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

ZARZĄDZENIE Nr 70/18
Burmistrza Miasta Świeradów-Zdrój
z dnia 12.06.18

Na podstawie art 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Zarządza się, co następuje:

§ 1.

Wprowadza się w Urzędzie Miasta Świeradów-Zdrój dokumentację dotyczącą ochrony danych osobowych, która stanowi załączniki do n/n Zarządzenia.

§ 2.

Każdy pracownik jest obowiązany zapoznać się z treścią załączników zarządzenia.

§ 3.

Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do dokumentacji ochrony danych osobowych.

§ 4.

Pracodawca zobowiązuje wszystkich pracowników do zapoznania się z dokumentacją zawartą w załącznikach do n/n zarządzenia.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia

L.p.	Imię i nazwisko	Zakres kompetencji	Data i podpis	Uwagi
1.	Sylwia Zgierska – Inspektor Ochrony Danych	przygotował	INSPEKTOR OCHRONY DANYCH Sylwia Zgierska	
2.	Diana Timoftiewicz-Żak- insp. ds. obsługi Rady Miasta, Kierownik Referatu Administracyjnego	przegląd	18.06.2018.	
3.	Radca prawny	opinia	20.06.2018 E. Łoyen-cyf	
4.	Skarbnik Gminy	opinia	BURMISTRZ Roland Marciniak	
5.	Burmistrz Miasta	zatwierdził		

Załącznik nr 1

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W

Gminie Miejskiej Świeradów-Zdrój

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Rozdział 1
Postanowienia ogólne

§ 1. Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2) **ustawie** – Ustawa z dnia 10 maja 2018r. O ochronie danych osobowych;
3) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
5) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

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) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **administratorze danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
10) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
11) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
12) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
13) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
14) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
15) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
16) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

17) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
18) **naruszeniu ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Rozdział 2
Administrator danych

§ 2. Administrator danych w szczególności:
1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Prowadzi rejestr czynności przetwarzania.
3. Wyznacza Inspektora Ochrony Danych (IOD).

Rozdział 3
Środki techniczne i organizacyjne

§ 3. W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:
a) przeprowadzono ocenę skutków dla ochrony danych zgodnie,
b) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach,
c) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych;
d) zawarto umowy powierzenia przetwarzania danych,
e) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

§ 4. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:
a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);
b) pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy;
c) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;
d) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie;
e) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie;

f) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy;
g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 5. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
b) dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła;
c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
e) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
f) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
g) użyto system Firewall do ochrony dostępu do sieci komputerowej;

§ 6. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
b) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
c) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
d) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

§ 7. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
e) 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.

Rozdział 4
Procedura DPIA
(Data Protection Impact Assessment)

§ 8. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych.

§ 9. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.

§ 10. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 5
Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 11. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie.

§ 12. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 13. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.

§ 14. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

§ 15. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA.

Rozdział 6
Procedura współpracy z podmiotami zewnętrznymi

§ 16. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych.

§ 17. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.

Rozdział 7
Procedura domyślnej ochrony danych

§ 18. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.

§ 19. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 8
Procedura zarządzania incydentami

§ 20. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 21. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.

§ 22. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 23. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.

Rozdział 8
Procedura realizacji praw osób

§ 24. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

§ 25. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

§ 26. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 27. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 9
Procedura odbierania zgód oraz informowania osób

§ 28. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą o administratorze i jego siedzibie, celu przetwarzania oraz przysługujących mu prawach.

§ 29. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą.

§ 30. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody.

Rozdział 10
Postanowienia końcowe

§ 31. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 32. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

INSPEKTOR
OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 2

ANALIZA ZAGROŻEŃ I RYZYKA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA ŚWIERADÓW-ZDRÓJ

Spis treści

1. Podstawy prawne
2. Wymogi bezpieczeństwa
3. zagrożenia dla systemu
4. Poufność, Rozliczalność i Integralność
5. Stopień ważności informacji
6. Podatność na zagrożenia
7. Analiza zagrożeń i ryzyka
8. podsumowanie

Podstawa prawna dokumentu

Art. 35 ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Wymogi bezpieczeństwa

§1 Celem Urzędu Miasta w Świeradowie-Zdroju jest bezpieczne oraz prawidłowe przetwarzanie danych osobowych zarówno w wersji papierowej, jak i w systemach informatycznych.

§2 Ryzyko strat w wyniku błędy ludzkiego lub niesprawności systemu informatycznego, a także w wyniku czynników zewnętrznych może wpływać na wykonywanie zadań ustawowych Urzędu.

§3 Wszelkie czynności wykonywane na danych osobowych przez pracowników obarczone jest ryzykiem operacyjnym. W ramach tego ryzyka przeprowadzana jest analiza, która obejmuje identyfikację i ocenę zagrożeń związanych z przetwarzaniem poszczególnych kategorii danych. Wszystkie podejmowane działania mają na celu ograniczenie lub wyeliminowanie ryzyka.

§4 Szacowanie ryzyka wykonywana jest przez Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych raz w roku w miesiącu czerwcu lub w ciągu 14 dni od pojawienia się nowych zagrożeń. Wyniki analizy przedstawiane są w ciągu 30 dni od jej przeprowadzenia Administratorowi Danych Osobowych.

§5 Nieakceptowana jest niekompetencja pracowników, nieznajomość prawa, a także świadome działania na rzecz jednostki. Każdy incydent analizowany będzie indywidualnie przez Inspektora Ochrony Danych, a wniosek przedstawiany będzie Administratorowi. Pracodawca ma prawo nałożyć na pracownika karę za niestosowanie się do wprowadzonych zasad.

§6 Dane osobowe przetwarzane w Urzędzie występują w następującej postaci:

- Pliki przechowywane na dysku twardym komputera;
- pliki przechowywane w pamięci operacyjnej komputera;
- pliki zapisywane na nośnikach informacji;
- gotowe dokumenty w wersji papierowej.

§7 Bezpieczeństwo przetwarzanych oraz przechowywanych w Urzędzie danych osobowych wymaga:

- Zapewnienia ochrony fizycznej pomieszczenia;
- zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;

- ochrony nośników informacji i wydrukowanych dokumentów przed nieuprawnionym dostępem;
- zapewnienie dostępności do danych osobowych na nośnikach, w wersji papierowej oraz w systemach informatycznych tylko osobom uprawnionym;
- zapewnienie kontroli nośników, na których znajdują się dane osobowe.

Zagrożenia dla systemu

§8 System informatyczny, który służy do przetwarzania danych osobowych podatny jest na zagrożenia wystąpienia incydentu, który powoduje utratę:

- Poufności - to zapewnienie, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
- rozliczalności - to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- integralności - to zapewnienie, aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu; właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Zagrożenia w zakresie poufności obejmują:

- nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe,
- ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym,
- podgląd/podsłuch danych osobowych,
- naprawa i konserwacja sprzętu na którym przetwarzane są dane przez osoby nieuprawnione.

Zagrożenia w zakresie rozliczalności obejmują:

- brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- brak możliwości identyfikacji użytkownika na stanowisku komputerowym, gdzie przetwarzane są dane,
- nieuprawnione wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,
- błędy oprogramowania lub sprzętu,
- brak rejestracji udostępnień danych.

Zagrożenia w zakresie integralności obejmują:

- nielegalny dostęp danych osobowych, w tym do stanowiska komputerowego,
- czynnik ludzki (błędy, pomyłki),

- brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika,
- wadliwe działanie systemu operacyjnego,
- wirusy,
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych,
- zagrożenia zewnętrzne.

§9 **Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane osobowe mogą być:**

- siły natury – zdarzenia, które nie wynikają z działalności człowieka, tzn. uderzenie pioruna, pożar, starzenie się sprzętu, starzenie się nośników pamięci, smog, kurz, katastrofy budowlane, ulewny deszcz, huragan, ekstremalne temperatury, wilgotność, epidemia,
- ludzie – mogą to być pracownicy lub osoby z zewnątrz, którzy działają w sposób celowy lub przypadkowy; zagrożenia te, to przede wszystkim: błędy i pomyłki użytkowników, błędy i pomyłki administratorów, błędy utrzymania systemu w poufności, integralności i rozliczalności, zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu, zagubienie nośnika zawierającego dane osobowe, niewłaściwe zniszczenie nośnika, nielegalne użycie oprogramowania, choroba ważnych osób i nieuprawnione zastępstwo, epidemia kadry i brak osób upoważnionych do dostępu, podpalenie obiektu, zalanie wodą, katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka, zakłócenia elektromagnetyczne, radiotechniczne, podłożenie i wybuch bomby, ładunku wybuchowego, użycie broni, zmiany napięcia w sieci, utrata prądu, zbieranie się ładunków elektrostatycznych, utrata kluczowych pracowników, niedobór pracowników, defekty oprogramowania, szpiegostwo, terroryzm, wandalizm, destrukcja zbiorów i programów impulsem elektromagnetycznym, kradzież, włamanie do systemu, wyłudzenie, fałszowanie dokumentów, podszycie się pod uprawnionego użytkownika, podsłuch, użycie złośliwego oprogramowania, wykorzystanie promieniowania ujawniającego.

§10 **Każde z ww. zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:**

- rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,
- fizyczne zabezpieczenie obiektu, w którym działa system,
- wdrożenie systemu kontroli użytkowników,
- szkolenia pracowników.

Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowisko komputerowe, na których przetwarza się dane osobowe.

STOPIEŃ WAŻNOŚCI INFORMACJI

§11 Stopień ważności informacji zawierających dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa. W placówce przetwarza się dane osobowe zwykłe oraz wymagające szczególnej ochrony – merytorycznie związane z zakresem obowiązków użytkownika.
Dokładność i kompletność realizowanych czynności w zakresie prowadzonych spraw administracyjnych są zapewnione poprzez odpowiednie usytuowanie stanowisk komputerowych, na których się przetwarza dane osobowe (stanowiska jednoosobowe).

Wytwarzane dokumenty zawierające dane osobowe są rejestrowane, przechowywane do wglądu a następnie niszczone lub archiwizowane przez osoby posiadające stosowne upoważnienie.

PODATNOŚĆ NA ZAGROŻENIA

§12 Podatność na zagrożenia może wynikać z następujących czynników:

- dostępność systemu, która wynika np. z braku ochrony fizycznej pomieszczeń, braku upoważnień do zbiorów danych;
- celowe wprowadzenie luk w sprzęcie i oprogramowaniu, które dają możliwość wprowadzania wirusów;
- awarie sprzętów, wynikające z uszkodzenia, błędów lub celowego działania;
- przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne lub w niezabezpieczonych wiadomościach;

§13 W/w podatność ograniczona została przez:

- ochronę fizyczną pomieszczeń;
- nadanie upoważnień do przetwarzania danych osobowych zbiorach;
- audyty;
- okresowe przeglądy sprzętu komputerowego;
- audyty zgodności przetwarzania;
- zakup sprzętu do zasilania awaryjnego (UPS)
- tworzenie codziennej kopii zapasowej;
- użycie oprogramowania antywirusowego.

ANALIZA ZAGROŻEŃ I RYZYKA

§14 W celu oszacowania potencjalnego ryzyka wykonywana jest analiza, określająca przewidywane zagrożenia dla zasobów, zgodnie z zał. 1. Zidentyfikowane zagrożenia opisane zostały w zał. 2.

§15 W celu oszacowania ryzyka stosowany jest zał. 3. Wyniki przeprowadzonej analizy przekazywane są Administratorowi danych osobowych.

§16 Ryzyko na poziomie średnim określone jest jako akceptowalne. Dla każdego nieakceptowanego poziomu wymagana jest decyzja Administratora, co do zastosowanych rozwiązań. Administrator może akceptować ryzyko, transferować ryzyko przez np. ubezpieczenie oraz podjąć działania mające na celu zmniejszenie ryzyka.

PODSUMOWANIE

§17 Wyniki przeprowadzonej analizy są podstawą do przygotowania stosownej dokumentacji lub zmiany w zapisach obowiązującej dokumentacji. Stanowi również podstawę wniosku o dostosowanie pomieszczeń oraz systemów informatycznych do zachowania bezpieczeństwa przetwarzania danych osobowych.

§18 Termin wykonania kolejnej analizy zagrożeń i ryzyka to czerwiec 2019r.

Załącznik nr 1
do Analizy zagrożeń i ryzyka
przetwarzania danych osobowych
w Urzędzie Miasta Świeradów-Zdrój

PODSTAWOWE ZASADY ANALIZY RYZYKA

1. Należy określić:
   - zasoby/aktywa, które należy chronić,
   - zagrożenia – czynniki mogące spowodować wystąpienie incydentu,
   - prawdopodobieństwo – podatność, słabość zasobu
   - skutki – jaki wpływ na zasoby będzie miał zaistniały incydent
2. Wyjaśnienie podstawowych pojęć:
   - Zasoby/aktywa – wszystkie elementy mające wpływ na przetwarzanie danych osobowych (bezpieczeństwo, przechowywanie, przekazywanie), które podlegają ochronie (sprzęt teleinformatyczny, zasoby ludzkie, aplikacje, pomieszczenia)
   - prawdopodobieństwo – możliwość zaistnienia, wystąpienia zagrożenia z uwagi na słabość zasobów
   - Skutek – wartość strat po zaistnieniu zagrożenia
   - ryzyko – iloczyn wartości skutków i prawdopodobieństwa wystąpienia

Skala poziomu ryzyka 1-100

Wartość	Poziom ryzyka
1-10	Utrata bezpieczeństwa danych osobowych nie istnieje
11-20	Niski poziom utraty bezpieczeństwa danych osobowych
21-50	Średni poziom utraty bezpieczeństwa danych osobowych
51-80	Wysoki poziom utraty bezpieczeństwa danych osobowych
81-100	Maksymalny poziom utraty bezpieczeństwa danych osobowych

Prawdopodobieństwo wystąpienia określonego zagrożenia dla systemu informatycznego

Wartość	Poziom
0-1	Nieprawdopodobne
2-3	Niskie
4-6	Średnie
7-8	Wysokie
9-10	Bardzo wysokie

Skutki utraty zasobów dla atrybutu poufności

Wartość	Poziom ryzyka
1	Utrata poufności nie występuje
2-3	Niski skutek utraty poufności
4-6	Średni skutek utraty poufności
7-8	Wysoki skutek utraty poufności
9-10	Bezwzględny skutek utraty poufności

Załącznik nr 2
do Analizy zagrożeń i ryzyka
przetwarzania danych osobowych
w Urzędzie Miasta Świeradów-Zdrój

Zagrożenia w obszarze przetwarzania danych osobowych
w Urzędzie Miasta w Świeradowie-Zdroju

1. Niedokładne wykonanie kontroli zarządczej w zakresie ochrony danych osobowych.
2. Zagrożenia związane z bezpieczeństwem przetwarzania danych osobowych.
3. Zagrożenia związane z poufnością danych osobowych w systemie informatycznym.
4. Zagrożenia związane z integralnością danych.
5. Zagrożenia związane z rozliczalnością danych.

Skutki utraty zasobów dla atrybutu integralności.

Wartość	Poziom ryzyka
1	Utrata integralności nie występuje
2-3	Niski skutek utraty integralności
4-6	Średni skutek utraty integralności
7-8	Wysoki skutek utraty integralności
9-10	Bezwzględny skutek utratyintegralności

Skutki utraty zasobów dla atrybutu rozliczalności

Wartość	Poziom ryzyka
1	Utrata dostępności nie występuje
2-3	Niski skutek utraty rozliczalności
4-6	Średni skutek utraty rozliczalności
7-8	Wysoki skutek utraty rozliczalności
9-10	Bezwzględny skutek utraty rozliczalności

Prawdopodobieństwo (P)						
	B.wysokie	10	30	60	80	100
	Wysokie	8	24	48	64	80
	Średnie	6	18	36	48	60
	Niskie	3	9	18	24	30
	Brak	1	3	6	8	10
		Utrata nie następuje	Niski stopień utraty	Średni stopień utraty	Duży stopień utraty	Bardzo duży stopień utraty
		Skutki (S)				

Reakcja na ryzyko:

	akceptacja
	Do decyzji ADO
	Brak akceptacji, ADO podejmuje decyzję

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 3

REJESTR CZYNNOŚCI PRZETWARZANIA

(podstawa prawna art. 30 ogólnego rozporządzenia o ochronie danych)

L.p.	Nazwa oraz dane kontaktowe administratora oraz Inspektora Ochrony Danych	Cele przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust.1)
1.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Prowadzenie spraw administracyjnych	Pracownicy, Petenci	GUS, DUW	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zamykane szafy z danymi osobowymi, upoważnienia pracowników, szkolenia pracowników, zabezpieczenie systemów informatycznych
2.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Wymiana korespondencji	Dane osób, których dotyczy korespondencja, petenci	-	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zamykane szafy z danymi osobowymi, upoważnienia pracowników, szkolenia pracowników, zabezpieczenie systemów informatycznych
3.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Ewidencja i naliczanie podatku	Podatnicy	-	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zamykane szafy z danymi osobowymi, upoważnienia pracowników, szkolenia pracowników, zabezpieczenie systemów informatycznych

4.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Prowadzenie księgowości	Petenci, Pracownicy	Komornik Sądowy, ZUS, GUS, Urząd Skarbowy	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zamykane szafy z danymi osobowymi, upoważnienia pracowników, szkolenia pracowników, zabezpieczenie systemów informatycznych
5.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Wykonanie wymogów zawartych w Kodeksie Pracy	Pracownicy	ZUS, Urząd Skarbowy, Komornik Sądowy, Firmy Ubezpieczeniowe, Urząd Gminy	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zabezpieczenia systemów informatycznych, zamykane na klucz szafy metalowe, upoważnienia dla pracowników, szkolenia pracowników
6.	Urząd Miasta Świeradów-Zdrój, ul. 11 Listopada 35, 59-850 Świeradów-Zdrój, reprezentowany przez Burmistrza Rolanda Marciniaka; Inspektor Ochrony Danych – Sylwia Zgierska	Obsługa petenta	Petenci, pracownicy	Urząd Gminy/Miasta, Policja, Firmy zewnętrzne	Nie dotyczy	Do czasu trwania obowiązku ustawowego	Zabezpieczenie systemów informatycznych, zamykane szafy, upoważnienia dla pracowników, szkolenia dla pracowników

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska

	Odnotowywanie w systemie informatycznym informacji o udostępnianiu danych osobowych	Załącznik nr 4

1. Cel

Określenie zasad związanych ze sposobem odnotowywania informacji w systemie informatycznym dotyczących udostępniania danych osobowych.

2. Zakres obowiązywania

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych w systemie informatycznym oraz informatyka.

2. Opis postępowania

1) Dane osobowe udostępnia się osobom lub podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Zgodę na udostępnienie danych wydaje Inspektor Ochrony Danych Osobowych lub ADO.

2) W przypadku, gdy udostępniane są dane osobowe znajdujące się w zbiorach danych przetwarzanych w systemie informatycznym, system ten powinien umożliwić odnotowanie następujących informacji:

a) data udostępnienia;

- osoba lub podmiot, której udostępnia się dane;
- zakres udostępnionych danych;
- podstawa prawna udostępnienia.

3) W przypadku przetwarzania danych w co najmniej dwóch systemach informatycznych, dopuszczalne jest odnotowywanie informacji o których mowa w pkt. 2 w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

INSPEKTOR
OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr **5**

Ewidencja udostępniania danych osobowych

Lp.	Podmiot, któremu udostępniono dane osobowe	Zbiór danych, z którego udostępniono dane	Zakres udostępnienia	Podstawa prawna udostępnienia	Data udostępnienia
1					
2					
3					
4					
5					
6					
7					
8					

INSPEKTOR
OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 6

Cel

Określenie zasad dotyczących postępowania zapewniającego bezpieczeństwo danych osobowych w systemie informatycznym.

Zakres obowiązywania

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym.

Opis postępowania

1) Stosowane są następujące zasady rozpoczęcia pracy w systemie informatycznym:

a) Przed przystąpieniem do pracy, użytkownik zobowiązany jest do sprawdzenia czy stacja robocza wykorzystywana do przetwarzania danych osobowych w systemie informatycznym nie wskazuje na ingerencję osób trzecich, a także czy stanowisko pracy zastano w takim stanie jak pozostawiono po zakończeniu pracy.

b) Przed uruchomieniem stacji roboczej, użytkownik zobowiązany jest do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądnięcie jego zawartości.

c) Każde rozpoczęcie pracy w danym systemie wymaga logowania.

d) W trakcie pracy, użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.

e) W trakcie pracy, użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych.

2) Stosowane są następujące zasady zawieszenia pracy w systemie informatycznym:

a) W przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane.

b) W przypadku opuszczenia stanowiska pracy materiały zawierające dane wymagające ochrony powinny być zabezpieczane przed dostępem osób nieuprawnionych.

c) W przypadku bezczynności użytkownika trwającego dłużej niż 10 min, uruchamiany jest automatycznie wygaszacz ekranu. Wznowienie pracy możliwe jest po ponownym uwierzytelnieniu się poprzez podanie własnego hasła.

3) Stosowane są następujące zasady zakończenia pracy w systemie informatycznym:

1. Po zakończeniu pracy należy wylogować się z systemu.
2. Po zakończeniu dnia pracy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających dane osobowe, w celu uniemożliwienia dostępu do nich osób nieupoważnionych. Należy uprzątnąć z miejsca pracy wszelkie dokumenty, nośniki, notatki i umieścić je w miejscu niedostępnym dla osób nieupoważnionych.

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 7

EWIDENCJA HASEŁ

.....

(nazwa administratora)

Nazwa systemu / Rodzaj hasła	Hasło	Data utworzenia	Osoba, której przypisano hasło	Podpis administratora

INSPEKTOR
OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 8

PROCEDURA

Zarzadzania incydentami

Incydentem będzie każde działanie niezgodne z wewnętrznymi procedurami bezpieczeństwa, czyli nie tylko sam wyciek danych osobowych czy też ich utrata, le również wszelkie zagrożenia w stosunku do danych osobowych, jak np. postepowanie przez użytkownika niezgodnie z procedurami bezpieczeństwa.

Przykładowy katalog zdarzeń, które stanowią incydent ochrony danych osobowych.

- pozostawienie dokumentu z danymi osobowymi z możliwością dostępu osób nieuprawnionych;
- pozostawionego bez opieki włączonego komputera PC lub laptopa;
- udostępnienie innej osobie swojego loginu i hasła do programu komputerowego z danymi osobowymi;
- przetwarzanie danych osobowych na prywatnych - zewnętrznych dyskach przenośnych;
- przesyłanie niezabezpieczonych (nieszyfrowanych) danych osobowych pocztą elektroniczną;
- przesyłanie specjalnych danych osobowych pocztą w zwykłej kopercie (winny być zabezpieczone w kopercie tzw. bezpiecznej);
- ustawienie ekranu komputerowego w sposób umożliwiający odczyt cudzych danych osobowych przez interesanta;
- ujawnienie dostępu do danych osobowych osoby nieuprawnionej

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska

Załącznik nr 9

Rejestr incydentów i zdarzeń

Lp.	Incydent lub zdarzenie	Źródło zgłoszenia	Data zgłoszenia	Przyczyna niezgodności	Działania korygujące i zapobiegawcze	Odpowiedzialny za realizację	Data zakończenia	Ocena skuteczności
1	2	3	4	5	6	7	8	9

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska

Załącznik 10

Świeradów-Zdrój, ...

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** niniejszym upoważniam do przetwarzania danych osobowych:

.....

w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Okres ważności upoważnienia:

od: .....

Do: ustania stosunku pracy

_____ _____

((podpis osoby upoważnionej) *(podpis osoby nadającej upoważnienie)*

Ja niżej podpisany/a zobowiązuję się do przestrzegania zasad panujących w w/w podmiocie w zakresie ochrony danych osobowych, a w szczególności **„Polityki Bezpieczeństwa"** i **„Instrukcji Zarządzania Systemem Informatycznym"** oraz respektowania zapisów RODO oraz Ustawy z dnia 10 maja 2018r. O ochronie danych osobowych. Zobowiązuję się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w w/w podmiocie oraz sposobów zabezpieczeń, a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie odpowiedzialności karnej za nie przestrzeganie przepisów ochrony danych osobowych. Niezależnie od odpowiedzialności przewidzianej przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną

.....

(data i podpis pracownika)

INSPEKTOR OCHRONY DANYCH
Sylwia Zgierska