory)
lub/oraz

b) w formie elektronicznej z wykorzystaniem następujących systemów informatycznych służących do przetwarzania danych osobowych: ..... (wskazać systemy informatyczne w jakich przetwarzane są dane osobowe).

2. Zakres przetwarzania danych osobowych obejmuje następujący poziom uprawnień: ..... (przetwarzanie bez ograniczeń lub ograniczone: podgląd danych, odczytywanie danych, wprowadzanie/rejestrowanie danych, opracowywanie danych, modyfikowanie danych, usuwanie danych, itp.)

§5

Upoważnienie traci ważność z dniem (np. rozwiązania umowy o pracę, umowy cywilnoprawnej)

(albo)

Upoważnienie zostaje udzielone na okres od dnia … do dnia ….

.....

Podpis osoby nadającej
upoważnienie

Załącznik nr 3 do polityki ochrony danych osobowych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH URZĄD MIASTA ŚWIERADÓW-ZDRÓJ

Nr	Imię i nazwisko	Identyfikator	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data i podpis ADO	Data Odebrania uprawnień Podpis ADO

Załącznik nr 4 do polityki ochrony danych osobowych

Umowa
powierzenia przetwarzania danych osobowych
(wzór)

zawarta w dniu ..... pomiędzy

Panią/Panem ..... – Burmistrzem Miasta Świeradów-Zdrój działającym jako Administrator Danych, Urzędu Miasta Świeradów-Zdrój z siedzibą pod adresem ul. 11 Listopada 35, 59-850 Świeradów-Zdrój
zwanym w dalszej części umowy **Administratorem**

oraz
..... z siedzibą ..... zwaną w dalszej części umowy **Podmiotem przetwarzającym**
reprezentowaną/ym przez:
.....

Niniejsza umowa stanowi integralną część umowy ..... nr ..... z dnia ..... zawartej pomiędzy Urzędem Miasta Świeradów-Zdrój reprezentowanym przez Administratora, a Podmiotem przetwarzającym, zwaną dalej: **Umową podstawową**.

§ 1
Powierzenie przetwarzania danych osobowych – zakres i cel

1. Na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE.L.2016.119.1) zwanego w dal-

szej części „RODO" Administrator powierza Podmiotowi przetwarzającemu dane osobowe, o których mowa w niniejszej umowie do ich przetwarzania na zasadach i w celu określonym poniżej.

2. Administrator oświadcza, że jest administratorem danych osobowych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
3. Powierzone dane osobowe będą przetwarzane w związku z realizacją Umowy podstawowej. Administrator upoważnia Podmiot przetwarzający do przetwarzania danych osobowych niezbędnych do realizacji umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji celu tej umowy.
4. Zakres przetwarzania obejmuje następujące dane osobowe .....*[wskazać zakres przetwarzania, z dokładnym określenie jakie dane będziecie przekazywać do firmy świadczącej usługę np. imię i nazwisko, adresy właścicieli nieruchomości z którymi są zawarte umowy na odbiór odpadów]*
5. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
6. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000) oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
7. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający, podczas przetwarzaniu powierzonych danych osobowych, zobowiązuje się do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Przetwarzający nie będzie kopiować, powielać lub w jakikolwiek sposób rozpowszechniać danych osobowych, z wyjątkiem sytuacji, gdy wykorzystanie tych danych następuje w celu wykonania niniejszej Umowy. W tym przypadku wszelkie kopie będą własnością Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Administrator może udzielić odrębnej zgody na dalsze przechowywanie powierzonych danych osobowych, ze wskazaniem sposobu, celu oraz czasu ich przechowywania.
7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.

§3

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający i jego podwykonawców przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator będzie realizował swoje prawo kontroli z minimum 7 dniowym uprzedzeniem prawo kontroli w godzinach pracy Podmiotu przetwarzającego, przy zachowaniu jak najniższej dopuszczalnej ingerencji w funkcjonowaniu Podmiotu przetwarzającego.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§4

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §4 ust. 1 umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 5

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
3. Podmiot przetwarzający odpowiada za szkody jakie powstały wobec Administratora oraz wyrządzone osobom trzecim.

§6

Czas obowiązywania umowy i jej rozwiązanie

1. Niniejsza umowa obowiązuje od dnia ..... r. do dnia ..... r., a więc na czas trwania umowy podstawowej.
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem miesięcznego okresu wypowiedzenia.
3. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
   b) przetwarza dane osobowe w sposób niezgodny z umową,

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§7

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązany jest do zachowania w tajemnicy wszelkich informacji oraz danych, w tym danych osobowych, które powziął od Administratora lub podmiotu z nim współpracującego podczas lub w związku z wykonywaniem umowy, w okresie jej obowiązywania i po jej zakończeniu, a także do nieujawniania i nieudostępniania tych informacji jakimkolwiek podmiotom innym niż Administrator, bez jego pisemnej zgody, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub umowy. Obowiązek zachowania tajemnicy, o którym mowa w zdaniu poprzedzającym obejmuje w szczególności zarówno informacje dotyczące samego Administratora, jak i rozpatrywanej dokumentacji, a w szczególności wszelkich innych danych osobowych pozyskanych w jakikolwiek inny sposób zamierzony czy przypadkowy w formie ustnej, pisemnej czy elektronicznej.

§8

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy kodeksu cywilnego, RODO oraz ustawy o ochronie danych osobowych.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych.

.....	.....
Administrator danych	Podmiot przetwarzający

LEŚNY & WSPÓLNICY
KANCELARIA PRAWNA

Załącznik nr 7 do polityki ochrony danych osobowych	**Wykaz budynków, pomieszczeń, lub części pomieszczeń, w których przetwarzane są dane osobowe.**

Budynek/ Kondygnacja	Numer pokoju	Opis (w tym forma przetwarzanych danych np. elektroniczna, tradycyjna)

00-682 Warszawa, ul. Hoża 86/ 410; 62-200 Gniezno ul. Platanowa nr 15
61-806 Poznań, ul. Święty Marcin 29/8; konto nr 45 1940 1076 3105 0557 0000 0000
KRS 0000 406 825; NIP: 784-248-78-16; Regon: 302 011 576
www.lesny.com.pl; kancelaria@lesny.com.pl

LEŚNY & WSPÓLNICY
KANCELARIA PRAWNA

Załącznik nr 5 do polityki ochrony danych osobowych

EWIDENCJA UMÓW POWIERZENIA ZAWARTYCH PRZEZ URZĄD MIASTA ŚWIERADÓW-ZDRÓJ

Nr	Imię i nazwisko	Nr umowy	Zakres powierzenia do przetwarzania danych osobowych	Data powierzenia	Data i podpis ADO	Data Odebrania uprawnień Podpis ADO

Załącznik nr 6 do polityki ochrony danych osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

URZĄD MIASTA ŚWIERADÓW-ZDRÓJ

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych związanego z przetwarzaniem danych osobowych.

2. Instrukcja została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§ 2

Instrukcja określa stosowne procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniające ochronę przetwarzania danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

§ 3

Ilekroć w instrukcji jest mowa o:

1. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalne;

2. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, taki jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym;

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

4. Kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierający dane osobowe;

5. Administratorze Danych – rozumie się przez to Burmistrza Miasta Świeradów-Zdrój jako administratora danych przetwarzanych w Urzędzie Miasta Świeradów-Zdrój;

6. Inspektora Ochrony Danych Osobowych – rozumie się przez to osobę wyznaczoną przez Administratora Danych nadzorującą przestrzegania zasad ochrony przetwarzania danych osobowych. Nadzór dotyczy przede wszystkim stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przez ich udostępnianiem osobom nieupoważ-

nionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Przeprowadza on również kontrole w zakresie określonym regulacjami wewnętrznymi obowiązującymi u Administratora Danych;

7. Administratorze Systemów Informatycznych (ASI) – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację wyznaczonego przez Administratora Danych;

8. Użytkowniku – rozumie się osobę upoważnioną przez Administratora Danych do przetwarzania danych osobowych w systemie informatycznym oraz w kartotekach;

9. Pomieszczeniach – rozumie się prze to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 4

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, prze cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności systemu informatycznego.

2. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

3. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,

   2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 5

1. W celu uwzględnienia ewentualnych zagrożeń oraz kategorii przetwarzanych danych osobowych wprowadza się następujące poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

   1) podstawowy,

   2) podwyższony,

3) wysoki.

2. Poziom co najmniej podstawowy stosuje się, gdy:

   1) w systemie informatycznym nie są przetwarzane dane osobowe,

   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Poziom podwyższony stosuje się gdy:

   1) w systemie informatycznym są przetwarzane dane osobowe,

   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.

5. W systemach informatycznych Administratora Danych stosuje się poziom wysoki.

§ 6

1. Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:

   1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,

   2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,

   3) podpisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasło, identyfikatory) oraz zapewniający dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia,

   4) podejmowanie niezbędnych działań w celu likwidacji stałych ogniw w systemie zabezpieczeń,

   5) okresowe sprawdzenie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,

   6) opracowanie procedur odtworzenia systemu w przypadku wystąpienia awarii,

   7) śledzenie osiągnięć w dziedzinie zabezpieczenia systemów informacyjnych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrożenie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

2. Przez politykę ochrony danych osobowych należy rozumieć określenie zadań, które należy realizować dla zapewnienia spójności wszystkich zabezpieczeń danych osobowych. Została on sformułowana w Polityce Ochrony Danych Osobowych oraz w kolejnych rozdziałach niniejszej Instrukcji. Odzwierciedla ona podstawowe zasady bezpieczeństwa, a także zarządzania systemem informatycznym oraz kartotekami u Administratora Danych.

ROZDZIAŁ II
Przydział uprawnień i identyfikatorów

§7

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych osobowych. stanowi do Polityki Ochrony Danych Osobowych.
2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
4. Postanowienia ust. 2 nie dotyczą użytkowników, którzy przetwarzają wyłącznie dane osobowe gromadzone w kartotekach.
5. Prowadzona jest ewidencja przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§8

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§9

1. Każdy użytkownik - przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe - podlega przeszkoleniu w zakresie:
   1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał,
   2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§10

1. Za organizację szkoleń, o których mowa w § 9 ust. 1 pkt 1 odpowiedzialny jest ASI, zaś szkoleń, o których mowa w § 9 ust. 1 pkt 2 odpowiedzialny jest Inspektor Ochrony Danych Osobowych.

§11

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§12

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§13

1. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela ASI lub inna osoba upoważniona przez Administratora Danych.
2. Zakres uprawnień przypisany do identyfikatora przyznaje ASI na wniosek Administratora Danych.
3. Identyfikator użytkownika nie podlega zmianie.
4. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§14

1. Pierwsze hasło dla użytkownika ustala ASI przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Hasła muszą odpowiadać następującym wymogom:
   1) hasła składają się co najmniej z:
      a) dla poziomu bezpieczeństwa podstawowego 6 znaków,
      b) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
   2) nie mogą być zapisywane w systemie w postaci jawnej,
   3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,
   4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

§15

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisywaniu hasło nie może być wyświetlane na ekranie.
2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

§16

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§17

1. Hasła nie mogą być nigdzie zapisywane.
2. Tryb przechowywania i udostępniania haseł ASI określa załącznik nr 1 do niniejszej instrukcji.

ROZDZIAŁ III
Rejestrowanie i wyrejestrowywanie użytkowników

§18

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych w zbiorach prowadzi osoba wyznaczona przez Administratora Danych. Wzór upoważnień do przetwarzania danych osobowych, stanowi załącznik nr 3 do Polityki Ochrony Danych Osobowych.

§19

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencję użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których ma dostęp wyłącznie ASI lub osoba upoważniona przez Administratora Danych.

§20

Zmiany dotyczące użytkownika, takie jak:

1. zmiana imienia lub nazwiska,
2. zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w § 18 Instrukcji.

§21

Zmiany dotyczące użytkownika, takie jak:

1. rozwiązanie umowy,
2. utrata upoważnienia do przetwarzania danych osobowych,
3. zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

powodują wyrejestrowanie użytkownika przez ASI, w trybie natychmiastowym, z ewidencji, o której mowa w § 18 Instrukcji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

§22

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

2. Osoba prowadząca ewidencję, o której mowa w § 18 Instrukcji, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

§23

Dane dotyczące osób, które zostały wyrejestrowane z ewidencji osób upoważnionych do przetwarzania danych osobowych, z przyczyn, których mowa w § 21 ust. 1 Instrukcji. są gromadzone w postaci odrębnych zbiorów archiwalnych lub stosuje się odpowiednie ich oznaczenia.

ROZDZIAŁ IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§24

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§25

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce Ochrony Danych Osobowych.

§26

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.

2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.

3. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.

4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Inspektora Ochrony Danych Osobowych lub osobę przez niego wyznaczoną.

§27

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z systemu informatycznego lub,

2) poczekać, aż zaktywizuje się blokowany hasłem wygaszacz ekranu.

§28

Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

ROZDZIAŁ V
Procedury tworzenia kopii zapasowych

§29

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 powinny być sporządzane regularnie w okresach wyznaczonych w załączniku nr 2 do Instrukcji.
3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest ASI
4. Odpowiada on także za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.
5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§30

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez ASI.
2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.

§31

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje ASI w obecności Administratora Danych lub osoby przez niego wyznaczonej.
3. Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
4. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI

Przetwarzanie danych osobowych

§32

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.

2. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

3. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

4. Opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce Ochrony Danych Osobowych.

§33

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.

2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§34

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych.

§35

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych. Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1. datę dokonania likwidacji,

2. przedmiot likwidacji (nośniki, kartoteka),

3. przedział czasowy likwidowanych zbiorów danych osobowych,

4. podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII
Zabezpieczenie systemu informatycznego

§36

System informatyczny zabezpiecza się przed:

1. działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

2. utratą danych spowodowaną:

a) działaniem nieautoryzowanego oprogramowania.

b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§37

1. ASI odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.

2. Nowe wersje oprogramowania instaluje wyłącznie ASI niezwłocznie po ich otrzymaniu lub osoba upoważniona przez ASI.

3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona.

§38

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.

2. Program antywirusowy należy instalować również na komputerach przenośnych.

§39

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§40

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych.

2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.

3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

§41

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§42

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI.

2. ASI usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Inspektora Ochrony Danych Osobowych lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§43

W razie niemożności usunięcia wirusa, ASI za zgodą Inspektora Ochrony Danych Osobowych, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§44

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.

2. Prace określone w ust. 1 są wykonywane pod nadzorem ASI lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§45

1. ASI jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.

2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.

§46

1. Po usunięciu wirusa ASI sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.

2. ASI sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:

   1) nazwę wirusa,

   2) datę wykrycia wirusa,

   3) miejsce zainfekowania,

   4) źródło infekcji.

3. Raport, o którym mowa w ust. 2 przekazywany jest Inspektorowi Ochrony Danych Osobowych lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.

§47

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. I, obejmują one:

   1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,

   2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§48

ASI prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§49

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ VIII
Wymagania dotyczące sprzętu i oprogramowania

§50

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Szczegółowy wykaz sprzętu i oprogramowania wykorzystywanego do przetwarzania danych osobowych znajduje się w dokumentacji księgowej.

§51

Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.

§52

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest ASI.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

§53

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.
3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnętrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§54

Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

§55

1. ASI odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

2. System informatyczny wykorzystywany przez użytkowników wyłącznie w celach służbowych. Wyjątki od powyższej reguły możliwe są jedynie za wyraźna zgodą Administratora Danych.

3. System informatyczny może być monitorowany, w tym również z zastosowaniem specjalistycznego oprogramowania lub sprzętu, w celu rejestracji aktywności użytkowników oraz sposobu wykorzystywania systemu informatycznego przez użytkowników.

§56

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.

2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy.

§57

1. ASI jest odpowiedzialny za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:

   1) daty pierwszego wprowadzenia danych do systemu,

   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

   3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,

   4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

   5) sprzeciwu.

Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

1. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

3. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane

w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

4. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:

   1) daty pierwszego wprowadzenia danych,

   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

5. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt 3, 4 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ IX
Procedury wykonywania przeglądów i konserwacji

§58

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje ASI.

2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.

§59

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Inspektora Ochrony Danych Osobowych przez uprawnionych przedstawicieli tych firm pod nadzorem ASI lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§60

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.

2. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

§61

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje ASI lub osoba wyznaczona przez Administratora Danych.

ROZDZIAŁ X
Postanowienia końcowe

§62

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

§63

1. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

2. Oświadczenia przechowywane są w aktach osobowych.

§64

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

.....
(podpis Administratora Danych)

Załącznik nr 1 do Instrukcji
zarządzania systemem
informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ ASI

Ustala się następujący tryb postępowania z hasłami ASI:

1. Hasła ASI przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada wyłącznie Administrator i osoby przez niego upoważnione.
3. Hasła* o którym mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną, nieupoważnioną osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, o którym mowa w pkt 6 dokonuje ASI w obecności Administratora Danych lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Administrator Danych udostępnia hasło osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

Załącznik nr 2 do Instrukcji zarządzania
systemem informatycznym

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą częstotliwość tworzenia kopii awaryjnych:

1. Kopie dobowe i tygodniowe, wykonywane przez ASI lub użytkowników obejmujące:
    a. serwery danych,
    b. dział finansowy.
2. Kopie miesięczne, wykonywane na nośnikach zewnętrznych - magnetycznych lub optycznych umieszczane w zapieczętowanych kopertach, deponowane przez ASI w miejscu określonym w § 29 Instrukcji obejmujące:
        i. serwery danych,
        ii. dział finansowy,
        iii. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii awaryjnych należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Administrator udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

Załącznik nr 7 do polityki ochrony danych osobowych	**Wykaz budynków, pomieszczeń, lub części pomieszczeń, w których przetwarzane są dane osobowe.**

Budynek/ Kondygnacja	Numer pokoju	Opis (w tym forma przetwarzanych danych np. elektroniczna, tradycyjna)

Załącznik nr 8 do Polityki Ochrony Danych Osobowych	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Urząd Miasta Świeradów-Zdrój

L.P.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Forma przetwarzania zbioru[1]	Zabezpieczenia informatyczne[2]	Zabezpieczenia fizyczne[3]	Zabezpieczenia organizacyjne[4]
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						

Legenda:

(1) papierowa, elektroniczna (nazwa systemu informatycznego)

(2) np.: (UPS) – zasilacz awaryjny, (LH) – indywidulny login i hasło do systemu operacyjnego (LHA) – indywidualne hasło dostępu do aplikacji, (SD) – szyfrowanie dysku twardego, (S) – szyfrowanie transmisji danych, (F) – wydzielona fizycznie sieć, (AV) – program antywirusowy, (FW) – zapora systemu (firewall)

(3) np.: (K) – kraty w oknach, (A) – alarm, (W) – wzmocnienie drzwi, (D) – dozór całodobowy, (KD) – kontrola dostępu, (KL) – klimatyzacja, (SP) – sygnalizacja PPOŻ, (ZP) – zamki patentowe, (SF) – Sejf, (SK) – szafa zamykana na klucz, (M) – monitoring, (G) – gaśnica, (N) – niszczarka

(4) np.: (UP) – upoważnienie do przetwarzania danych osobowych, (OP) – oświadczenie o zachowaniu poufności, (SZK) – szkolenie lub zapoznanie osoby z dokumentacją i przepisami

Załącznik nr 8 do Polityki Ochrony Danych Osobowych	**Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych**	**Urząd Miasta Świeradów-Zdrój**

zał 9

Lp	Szczegóły naruszenia/incydentu						Konsekwencje naruszenia	Środki podjęte/które należy podjąć		
	Data zdarzenia	Liczba osób, których dotyczy	Charakter zdarzenia	Opis zdarzenia	Jak dowiedziałeś się o zdarzeniu	Opis danych		Wszystkie osoby poinformowane	Działania naprawcze	Data pierwszego zawiadomienia Prezesa UODO

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	Oskar Manowiecki - Kancelaria Prawna Leśny i Wspolnicy
Adres	ul. Platanowa 15, 62-200 Gniezno
Email	iod@lesny.com
Telefon	61 424 40 33

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 2 RODO

	1	2	3	4	5	6	7	8	9	10	11
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1											
2											
3											
4											
5											

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	Oskar Manowiecki - Kancelaria Prawna Leśny i Wspolnicy
Adres	ul. Platanowa 15, 62-200 Gniezno
Email	iod@lesny.com
Telefon	61 424 40 33

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

[illegible]

Lp.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														[illegible]	
	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategoria osób	Kategoria danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)	Kategorie odbiorców [illegible]	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju / podmiotu)	Jeśli transfer (art. 49 ust. 1 akapit drugi) - dokumentacja odpowiednich zabezpieczeń
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g	Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
1.															
2.															
3.															
4.															
5.															
6.															
7.															
8.															
9.															
10.															
11.															
12.															
13.															
14.															
15.															
16.															
17.															
18.															
19.															
20.															
21.															
22.															

Procedura realizacji praw osób, których dane dotyczą w Urzędzie Miasta Świeradów-Zdrój

Spis treści

Wprowadzenie

Niniejszy procedura ma za zadanie zapewnić realizację praw osób, których dane dotyczą przez pracowników Urzędu Miasta Świeradów-Zdrój oraz realizację obowiązków Urzędu Miasta Świeradów-Zdrój względem tych osób zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o

ochronie danych – dalej: RODO) oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. Ponieważ RODO ma na celu rozszerzenie ochrony podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych, celem niniejszej procedury jest dostarczenie osobom, których dane przetwarzane są w w informacji o przysługujących prawach oraz sposobie ich realizacji oraz wsparcie w realizacji przysługujących uprawnień.

Każda osoba, której dane dotyczą (podmiot danych), jest uprawniona do wniesienia żądania do Urzędu Miasta Świeradów-Zdrój, w którym funkcję Administratora Ochrony Danych pełni Burmistrz Miasta Świeradów-Zdrój, o zrealizowanie praw, o których mowa w art. 15 – 21 RODO, tj.:

a) prawo dostępu do danych,

b) prawo do sprostowania danych,

c) prawo do usunięcia danych („prawo do bycia zapomnianym"),

d) prawo do ograniczenia przetwarzania,

e) prawo do przenoszenia danych,

f) prawo do sprzeciwu wobec przetwarzania danych osobowych.

Urząd Miasta Świeradów-Zdrój rozpatruje żądania osób, których dane dotyczą, z należytą starannością, uwzględniając stosowane przepisy prawa oraz prawa i wolności innych osób, których dane mogą dotyczyć.

Realizacja uprawnienia dostępu do danych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy w Urzędzie Miasta Świeradów-Zdrój przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:
   a) w jakim celu są przetwarzane jej dane osobowe;
   b) jakich kategorii danych osobowych dotyczy przetwarzanie;
   c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;

e) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) o prawie wniesienia skargi do organu nadzorczego;
g) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

2. Osoba fizyczna otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie kopii przetwarzanych danych osobowych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Pierwsza kopia i jej przekazanie odbywa się bezpłatnie, lecz za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator będzie miał prawo pobrać „opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora).
3. Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych. Uzyskując wgląd do swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych.
4. W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
3. Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres urzędu. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej zobowiązany jest dokonać weryfikacji przetwarzanych danych. W przypadku stwierdzenia konieczności wprowadzenia zmian informuje o tym bezpośredniego przełożonego. Następnie niezwłocznie dokonuje zmian,

rejestrując ten fakt w aktach sprawy. Uzupełnienie danych następuje zawsze z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych w trybie art. 16 RODO nie znajdzie zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 KPA.

Prawo do żądania usunięcia danych (tzw. prawo do bycia zapomnianym)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zarówno danych zwykłych jak i szczególnych kategorii danych, a jednocześnie nie ma innej podstawy prawnej ich przetwarzania;
   c) osoba, której dane dotyczą, wnosi sprzeciw, o którym mowa w punkcie 3.2.7. niniejszego dokumentu, wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.
2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
   a) do korzystania z prawa do wolności wypowiedzi i informacji;
   b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do

wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

d) do ustalenia, dochodzenia lub obrony roszczeń.

4. W sytuacji gdy żądanie osoby, której dane dotyczą jest uzasadnione, a po stronie Urzędu Miasta Świeradów-Zdrój nie ma podstaw prawnych odmowy realizacji żądania zgłasza się sprawę pracownikowi prowadzącemu archiwum zakładowe w celu dokonania usunięcia danych zgodnie z przepisami w zakresie brakowania dokumentacji archiwalnej lub niearchiwalnej stosownie do kategorii dokumentacji. Postępowanie dotyczy zarówno danych przetwarzanych w formie tradycyjnej jak i elektronicznej. W miejscu prowadzonej sprawy pozostawia się notatkę wraz z kopią zgody archiwum państwowego na niszczenie oraz kopię protokołu zniszczenia.

Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.
2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Do ograniczenia może dojść w następujących przypadkach:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych. W tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) osoba, której dane dotyczą, wobec przetwarzania wniosła sprzeciw, o którym mowa w punkcie 3.9. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy

prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każda osoba, która jest upoważniona do przetwarzania tych danych była świadoma iż dane te można jedynie przechowywać.
5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

Prawo do przenoszenia danych osobowych

1. Jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany osoba ta ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące. Dotyczy to danych, które osoba składająca żądanie wcześniej dostarczyła. Osoba ta ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Urzędu Miasta Świeradów-Zdrój.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Urząd Miasta Świeradów-Zdrój bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe i osoba wykaże, iż administrator, któremu mają zostać dane przekazane akceptuje taki sposób pozyskania danych.
3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.
4. Wykonanie prawa, o którym mowa w ust. 1 niniejszego działu, pozostaje bez uszczerbku dla prawa do usunięcia danych.
5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Prawo do wniesienia sprzeciwu

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym, jakim jest między innymi dostęp do informacji publicznej, w tym umieszczanie danych w Biuletynie Informacji Publicznej, z przyczyn związanych z jej

szczególną sytuacją, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw, wobec przetwarzania dotyczących jej danych osobowych.

2. Jeżeli dane osobowe są przetwarzane do celów badań naukowych, celów historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
3. Administratorowi nie wolno już przetwarzać danych osobowych względem, których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
4. Najpóźniej przy okazji pierwszego kontaktu z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa powyżej, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
5. W momencie złożenia sprzeciwu wobec przetwarzania Urzędu Miasta Świeradów-Zdrój niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli Urząd Miasta Świeradów-Zdrój posiada podstawę prawną, o której mowa powyżej informuję osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku gdy uzasadniona jest przesłanka do zrealizowania żądania postępuje się zgodnie z zasadami usunięcia danych osobowych w przypadku zasadności wniosku o usunięcie danych (*rozdział: Prawo do żądania usunięcia danych – pkt 4*).

Terminy

1. Administrator zobowiązany jest do udzielenia odpowiedzi na każdy wniosków osoby fizycznej dotyczący korzystania z uprawnień przysługujących w ramach ochrony danych osobowych bez zbędnej najpóźniej w terminie miesiąca od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne 2 miesiące, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca, licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

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

Inspektor Ochrony Danych (IOD)

1. W Urzędzie Miasta Świeradów-Zdrój został wyznaczony Inspektor Ochrony Danych. W celu ułatwienia kontaktu z inspektorem utworzony został adres: iod@lesny.com.pl, podany do publicznej wiadomości na stronie internetowej Urzędu, w Biuletynie Informacji Publicznej oraz w treści klauzul zgody i klauzul informacyjnych, na który każda osoba fizyczna, której dane są przetwarzane w związku z działaniami Urzędu ma prawo się skontaktować i uzyskać informacje wynikające z realizacji swoich praw.

Obsługa wniosków

1. Każdy wniosek o realizację praw osób wpływający na adres mailowy Urzędu, bezpośrednio do kancelarii lub na skrzynki mailowe pracowników Urzędu (wówczas jest drukowany przez pracownika i niezwłocznie przekazywany do Kancelarii) musi zostać rejestrowany w książce korespondencji i zgodnie z instrukcją kancelaryjną przekazywany do Sekretarza celem zadekretowania.
2. Sekretarz przekazuje wniosek do Inspektora, który koordynuje jego realizację poprzez przekazanie do właściwych komórek organizacyjnych, w celu ustalenia, gdzie znajdują się dane osobowe wnioskodawcy oraz uzgadnia sposób załatwienia sprawy.
2. Odpowiedź przygotowują pracownicy poszczególnych komórek organizacyjnych, merytorycznie odpowiedzialnych za przetwarzanie danych w przedmiotowej sprawie. Pracownik Wydziału odpowiada za poprawność danych i identyfikację wnioskodawcy oraz wskazanie podstawy prawnej na podstawie której przetwarzane są dane osobowe. Inspektor doradza w zakresie terminu realizacji wniosku oraz poprawnego merytorycznie sformułowania odpowiedzi. Wzór odpowiedzi stanowi *załącznik nr 2.*
3. W celu zapewnienia udostępnienia danych jedynie osobom, których dane dotyczą dopuszcza się trzy kanały komunikacji:

- ✓ elektroniczny – z podpisem kwalifikowanym lub potwierdzony profilem zaufanym e-PUAP, jeśli wniosek wpłynie „zwykłym mailem" można zażądać ponownego złożenia wniosku w dopuszczonym trybie;
- ✓ tradycyjny – w formie papierowej opatrzony własnoręcznym podpisem;
- ✓ ustnie (nie dotyczy kontaktu telefonicznego) – należy taką osobę wylegitymować w celu potwierdzenia tożsamości i sporządzić notatkę z podpisem wnioskodawcy. Notatka winna być włączona w akta sprawy.

4. Po załatwieniu sprawy komórka organizacyjna przekazuje wniosek i odpowiedź w sprawie, do Inspektora.

Postanowienia końcowe

1. Wszyscy pracownicy są zobowiązani do zapoznania się i przestrzegania zasad określonych w niniejszym dokumencie.
2. Procedury podlegają przeglądowi przynajmniej raz w roku.

Załączniki:

1. Wzór odpowiedzi dotyczącej wydłużenia terminu
2. Wzory odpowiedzi

Załącznik nr 1

Wzór odpowiedzi dotyczącej wydłużenia terminu

Świeradów-Zdrój, dnia .....

Numer sprawy: .....

Data wpływu: .....

Dotyczy: wydłużenia terminu realizacji prawa do .....

Pani/Pan

XYZ

W związku z upływającym w dniu ..... terminem realizacji Pana prawa do ..... informuję, że na podstawie art. 12 ust.3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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, dalej – RODO) powyższy termin zostaje przedłużony o miesiąc/ dwa miesiące, tj. do dnia .....

Powyższe opóźnienie spowodowane jest .....

Załącznik nr 2

Wzór odpowiedzi na wniosek

Świeradów-Zdrój, dnia .....

Numer sprawy: .....

Data wpływu: .....

Dotyczy: realizacji prawa do .....

Pani/Pan

XYZ

Informuję, iż na podstawie art 15-22[1] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Urząd Miasta Świeradów-Zdrój:

przetwarza/nie przetwarza Pana dane osobowe w zakresie ..... zgromadzone w ramach ..... i jednocześnie informuje, że:

1) celem przetwarzania Pani/Pana danych osobowych jest ...;

2) (administrator) przetwarza Pani/Pana dane osobowe w zakresie ... (należy wskazać kategorię danych osobowych);

3) dane osobowe będą ujawniane ... (należy wskazać odbiorcę lub kategorie odbiorców);

4) dane osobowe będą przechowywane przez okres ...;

5) przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;

6) (administrator) uzyskał Pani/Pana dane osobowe z ... (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);

7) (należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

lub

1 Wskazać odpowiednio

/ dokonał/ nie dokonał[2] sprostowania/ usunięcia/ ograniczenia przetwarzania danych, o które Pan wnioskował/ zrealizował/ nie zrealizował prawo do sprzeciwu w zakresie .....

[3]Powyższa decyzja wynika z .....

2 Niewłaściwe skreślić

3 W przypadku odmowy realizacji prawa