BURMISTRZ MIASTA
JEDLINA-ZDRÓJ

ZARZĄDZENIE NR 84/2018
BURMISTRZA MIASTA JEDLINA-ZDRÓJ

z dnia 31 grudnia 2018 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Miasta w Jedlinie-Zdroju

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2018 r., poz. 994 z późn. zm.), art. 24 ust. 2 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, dalej też zwane RODO), ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 z późn. zm.) Burmistrz Miasta Jedlina-Zdrój zarządza, co następuje:

§ 1. Wprowadza się do użytku i stosowania Politykę Ochrony Danych Osobowych Urzędu Miasta Jedlina-Zdrój, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Miasta Jedlina-Zdrój oraz osoby odbywające staż w Urzędzie do stosowania i przestrzegania niniejszej Polityki.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Miasta Jedlina-Zdrój.

§ 4. Traci moc zarządzenie nr 15/2012 z dnia 14 marca 2012 r. w sprawie wprowadzenie Polityki Bezpieczeństwa danych osobowych w Urzędzie Miasta w Jedlinie-Zdroju oraz zarządzenie nr 14/2012 z dnia 14 marca 2012 r. w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta w Jedlinie-Zdroju.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ MIASTA
Jedlina-Zdrój
Leszek Orpel

Nie wnoszę uwag pod względem
formalno-prawnym
data: 31.12.2018r.

adwokat
dr Agnieszka Skorupka

Złącznik Nr 1

do Zarządzenia Nr 84/2018

Burmistrza Miasta Jedlina-Zdrój

z dnia 31 grudnia 2018r.

POLITYKA OCHRONY DANYCH OSOBOWYCH URZĘDU MIASTA JEDLINA-ZDRÓJ

ZATWIERDZAM

BURMISTRZ MIASTA
Jedlina-Zdrój
Leszek Orpel

.....

(data i podpis Administratora Danych)

I. POSTANOWIENIA OGÓLNE

§1

Deklaracja i zastosowanie

1. **Celem** niniejszej Polityki ochrony danych osobowych (PODO) jest wypełnienie założeń 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, dalej też zwane RODO).
2. Niniejsza Polityka stanowi zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administratora danych osobowych**, którym jest Burmistrz Miasta Jedlina-Zdrój, (dalej jako Administrator).
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (PODO lub Polityka), obowiązują wszystkich pracowników Urzędu Miasta Jedlina-Zdrój.
4. Procedury i dokumenty związane z Polityką są weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
5. Polityka określa środki techniczne i organizacyjne zastosowane przez Administratora dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
6. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
7. Zakres obowiązywania dokumentu:

a. Niniejsza Polityka obowiązuje wszystkich pracowników Urzędu Miasta Jedlina-Zdrój.

b. Każdy z pracowników Urzędu Miasta Jedlina-Zdrój ma obowiązek zapoznania się z treścią niniejszej Polityki.

c. Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej i papierowej.

d. Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.

8. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator, a za nadzór i monitorowanie jej przestrzegania odpowiada: ***Inspektor ochrony danych (dalej IOD).***

9. Politykę ochrony danych opracowano na podstawie:

a. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

b. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 z późn. zm.).

c. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

d. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247).

§ 2

Określenia użyte w polityce

1. **U.M. Jedlina-Zdrój** oznacza Urząd Miasta Jedlina-Zdrój;

2. **Administrator danych osobowych** - „Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; **Administratorem jest Burmistrz Miasta Jedlina-Zdrój** (dalej jako **Administrator**);

3. **Administrator Systemu Informatycznego (ASI)** – rozumie się przez to osobę odpowiedzialną za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora Danych, wyznaczoną przez Administratora;

4. **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

5. **dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6. **dane szczególne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

7. **eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;

8. **hasło** – rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;

9. **identyfikator** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

10. **incydent ochrony danych osobowych** – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;

11. **Inspektor ochrony danych (IOD)** – osoba sprawująca nadzór nad przestrzeganiem zasad ochrony danych osobowych wyznaczona przez Administratora;

12. **naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13. **obszar przetwarzania danych** – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione; obszar przetwarzania danych opisany jest w **załączniku nr 10** do niniejszej Polityki;

14. **odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

15. **osoba, podmiot danych** - oznacza osobę, której dane dotyczą;

16. **podmiot przetwarzający** - oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych (np. usługodawca IT, dostawca ESOK czy innego systemu informatycznego);

17. **polityka** oznacza niniejszą politykę ochrony danych osobowych;

18. **postępowanie z ryzykiem** – proces planowania i wdrażania działań wpływających na ryzyko;

19. **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

20. **raport** – rozumie się przez to przygotowanie przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

21. **RCPDO lub rejestr** oznacza rejestr czynności przetwarzania danych osobowych;

22. **RODO** oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych) (dz.urz. UE l 119, s. 1).

23. **ryzyko** – niepewność osiągnięcia zamierzonych celów;

24. **serwisant** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

25. **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

26. **szacowanie ryzyka** – proces identyfikowania, analizowania i oceniania ryzyka;

27. **Teczka ODO** – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez IOD.

28. **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

29. **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

30. **użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

31. **zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3

Zasady ochrony danych

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:

a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

b. rzetelnie i uczciwie (rzetelność);

c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

d. w konkretnych celach i nie „na zapas" (minimalizacja);

e. nie więcej niż potrzeba (adekwatność);

f. z dbałością o prawidłowość danych (prawidłowość);

g. nie dłużej niż potrzeba (czasowość);

h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

Podstawy prawne

1. Dane osobowe przetwarzane są w Urzędzie Miasta Jedlina-Zdrój wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

2. W przypadku, gdy podstawą przetwarzania jest zgoda osoby, której dane dotyczą, administrator ewidencjonuje oświadczenia o wyrażeniu zgody, aby być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

3. W przypadku podstawy przetwarzania określonej w ust. 1 lit. c i e musi ona wynikać z przepisu prawa.

§ 5

Cel ochrony danych osobowych i strategie bezpieczeństwa

1. Ochrona danych osobowych w Urzędzie Miasta Jedlina-Zdrój realizowana jest poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

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

a. **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

b. **integralność** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

c. **poufność** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

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

e. **dostępność** – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.

f. **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;

g. **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana;

3. Cele i strategie bezpieczeństwa:

a. zgodność z prawem,

b. ochrona zasobów informacyjnych i innych aktywów,

c. uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,

d. zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty,

e. zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

II. ZAKRES ODPOWIEDZIALNOŚCI

§ 6

Administrator danych osobowych

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

3. Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. *Procedura zarządzania ryzykiem* stanowi załącznik nr 8 do niniejszej

Polityki.

4. We wszystkich umowach, które mogą dotyczyć przetwarzania danych, Administrator uwzględnia zapisy zobowiązujące drugą stronę do przestrzegania art. 28 RODO oraz obowiązujących przepisów krajowych.

5. Administrator stosuje środki techniczne oraz organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

6. Administrator prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz sposób ich zabezpieczenia, w szczególności w postaci polityk, procedur, wytycznych oraz formularzy.

7. Administrator dopuszcza do przetwarzania danych osobowych jedynie osoby upoważnione przez administratora, które złożyły oświadczenie o zachowaniu danych oraz sposobu ich zabezpieczeń w poufności.

8. Administrator prowadzi rejestr osób upoważnionych oraz przechowuje treść oświadczeń, o których mowa w ust. 7.

§ 7
Inspektor Ochrony Danych

1. Inspektor ochrony danych jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO, zgodnie z zapisami Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 ze zm.).

2. Do zadań Inspektora Ochrony Danych należy:

a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów i doradzanie im w tej sprawie,

b. monitorowanie przestrzegania RODO, innych przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c. współpraca z organem nadzorczym;

d. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

3. Status inspektora ochrony danych.

a. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie

włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

b. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby i przedsięwzięcia niezbędne do utrzymania właściwego poziomu oraz aktualizacji jego wiedzy fachowej;

c. Administrator zapewnia, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor ochrony danych bezpośrednio podlega Administratorowi;

d. osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;

e. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań;

f. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

§ 8.

Administrator Systemu Informatycznego

1. Administrator Systemu Informatycznego odpowiedzialny jest za:

a. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,

b. optymalizację wydajności systemu informatycznego, baz danych,

c. instalację i konfigurację sprzętu sieciowego i serwerowego,

d. instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania baz danych,

e. konfigurację i administrację oprogramowaniem systemowym sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,

f. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

g. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,

h. zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

i. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

j. przyznawanie na wniosek Administratora danych ściśle określonych praw dostępu do informacji w danym systemie,

k. wnioskowanie do Administratora danych w sprawie procedur bezpieczeństwa i standardów

zabezpieczeń,

l. zarządzanie licencjami i procedurami ich dotyczącymi,

m. prowadzenie profilaktyki antywirusowej.

§ 9.

Kierownicy komórek organizacyjnych oraz pracownicy

1. Każdy kierownik komórki organizacyjnej Urzędu Miasta Jedlina-Zdrój, w której przetwarzane są dane osobowe, odpowiedzialny jest za:

a. Zapewnienie, aby bieżące przetwarzanie danych osobowych było zgodne z powszechnie obowiązującymi przepisami prawa i aktami wewnętrznymi, w szczególności niniejszą Polityką;

b. współdziałanie z Inspektorem Ochrony Danych w zakresie zapewnienia przestrzegania ochrony danych osobowych;

c. występowanie z wnioskiem o nadanie lub odebranie uprawnień do przetwarzania danych osobowych, w tym do ich przetwarzania w systemie informatycznym, jeżeli dane przetwarzane są w formie elektronicznej,

d. zgłaszanie Inspektorowi ochrony danych zamiaru tworzenia, modyfikacji lub likwidacji zbioru, za który jest odpowiedzialny;

e. zgłaszanie Inspektorowi ochrony danych oraz Administratorowi zdarzeń zagrażających bezpieczeństwu danych osobowych.

2. Każdy pracownik Urzędu Miasta Jedlina-Zdrój obowiązany jest:

a. zapoznać się oraz stosować postanowienia niniejszej Polityki ochrony danych osobowych;

b. zapoznać się z obowiązującymi przepisami w zakresie ochrony danych osobowych;

c. zachować w tajemnicy wszelkie dane osobowe, które pozyskał w trakcie wykonywania obowiązków pracowniczych;

d. przestrzegać stosowanych przez Urzędu Miasta Jedlina-Zdrój środków oraz sposobów zabezpieczenia danych osobowych;

e. dbać o bezpieczeństwo danych osobowych, do których ma dostęp.

3. Obowiązek zachowania w tajemnicy danych osobowych, które pracownik pozyskał w trakcie zatrudnienia Urzędu Miasta Jedlina-Zdrój, nie gaśnie wraz z rozwiązaniem stosunku pracy.

4. Nowozatrudniony pracownik przed przystąpieniem do pracy, odbywa szkolenie z zakresu ochrony danych. Szkolenie przeprowadzane jest przez IOD. Potwierdzeniem odbycia szkolenia jest oświadczenie podpisane przez pracownika oraz IOD.

5. Wzór oświadczenia pracownika stanowi Załącznik nr 5 do Polityki i jest aktualizowany przez Inspektora ochrony danych, bez konieczności zmiany Polityki.

III. REJESTR CZYNNOŚCI PRZETWARZANIA

§ 10.

1. Administrator prowadzi rejestr czynności przetwarzania. Rejestr ten prowadzony jest w formie elektronicznej i papierowej.

2. Rejestr czynności przetwarzania zawiera:

a. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także przedstawiciela administratora oraz inspektora ochrony danych (jeżeli dotyczy);

b. nazwę czynności przetwarzania,

c. określenie komórki organizacyjnej, w której przetwarzane są dane osobowe,

d. określenie celu przetwarzania;

e. opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;

f. wskazanie kategorii przetwarzanych danych

g. określenie podstawy prawnej przetwarzania,

h. określenie źródła danych,

i. wskazanie planowanego terminu usunięcia danych,

j. nazwę i dane kontaktowe współadministratorów,

k. nazwę i dane kontaktowe podmiotu przetwarzającego,

l. opis kategorii odbiorców, który dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach poza Unią Europejską lub w organizacjach międzynarodowych (innych niż podmiot przetwarzający);

m. nazwę systemu lub oprogramowania,

n. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

o. wskazanie lokalizacji raportu – jeżeli wymagane jest przeprowadzenie DPIA

p. jeżeli dane przekazywane są do państw poza Unię Europejską lub do organizacji międzynarodowych - nazwę tego państwa lub organizacji oraz dokumentację odpowiednich zabezpieczeń;

q. Rejestr czynności przetwarzania jest na bieżąco aktualizowany i udostępniany przez administratora na każde żądanie Urzędu Ochrony Danych Osobowych.

3. Rejestr czynności przetwarzania w Urzędzie Miasta Jedlina-Zdrój stanowi załącznik nr 1

IV. OCENA SKUTKÓW DLA PRZETWARZANIA DANYCH

§ 11.

1. Administrator dokonuje oceny skutków dla ochrony danych i dokumentuje fakt dokonania tej oceny w przypadkach, kiedy zaistnieje, któraś z przesłanek określonych w ust. 2 i 3.

2. Wykonanie oceny skutków dla ochrony danych jest konieczne, jeżeli dany rodzaj

przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób których dane dotyczą. Dla podobnych operacji przetwarzania wiążących się z podobnym wysokim ryzykiem ocena skutków dla ochrony danych wykonywana jest pojedynczo.

3. Wykonanie oceny skutków dla ochrony danych osobowych wymagana w szczególności:

a. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO lub

b. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

4. Administrator monitoruje wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych opublikowany przez Urząd Ochrony Danych Osobowych i dokonuje oceny skutków czynności przetwarzania wskazanych w tym wykazie jako rekomendowanych do poddania tej ocenie.

5. Ocena skutków dla ochrony danych osobowych zawiera co najmniej:

a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;

b. ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celu, w jakim dane zostały pozyskane;

c. ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;

d. środki planowane w celu minimalizacji ryzyka, w tym zabezpieczenia, środki i mechanizmy bezpieczeństwa zapewniające ochronę danych oraz wykazanie przestrzegania przepisów Rozporządzenia.

6. Administrator dokonuje bieżącego przeglądu czynności przetwarzania, celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych osobowych.

7. Administrator konsultuje się z Urzędem Ochrony Danych Osobowych, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw i wolności pacjentów, jeżeli nie zastosowane zostałyby środki mitygujące ryzyko. Konsultacje z UODO dokonywane są przed rozpoczęciem przetwarzania danych osobowych.

V. POWIERZANIE DANYCH OSOBOWYCH PODMIOTOM ZEWNĘTRZNYM

§ 12.

1. Administrator może korzystać z usług podmiotów zewnętrznych w celu wspierania administratora w jego bieżącej działalności, w szczególności polegających na dostarczeniu oraz/lub utrzymaniu infrastruktury teleinformatycznej, w tym narzędzi wspierających

administratora w prowadzeniu dokumentacji w formie elektronicznej.

2. Administrator korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych osobowych i zgodności przetwarzania danych z przepisami Rozporządzenia.

3. Administrator zawiera z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym, w której określone zostają obowiązki podmiotu przetwarzającego wynikające z faktu powierzenia. Wzór umowy powierzenia przetwarzania oraz wzór zapisów do wprowadzenia do umowy „głównej" stanowią załącznik odpowiednio nr 8

4. W przypadku przekazywania danych do państw poza teren Unii Europejskiej, administrator spełnia dodatkowe warunki, o których mowa w RODO.

5. Administrator prowadzi Rejestr podmiotów zewnętrznych z którymi zawarł umowy powierzenia.

VI. PRAWA PODMIOTÓW DANYCH

§ 13.

1. Administrator wypełnia obowiązki informacyjne wobec osób których dane przetwarza, zgodnie z art. 13 i 14 RODO.

2. Każdej osobie, której dane osobowe są przetwarzane w Urzędzie Miasta Jedlina-Zdrój przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

a. uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;

b. uzyskania informacji o celu, podstawie prawnej, zakresie i sposobie przetwarzania danych osobowych;

c. uzyskania informacji, od kiedy są przetwarzane jej dane osobowe oraz podania w powszechnie zrozumiałej formie treści tych danych;

d. uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;

e. uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;

f. żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane

3. Polityka wypełniania obowiązku informacyjnego, sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą opisane są w załączniku nr 6 do niniejszej Polityki.

VII. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH ORAZ SPOSÓB POSTĘPOWANIA Z NARUSZENIAMI

§ 14

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania.

§ 15

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

a. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,

b. niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura,

c. awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

d. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

e. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

f. nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,

g. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

h. nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

i. ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,

j. praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od

założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,

k. ujawniono istnienie nieautoryzowanych kont dostępu do danych,

l. podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

m. naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 16

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

§ 17

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia – Procedura zgłaszania naruszeń stanowi **załącznik nr 7** do niniejszej Polityki.

VIII. UDOSTĘPNIANIE DANYCH

§ 18

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. 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.
4. 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 celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.
5. Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych i powinno zostać odnotowane w rejestrze udostępnień. Rejestr stanowi załącznik nr 9.

IX. ŚRODKI TECHNICZNE I ORGANIZACYJNE STOSOWANE DO ZAPEWNIENIA ROZLICZALNOŚCI, INTEGRALNOŚCI, POUFNOŚCI, INTEGRALNOŚCI SYSTEMU, DOSTĘPNOŚCI, UWIERZYTELNIANIA I AUTENTYCZNOŚCI

§ 19

Ochrona fizyczna

1. Budynki, w których mieści się Urząd Miasta Jedlina-Zdrój, w których przetwarzane są dane osobowe są zamykane na klucz po zakończeniu pracy. Budynki są dozorowane system alarmowy monitorowany przez firmę ochroniarską.

2. Serwerownie zlokalizowane są w pomieszczeniach zamykanych i klimatyzowanych do których dostęp ma Administrator systemu informatycznego. Przebywanie w pomieszczeniach w których znajduje się serwerownia osób nieuprawnionych (np.: personel sprzątający, serwisant) dopuszczalne jest tylko w obecności Administratora systemu informatycznego albo osoby przez niego upoważnionej.

3. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych jest dopuszczone tylko w obecności osoby upoważnionej do przetwarzania danych.

4. Pomieszczenia w których przetwarzane są dane osobowe są zamykane na czas nieobecności w nich osób upoważnionych, aby uniemożliwić do nich dostęp osób nieuprawnionych.

5. W przypadku przebywania w pomieszczeniu, w którym przetwarzane są dane osobowe osób postronnych ekran monitora należy ustawić w taki sposób, aby uniemożliwić wgląd w dane.

§ 20

Ochrona organizacyjna

1. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki organizacyjne:**

a. Administrator danych przyznaje uprawnienia dostępu do przetwarzania danych osobowych w formie pisemnego upoważnienia. Wzór upoważnienia stanowi załącznik nr 3.

b. Administrator prowadzi ewidencję osób upoważnionych.

c. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy muszą przejść obowiązkowe szkolenie z zakresu obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz zostać poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych.

d. Szkolenie przeprowadza Inspektor Ochrony Danych.

e. Potwierdzeniem udziału w szkoleniu jest Karta szkolenia, podpisana przez pracownika i Inspektora ochrony danych.

f. Karta szkolenia wpinana jest do teczki akt osobowych

g. Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu

wszelkich nośników z danymi.

h. Należy chronić dane przed wszelkim dostępem do nich osób nieuprawnionych.

i. Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.

j. Dostęp do kluczy posiadają tylko upoważnieni pracownicy.

k. Klucze pobierane są z Biura Obsługi Klienta w budynku Urzędu. Po zakończeniu pracy klucze zdawane są w Biurze Obsługi Klienta.

l. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W przypadku, gdy dostęp do pomieszczenia jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora lub bezpośredniego przełożonego.

m. Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.

n. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

o. Szafy w których przechowywane są dane są zamykane na klucz.

p. Klucze do tych szaf posiadają tylko upoważnieni pracownicy.

q. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.

r. Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki techniczne:**

a. Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.

b. Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.

c. Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.

d. W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. Nie należy udostępniać osobom nieupoważnionym tych komputerów.

e. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.

f. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.

g. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.

h. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

i. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

j. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

X. BEZPIECZENSTWO TELEINFORMATYCZNE

§ 21

Wykorzystywanie zasobów

1. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami Polityki

2. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków.

3. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Systemu Informatycznego (ASI).

4. Zakazane jest bez zgody ASI:

a. użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,

b. użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,

c. użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,

d. użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,

e. wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.

5. Wykorzystanie należących do Administratora danych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą Administratora.

6. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia

przez osoby lub czynniki środowiskowe.

7. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą ADO.

8. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.

9. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.

10. Pracownicy zobowiązani są stosować zasadę czystego biurka - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach.

11. Pracownicy zobowiązani są przestrzegać zasady czystego ekranu, która została określona w części Polityki dot. „SPOSOBÓW POSTĘPOWANIA Z DOKUMENTACJĄ ELEKTRONICZNĄ"

12. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.

13. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego przechowywane są przez Administratora.

§ 22

Metody i środki uwierzytelnienia i autoryzacji oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Zasady ogólne uwierzytelniania i autoryzacji w systemie

a. W systemach komputerowych wspomagających czynności merytoryczne, a w szczególności przetwarzających dane osobowe, użytkownicy podlegają uwierzytelnieniu za pomocą identyfikatora użytkownika i autoryzacji za pomocą hasła.

b. Przy opuszczeniu stanowiska pracy należy zablokować system kombinacją klawiszy [Windows]+[L]

c. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wylogować się z systemu.

d. Przed wyłączaniem komputera należy bezwzględnie:

- Zakończyć pracę uruchomionych programów,
- Wykonać zakończenie systemu połączone z wylogowywaniem,

e. Niedopuszczalne jest wyłączanie komputera bez zamknięcia wszystkich użytkowanych programów i wylogowania się z systemu.

2. **Zasady nadawania identyfikatora**

a. Identyfikator użytkownika jest unikalny w obrębie systemu, w którym jest stosowany.

b. Identyfikator jest konstruowany z pierwszej litery imienia i nazwiska.

c. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

3. **Zasady zarządzania hasłami**

a. W systemach umożliwiających samodzielną zmianę haseł przez użytkowników, hasło powinno być zmienione przy pierwszym logowaniu do systemu.

b. Hasło użytkownika jest poufne, jest własnością użytkownika i zna je tylko dany użytkownik. Zabronione jest przekazywanie hasła innym lub w jakikolwiek sposób narażanie na poznanie hasła przez osoby postronne.

c. Za zachowanie poufności swoich haseł odpowiedzialni są użytkownicy.

d. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

e. Dla haseł grupowych użytkownik nie ma prawa udostępniania haseł danej grupy osobom spoza grupy, dla której zostały one utworzone.

f. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

g. W sytuacji, gdy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

h. Przy wyborze hasła obowiązują zasady:

1. minimalna długość hasła – 8 znaków,

2. zakazuje się stosować:

- haseł, które użytkownik stosował uprzednio w okresie minionego roku,
- swojej nazwy użytkownika w jakiejkolwiek formie,
- swojego imienia, drugiego imienia, nazwiska, imion osób z najbliższej rodziny, w jakiejkolwiek formie,
- ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracji samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje,
- przewidzianych w sekwencji znaków klawiatury QWERTY, 12345678, itp.

3. należy stosować:

- hasła zawierające kombinację dużych i małych liter,
- hasła zawierające znaki specjalne,
- hasła, które łatwo zapamiętać,
- hasła szybkie do wprowadzenia,

a. Zmiany hasła nie wolno zlecać innym osobom,

b. Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora w

zamkniętej kopercie w metalowej szafie zamykanej na klucz.

c. W przypadku systemów uwierzytelniających za pomocą kart kryptograficznych piny do kart nie mogą być nigdzie zapisywane, a w szczególności nie na kartach lub w ich pobliżu.

d. Karty z kodami PUK pozwalającymi na zmianę PIN kart kryptograficznych winny być przechowywane oddzielnie od odpowiadających im kart kryptograficznych.

4. Zasady nadawania uprawnień w systemie informatycznym

a. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.

b. Nowe konto dla użytkownika zakładane jest przez Administratora systemu na podstawie *Wniosku o nadanie/zmianę uprawnień do pracy w systemie*, podpisanego przez przełożonego pracownika

c. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać się na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:

- wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe,
- wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego, autoryzacji przyznania praw dostępu do systemów informatycznych.

5. Zasady wyrejestrowywania użytkownika z systemu informatycznego

a. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek Kierownika komórki organizacyjnej, w której był zatrudniony pracownik.

b. Wyrejestrowanie może mieć charakter czasowy, trwały lub automatyczny.

c. Wyrejestrowanie następuje poprzez:

- nieobecność użytkownika w pracy, przez okres dłuższy niż 90 dni,
- rozwiązanie stosunku pracy,
- wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych
- incydentu bezpieczeństwa z udziałem konta nieobecnego w danej chwili użytkownika systemu informatycznego.

a. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

6. Zarządzanie uprawnieniami.

a. Nowy użytkownik systemu może dostać uprawnienia do systemu komputerowego po:

- otrzymaniu upoważnienia do przetwarzania danych osobowych,

- odbyciu szkolenia w zakresie ochrony danych osobowych,
- zapoznaniu się z niniejszą Polityką i potwierdzeniem tego faktu poprzez złożenie oświadczenia stanowiącego załącznik nr 2 do Polityki

b. Użytkownik systemu nie może uruchamiać innego oprogramowania niż zainstalowane przez Administratora systemu i do którego ma przyznane uprawnienia. Nie może samodzielnie instalować oprogramowania i w jakikolwiek sposób obchodzić zabezpieczenia uniemożliwiające instalację lub uruchomienie innego oprogramowania.

c. Administrator systemu ma dostęp do całości systemu informatycznego, w tym uprawnienia do nadawania i odbierania uprawnień, zakładania kont użytkowników, zakładania i zmiany haseł.

d. Użytkownik systemu może mieć dostęp tylko do tych zasobów sieci informatycznej Urzędu Miasta Jedlina-Zdrój do której posiada przyznane przez Administratora systemu uprawnienia.

e. Zmiany uprawnień dokonuje się każdorazowo na wniosek przełożonego użytkownika poprzez złożenie Wniosku o nadanie/zmianę uprawnień do pracy w systemie.

f. Osoby trzecie wykonujące zadanie w sieci Urzędu Miasta Jedlina-Zdrój muszą każdorazowo uzyskać pozwolenie ADO. Praca ta musi przebiegać pod nadzorem Administratora systemu.

g. Każde oprogramowanie konieczne do uruchomienia lub instalacji przez osoby trzecie musi być sprawdzone i zatwierdzone przez Administratora systemu.

§ 23

Tworzenie kopii zapasowych

1. Konfiguracja programów użytkowych powinna zapewnić przechowywanie zbiorów danych na wydzielonym zasobie serwera.
2. Serwer zapewnia automatyczną całościową archiwizację danych w cyklu codziennym lub z odstępem parudniowym w zależności od częstości wprowadzania danych.
3. Czasookres przechowywania kopii zapasowych na zasobach pamięci dyskowej wynosi nie mniej niż pół roku.
4. Każda kopia jest zachowywana z odnotowaniem daty i godziny powstania jako części jej nazwy.
5. Do utworzenia kopii używane są narzędzia przewidziane w serwerach baz danych (SQL Serwer) oraz program do archiwizacji.
6. Nad poprawnością funkcjonowania systemu archiwizacji czuwa ASI.
7. Kopie awaryjne tworzone doraźnie należy usuwać bezzwłocznie po ustaniu ich użyteczności.

§ 24

Ochrona systemu przed wirusami i złośliwym oprogramowaniem

Środki ochrony systemu przed wirusami i innym złośliwym oprogramowaniem

1. Na każdym stanowisku komputerowym zainstalowane jest oprogramowanie antywirusowe wychwytujące wirusy jak i inne złośliwe oprogramowanie.
2. Każda odbierana wiadomość przychodząca drogą elektroniczną (jak i załączniki) jest sprawdzana oprogramowaniem antywirusowym.
3. Każdy nośnik wymienny musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który korzysta z nośnika.
4. Zabrania się pobierania z internetu plików niewiadomego pochodzenia. Każdy plik pobrany z internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
5. W przypadku wykrycia wirusów komputerowych sprawdzane jest:

a. stanowisko komputerowe na którym wykryto wirus,

b. wszystkie nośniki wymienne posiadane przez użytkownika pracującego na stanowisku komputerowym

c. komputery wszystkich osób logujących się na danej stacji.

d. zasoby i użytkownicy wspólnych grup dzielących zasoby.

§ 25

Sposoby postępowania z dokumentacją elektroniczną

1. **Zasady przechowywania dokumentów elektronicznych**

a. Podczas logowania tworzony jest na pulpicie skrót do zasobu wspólnego właściwego dla danej komórki organizacyjnej lub stanowiska.

b. Wszystkie dokumenty elektroniczne danej komórki należy przechowywać na zasobach wspólnych lub w systemie Elektronicznego Obiegu Dokumentów.

c. Przydział uprawnień do czynności wykonywanych na wspólnych zasobach dokonuje się za pomocą Wniosku o nadanie/zmianę uprawnień do pracy w systemie

2. **Zasada „Czystego ekranu"**

a. Dokumenty elektroniczne powinny być przechowywane w sposób zapewniający ich bezpieczeństwo.

b. Dokumenty zawierające dane poufne lub osobowe powinny być wyświetlane na monitorze w sposób uniemożliwiający ich odczyt przez osoby nieuprawnione.

c. Po zakończeniu pracy na pulpicie oraz w folderach umieszczonych na nim nie wolno przechowywać żadnych dokumentów.

d. Dokumenty wolno przechowywać na pulpicie tylko podczas bezpośredniej edycji. Po zakończeniu pracy muszą zostać przeniesione na zasób wspólny, a z pulpitu usunięte.

§ 26

Sposoby postępowania z nośnikami mobilnymi i zasady użytkowania komputerów przenośnych

1. **Rodzaje nośników mobilnych**

Do nośników mobilnych zalicza się: płyty CD, DVD, Bluray, taśmy streamerów, masowe urządzenia magazynujące podłączane pod port USB, FireWire lub inny port wymiany danych komputera, pamięć wewnętrzna komputerów przenośnych, i innych urządzeń taką pamięć posiadających w tym: odtwarzacze mp3, mp4, palmtopy, telefony komórkowe, smartfony, nawigacje satelitarne.

2. **Zasady użytkowania nośników mobilnych**

a. Uprawnienia do użytkowania nośników mobilnych nadawane są za pomocą Wniosku o nadanie/zmianę uprawnień do pracy w systemie.

b. Nośniki USB są imiennie rejestrowane i tylko takie nośniki mogą być skutecznie użytkowane.

c. Rejestr użytkowników posiadających uprawnienia do przechowywania danych na nośnikach mobilnych prowadzi IOD.

d. Nośniki mobilne muszą być trwale oznaczone:

- Środki trwałe posiadające wbudowane nośniki mobilne powinny być oznaczone etykietą zgodnie z oznaczeniami stosowanymi w Urzędzie Miasta Jedlina-Zdrój,
- Inne nośniki powinny być oznaczone pieczątką Urzędu Miasta Jedlina-Zdrój lub niezmazywanym markerem „Urzędu Miasta Jedlina-Zdrój"

a. Nie wolno dokonywać zapisu i odczytu nośników danych innych niż oznaczone z wyjątkiem nośników obrotu danymi podlegających regulacjom odrębnych umów.

b. Dane osobowe powinny być przechowywane na nośnikach mobilnych w sposób bezpieczny. Chronione programem pozwalającym na szyfrowanie oparte na algorytmach AES lub RSA kluczem minimum 128.

c. Nośniki wykorzystywane do przenoszenia danych osobowych przed ponownym wykorzystaniem powinny być czyszczone oprogramowaniem nadpisującym, wolną przestrzeń.

d. Niepotrzebne i uszkodzone nośniki mobilne oddawane są do Referatu Spraw Obywatelskich i Ogólnoorganizacyjnych.

e. Użytkownik nośników mobilnych podlega wstępnemu i okresowemu szkoleniu z zasad bezpiecznego przechowywania danych na nośnikach, zasad ich udostępniania oraz bezpiecznej pracy na urządzeniach mobilnych przy przetwarzaniu danych osobowych.

3. Zasady użytkowania komputerów przenośnych.

a. Osoba użytkująca komputer przenośny, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego

komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w niniejszej Polityce.

b. W celu zapobiegania dostępowi do tych danych przez osobę nieuprawnioną należy Użytkować wyłącznie urządzenia w domenie ActiveDirectory.

c. Nie zezwalać na użytkowanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

d. W przypadku konieczności przechowywania danych osobowych lub innych poufnych danych na dysku lokalnym należy takie dane zaszyfrować.

§ 27

Zasady korzystania z poczty e-mail

1. Serwer poczty elektronicznej funkcjonuje w wewnętrznej sieci Urzędu Miasta Jedlina-Zdrój i zajmuje się dystrybucją wiadomości email w sieci wewnętrznej oraz na serwery zewnętrzne.
2. Wysyłanie poczty elektronicznej działa w oparciu o protokół SMTP.
3. Pobieranie wiadomości z serwera poczty elektronicznej wykonuje się w oparciu o protokół POP 3 lub IMAP
4. Ustawienia serwera wymagają uwierzytelnienia wysyłania wiadomości tj. przed wysłaniem każdej wiadomości pocztowej program pocztowy musi podać dane uwierzytelniające.
5. Konta poczty elektronicznej przydzielane są użytkownikom na podstawie Wniosku o nadanie/zmianę uprawnień do pracy w systemie.
6. Konta poczty elektronicznej przydzielane są według klucza: „pierwsza litera imienianazwisko@jedlinazdroj.eu"
7. Administrator systemu generuje hasła do poczty oraz przeprowadza konfigurację programu pocztowego.
8. Wiadomość pocztowa jest wysyłana i odbierana nieszyfrowanym połączeniem, niewolno jej stosować do przesyłania danych osobowych bez zastosowana odpowiednich procedur szyfrowania załączników.
9. W przypadku wysyłana wiadomości do wielu odbiorców zwłaszcza na adresy prywatne lub do instytucji innych niż administracja publiczna należy używać pola ukrytego

§ 28

Zasady usuwania danych z informatycznych nośników zawierających dane osobowe

1. Usuwanie danych z nośnika polega na trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenia przez osoby niepowołane, przy zastosowaniu powszechnie dostępnych metod.
2. W zależności od nośnika na którym przechowywane są dane osobowe, ich usuwanie polega na:

a. Nośniki optyczne (płyty CD/DVD/BLU-RAY) - należy w taki sposób zniszczyć nośnik, aby uniemożliwić odczytanie danych z płyty. W tym przypadku zalecane jest wykorzystywanie niszczarek spełniających wymagania:

- Klasa B – ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców,
- Stopień 3 - nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony – kategoria O-3 dla płyt CD/DVD/BLU-RAY,
- Stopień 4: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają szczególnej ochronie – dane szczególnych kategorii – kategoria O- 4 dla płyt CD/DVD/BLU-RAY,

b. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:

- Niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych. Istnieje specjalnie oprogramowanie dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych.
- Niszczenie sprzętowe -p polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.

c. Nośniki magnetyczne (dyski twarde HDD) – oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.

d. Przynajmniej raz w roku ASI dokonuje przeglądu informatycznych nośników danych w celu przeznaczenia ich do zniszczenia.

e. Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone zniszczenia, samo ich zniszczenie powinno odbywać się komisyjnie, a z samej operacji jest sporządzany protokół.

f. Komisja w składzie trzech osób (ASI, IOD osoba wyznaczona przez Administratora) powoływana jest Zarządzeniem Burmistrza Miasta Jedlina-Zdrój.

XI. POSTANOWIENIA KOŃCOWE

§ 29

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie RODO.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

XII. SPIS ZAŁĄCZNIKÓW

1. Rejestr czynności przetwarzania - załącznik nr 1
2. Karta szkolenia wstępnego w zakresie ochrony danych osobowych - załącznik nr 2
3. Upoważnienie do przetwarzania danych osobowych - załącznik nr 3
4. Procedura analizy ryzykiem i oceny skutków przetwarzania – załącznik nr 4
5. Oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych - załącznik nr 5
6. Polityka wypełniania obowiązku informacyjnego - załącznik nr 6
7. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych – załącznik nr7
8. Wzór umowy powierzenia przetwarzania danych osobowych - załącznik nr 8
9. Rejestr udostępnień danych osobowych - załącznik nr 9
10. Obszar przetwarzania danych - załącznik nr 10

Przedstawione powyżej wzory nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę ochrony danych osobowych. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna ADO dotycząca obszaru ochrony danych osobowych stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga jej zmiany.

Rejestr czynności przetwarzania - załącznik nr 1

REJESTR CZYNNOŚCI RZETWARZANIA

Administratorem danych osobowych jest Burmistrz Miasta Jedlina-Zdrój ul. Poznańska 2, 58-330 Jedlina Zdrój tel.: 74 84 55 215, email: urzad@jedlinazdroj.eu

Inspektorem ochrony danych, kontakt: tel.: 74 84 55 215, email: iodo@jedlinazdroj.eu adres do korespondencji: Urząd Miasta Jedlina-Zdrój ul. Poznańska 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
														Transfer do kraju trzeciego lub org. międzynarodowej	
Nazwa czynności przetwarzania	**Jednostka organizacyjna (departament, dział itp.)**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontaktowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	**DPIA (jeśli tak, lokalizacja raportu)**	**Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)**	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**

Karta szkolenia wstępnego w zakresie ochrony danych osobowych - załącznik nr 2

Imię i nazwisko osoby odbywającej szkolenie: .....
Stanowisko: .....
Instruktaż przeprowadzony: .... (data) (imię i nazwisko przeprowadzającego instruktaż) ..... (imię i nazwisko przeprowadzającego instruktaż)
W ramach szkoleniach poruszone zostały następujące tematy i zagadnienia:
Zgodnie z Polityką Ochrony Danych Osobowych służącym do przetwarzania danych osobowych wymaga się tego, aby: 1) Dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych. 2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych. 3) Dane były chronione przed dostępem do nich osób nieupoważnionych. 4) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz. 5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy. 6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych. 7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy. 8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności. 9) Szafy, w których przechowywane są dane, powinny być zamykane na klucz. 10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy. 11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane. 12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do szaf. 13) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy. 14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby

nieupoważnione nie miały wglądu w dane.

15) W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.

16) Nie należy udostępniać osobom nieupoważnionym tych komputerów.

17) W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności.

18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.

19) Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie.

20) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi.

Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu,

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Uwagi:

.....

Przeczytałem poniższy instruktaż, w pełni go zrozumiałem i zaakceptowałem. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem*

.....

(data i podpis osoby, której udzielono instruktażu)

....

(podpis Inspektora Ochrony Danych) (miejscowość, data)

** Podpis jest potwierdzeniem odbycia instruktażu i zapoznania się z przepisami oraz zasadami przetwarzania i ochrony danych osobowych. Podpisaną kartę przechowuje dział kadr*

Upoważnienie do przetwarzania danych osobowych - załącznik nr 3

Jedlina-Zdrój, dnia ..... r.

Nr upoważnienia .....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. Nr 119, str. 1) i Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.).

Upoważniam

.....

zatrudnionego na stanowisku .....

do wykonywania następujących operacji na danych osobowych będących w dyspozycji Urzędu Miasta Jedlina-Zdrój, zawartych w zbiorach:

NAZWA ZBIORU DANYCH	NAZWA OPERACJI PRZETWARZANIA													
	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

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.*) i elektronicznej, wg wykazu zbiorów podanych w tabeli powyżej. Upoważnienie jest udzielone czas nieokreślony. Upoważnienie traci ważność z chwilą ustania stosunku pracy.

.....

Podpis ADO

Procedura analizy ryzykiem i oceny skutków przetwarzania – załącznik nr 4

Wstęp

Mając na uwadze konieczność uwzględnienia w procesie przetwarzania danych osobowych prawdopodobieństwa i powagi ryzyka naruszenia praw lub wolności osób, których przetwarzanie dotyczy, Administrator niniejszym dokumentem wprowadza do organizacji procedurę szacowania ryzyka w stosunku do aktualnie prowadzonych jak i planowanych operacji przetwarzania danych osobowych.

Administrator ma świadomość odpowiedzialności prawnej w kontekście przetwarzanych danych osobowych, dlatego wdraża takie środki techniczne i organizacyjne, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Zastosowane środki techniczne i organizacyjne są poddawane cyklicznemu doskonaleniu.

Administrator w procesie przetwarzania danych uwzględnia ochronę danych osobowych w fazie projektowania z uwzględnieniem zasady domyślnej ochrony danych.

Jeżeli za przeprowadzenie procesu szacowania ryzyka odpowiada inna osoba niż Administrator, jest ona odpowiedzialna za przeprowadzenie tego procesu w oparciu o zachowanie obiektywnej postawy względem zidentyfikowanego ryzyka.

§ 1

Cel szacowania ryzyka

1. Administrator przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa informacji w celu zidentyfikowania obszarów, które mogą istotnie wpływać na osobę, której przetwarzanie dotyczy. Administrator wdraża podejście oparte na ryzyku, aby zapewnić ochronę praw i wolności osób, których przetwarzanie dotyczy.
2. Na szacowanie ryzyka składa się:

1) Analiza Ryzyka Ogólnego,
2) Ocena Skutków Dla Przetwarzania Danych (DPIA).

§ 2

Wytyczne wykorzystywane do przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)

1. Z racji tego, iż Administrator w ramach realizacji praw podstawowych w zakresie ochrony danych osobowych, kieruje się zasadą legalności przetwarzania zgodnego z prawem, opiera proces szacowania ryzyka na następujących normach ISO oraz wytycznych Grupy Roboczej art. 29:

1) Norma PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji);

2) Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017);

3) Wytyczne Grupy Roboczej art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 z dnia 4 października 2017r.

§ 3

Definicje legalne

Ilekroć w „Analizie Ryzyka Ogólnego i Ocenie Skutków Dla Przetwarzania Danych (DPIA)" mówi się o:

1. **Szacowaniu ryzyka** – rozumie się przez to proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyka związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy;
2. **Analizie ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;
3. **Ocenie ryzyka** – proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka;
4. **Ryzyku** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;
5. **Ryzyku szczątkowym** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
6. **Postępowaniu z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;
7. **Akceptacji ryzyka** – rozumie się przez to decyzję Administratora/najwyższego kierownictwa organizacji o tym, aby ryzyko zaakceptować;
8. **Podatności** – rozumie się przez to słabość w strukturze fizycznej, technicznej, organizacyjnej organizacji;
9. **Incydencie** – rozumie się przez to zdarzenie mające lub mogące mieć negatywny wpływ na System Zarządzania Bezpieczeństwem Informacji w organizacji. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe organizacja przetwarza, szkodę o charakterze majątkowym lub niemajątkowym;
10. **Poufności** – rozumie się przez to właściwość polegająca na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają;
11. **Integralności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne;

12. **Dostępności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania;

13. **Bezpieczeństwie informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

§ 4

Oznaczenie uwarunkowań związanych z funkcjonowaniem organizacji – ustalenie kontekstu

1. Organizacja określa, które z uwarunkowań zewnętrznych bądź wewnętrznych mają znaczenie dla szacowania ryzyka.

2. Uwarunkowania zewnętrzne istotnie wpływające na organizację:

1) relacje z innymi administratorami danych osobowych,

2) relacje z innymi podmiotami zewnętrznymi,

3) zasięg terytorialny działalności organizacji,

4) uwarunkowania prawne organizacji.

3. Uwarunkowania wewnętrzne istotnie wpływające na organizację:

1) struktura i rozmiary organizacji,

2) uwarunkowania formalne wewnętrzne (polityki, regulaminy),

3) sposoby podejmowania decyzji w organizacji względem bezpieczeństwa przepływu danych,

4) kultura organizacji.

4. Organizacja na etapie tworzenia Polityki Bezpieczeństwa Informacji przeanalizowała:

1) podstawy legalności przetwarzania danych (w oparciu o przesłanki wynikające z RODO),

2) staranność po stronie organizacji w zakresie spełniania obowiązków informacyjnych oraz realizacji praw osób fizycznych, których dane osobowe dotyczą w oparciu o RODO,

3) cel przetwarzania danych osobowych, chyba, że organizacja działa w imieniu innego administratora (w procesie przetwarzania danych organizacja występuje w roli procesora),

4) zakres przetwarzanych danych kierując się zasadami przetwarzania danych określonymi w RODO,

5) wymagania dotyczące zabezpieczeń organizacyjnych, środków kontroli logicznej procesu przetwarzania, środków ochrony fizycznej danych.

Podstawa prawna:
Zgodnie z art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 5

Wybór metody na cele przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla

Przetwarzania Danych (DPIA)

1. Rozporządzenie ogólne o ochronie danych pozostawia Administratorowi wybór w zakresie zastosowania konkretnej metody szacowania ryzyka.

2. Administrator ma świadomość, iż w procesie szacowania ryzyka może kierować się metodą:

1) ilościową: wielkość poniesionych strat próbuje się wyrazić liczbowo, niejednokrotnie w oparciu o dane statystyczne, bądź,

2) jakościową: wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

3. Administrator ma świadomość, iż szacowanie ryzyka w procesie przetwarzanych danych osobowych powinno opierać się o metodę jakościową - strat związanych z ochroną danych osobowych bardzo często nie sposób wyrazić za pomocą liczb. W związku z powyższym Administrator decyduje się na wykorzystanie metody szacowania ryzyka CRAMM (CCTA Risk Analysis and Management Method).

4. Atrybuty, jakie Administrator przyjmuje w tabeli szacowania ryzyka to:

1) Poufność – osoba nieupoważniona bądź nieupoważniony podmiot nie mają dostępu do danych osobowych. Dane osobowe zgodnie z tym atrybutem nie są ujawniane w nieuprawniony sposób.

2) Integralność – konieczność zapewnienia spójności danych osobowych; atrybut determinujący konieczność ochrony danych osobowych przed przypadkowym ich zniekształceniem w przypadku ich zapisu, odczytu, transmisji bądź magazynowania.

3) Dostępność – zasób w postaci danych osobowych jest możliwy do wykorzystania na żądanie w konkretnym czasie przez osobę bądź podmiot upoważniony/uprawniony w zakresie dostępu do danych.

§ 6

Klasyfikacja czynności przetwarzania

1. Administrator, w pierwszej kolejności dzieli czynności przetwarzania (określone w załączniku nr 1 do Polityki Bezpieczeństwa Informacji) na te, które wymagają Oceny Skutków dla Przetwarzania Danych (DPIA) oraz te, względem których Administrator wykonuje Analizę Ryzyka Ogólnego.

2. Kryterium, według którego Administrator dokonuje wstępnej klasyfikacji z uwzględnieniem kontekstu przetwarzania danych są wytyczne Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679 tj.:

1) Ocena lub punktacja: w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub

zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motywy 71 i 91).

2) Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a)). Zagrożenie: przetwarzanie mogące prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium.

3) Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c)). Zagrożenie: osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).

4) Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10.

5) Dane przetwarzane na dużą skalę: przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, Administrator wespół z Inspektorem Ochrony Danych bierze pod uwagę w szczególności następujące czynniki:

a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;

b) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;

c) czas trwania lub trwałość czynności przetwarzania danych;

d) zakres geograficzny czynności przetwarzania.

6) Dopasowywanie lub łączenie zbiorów danych: zbiory pochodząc z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

7) Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą: przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób

wymagających szczególnej opieki, których dane dotyczą, zalicza się dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

8) Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu. Zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. Ocena skutków dla ochrony tych danych pomoże Administratorowi zrozumieć ryzyko i je wyeliminować.

9) Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy". Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

Podstawa prawna:

Zgodnie z wymogami wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679, s. 10 - 13

3. Powyższe wytyczne znajdują źródło w art. 35 ust. 3 RODO:

„Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie."

Podstawa prawna:

Zgodnie z art. 35 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

4. Administrator przyjmuje zasadę, że przetwarzanie spełniające dwa kryteria, będzie skutkowało koniecznością przeprowadzenia Oceny Skutków dla Przetwarzania Danych (DPIA).

5. Administrator może uznać, iż przetwarzanie wyczerpujące tylko jedno z przywołanych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych.

6. Administrator może równocześnie stwierdzić, iż przetwarzanie wyczerpuje więcej niż dwa kryteria, ale mimo to nie przeprowadza oceny skutków dla ochrony danych. W takim przypadku Administrator uzasadnia i dokumentuje powody, dla których nie przeprowadzono oceny skutków dla ochrony danych.

Zgodnie z art. 35 ust. 4 RODO:

„Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.".

Administrator, w procesie podejmowania decyzji o klasyfikacji operacji przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) bierze pod uwagę wytyczne Urzędu Ochrony Danych Osobowych w tym zakresie.

Podstawa prawna:

Zgodnie z art. 35 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

7. Ocena Skutków Dla Przetwarzania Danych (DPIA) nie jest obowiązkowa w przypadkach:

1) gdy nie jest prawdopodobne, aby operacja przetwarzania może powodować wysokie ryzyko,

2) gdy przeprowadzono już podobną ocenę skutków dla ochrony danych,

3) gdy operację przetwarzania zatwierdzono przed majem 2018r.,

4) gdy operacja przetwarzania posiada podstawę prawną, która reguluje daną operację przetwarzania,

5) gdy operacja przetwarzania znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

Podstawa prawna:

Zgodnie z wymogami wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679, s. 15

8. **„Klasyfikacja Czynności Przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)"** określa czynności przetwarzania względem których należy przeprowadzić analizę ryzyka ogólnego oraz czynności przetwarzania, względem których należy przeprowadzić ocenę skutków.

§ 7

Grupowanie podobnych czynności przetwarzania

1. Zgodnie z art. 35 ust. 1 RODO dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza pojedynczą ocenę.
2. Administrator grupuje podobne operacje przetwarzania dla Analizy ryzyka ogólnego (ARO) oraz Oceny Skutków Przetwarzania Danych (DPIA) uwzględniając kontekst ich przetwarzania w oparciu o następujące kryterium:

1) ARO-Gr.1 - dane osobowe związane z pracownikami,

2) ARO-Gr.2 - dane osobowe związane z usługami "na zewnątrz" (np. czynności dla społeczeństwa, programy dofinansowania itd...),

3) ARO-Gr.3 - dane osobowe związane z usługami "do wewnątrz" (np. kontrahenci, usługodawcy itp...),

4) DPIA-Gr.1 - dane osobowe związane z pracownikami,

5) DPIA-Gr.2 - dane osobowe związane z usługami "na zewnątrz" (np. czynności dla społeczeństwa, programy dofinansowania itd...).

3. Przedmiotowe grupowanie podobnych operacji przetwarzania znajduje odzwierciedlenie w „Grupowaniu podobnych czynności przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)"

§ 8

Szacowanie ryzyka

1. Proces szacowania ryzyka Administrator poprzedza identyfikacją aktywów organizacji, zagrożeń dla aktywów, zabezpieczeń stosowanych w organizacji, podatności (prawdopodobieństwa) oraz następstw (skutków).
2. **Organizacja identyfikuje aktywa** i dzieli je na aktywa podstawowe i aktywa wspierające.

1) Do aktywów podstawowych organizacja zalicza:

a) informacje - obejmują dane osobowe, które organizacja przetwarza w związku z prowadzoną działalnością; informacje niezbędne do ociągnięcia celów organizacji,

b) operacje przetwarzania: czynności w procesie przetwarzania danych osobowych, które organizacja jest zobowiązana podejmować/utrzymywać, by osiągać cele strategiczne jednostki przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzanych informacji w organizacji.

2) Do aktywów wspierających organizacja zalicza:

a) sprzęt - obejmuje przenośne oraz stacjonarne urządzenia komputerowe, urządzenia serwerowe, urządzenia peryferyjne (drukarki czy wymienny napęd dyskowy),

b) nośniki danych (papierowe) zawierające dane osobowe - dokumentacja zawierająca treści o charakterze osobowym,

c) nośniki danych (elektroniczne) - z racji swojego przeznaczenia mogą być podłączone do urządzenia komputerowego w celu przygotowania danych osobowych do przetwarzania (pendrive, płyta CD ROM, wymienny dysk twardy),

d) oprogramowanie - obejmuje wszystkie programy, dzięki którym bądź w oparciu o nie organizacja przetwarza dane osobowe. W zakresie oprogramowania uwzględnia się system operacyjny, oprogramowanie uzupełniające usługi systemu operacyjnego, oprogramowanie służące do obsługi poczty elektronicznej czy bazy danych, standardowe i dedykowane aplikacje biznesowe np. oprogramowanie księgowe, oprogramowanie służące do obsługi Klientów, pracowników organizacji.

e) okablowanie - sieć, którą należy rozumieć przez pryzmat urządzenia używanego do połączenia wielu komputerów i elementów systemu informacyjnego,

f) personel – osoby zaangażowane w proces przetwarzania danych osobowych oraz obsługę systemu informacyjnego. Do personelu zaliczamy kierownictwo, osoby upoważnione do przetwarzania danych, osoby, którym nadano uprawnienia do pracy w programach dziedzinowych bazodanowych, osoby, które mają w zakresie swoich obowiązków mają między innymi konieczność utrzymania systemu informacyjnego oraz twórców oprogramowania,

g) lokalizację - siedziba, ale również środowisko zewnętrzne. Siedziba organizacji odnosi się do budynków, jakie organizacja zajmuje oraz wszystkich obszarów przetwarzania wewnątrz budynków. Siedziba jest istotna ze względu na jej położenie geograficzne, obszar miejski, przestrzeń publiczną.

Podstawa prawna:
Zgodnie z wymogami normy PN-ISO/IEC 27005:2014-01 Zał. B

3. Organizacja identyfikuje zagrożenia i dzieli je na:

1) zniszczenia fizyczne:

a) pożar,

b) zalanie,

c) zanieczyszczenie,

d) poważny wypadek,

e) zniszczenie urządzeń lub nośników,

f) pył, korozja, wychłodzenie.

2) zjawiska naturalne:

a) zjawiska klimatyczne,

b) zjawiska sejsmiczne,

c) zjawiska wulkaniczne,

d) zjawiska pogodowe,

e) powódź.

3) utrata podstawowych usług:

a) awaria systemu klimatyzacji lub dostaw wody,

b) utrata dostaw prądu,

c) awaria urządzenia telekomunikacyjnego.

4) zakłócenia spowodowane promieniowaniem:

a) promieniowanie elektromagnetyczne,

b) promieniowanie cieplne,

c) impuls elektromagnetyczny.

5) naruszenia bezpieczeństwa informacji:

a) przechwycenie sygnałów na skutek zjawiska interferencji,

b) szpiegostwo zdalne,

c) podsłuch,

d) kradzież nośników lub dokumentów,

e) kradzież urządzenia,

f) odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników,

g) ujawnienie,

h) dane z niewiarygodnych źródeł,

i) manipulowanie urządzeniem,

j) sfałszowanie oprogramowania,

k) detekcja umiejscowienia.

6) awarie techniczne:

a) awaria urządzenia,

b) niewłaściwe funkcjonowanie urządzeń,

c) przeciążenie systemu informacyjnego,

d) niewłaściwe funkcjonowanie oprogramowania,

e) naruszenie zdolności utrzymania systemu informacyjnego.

7) nieautoryzowane działania:

a) nieautoryzowane użycie urządzeń,

b) nieuprawnione kopiowanie oprogramowania,

c) użycie fałszywego lub skopiowanego oprogramowania,

d) zniekształcenie danych,

e) nielegalne przetwarzanie danych.

8) naruszenia bezpieczeństwa funkcji:

a) błąd użytkowania,

b) naruszenie praw,

c) fałszowanie praw,

d) odmowa działania,

e) naruszenie dostępności personelu.

Podstawa prawna:

Zgodnie z wymogami normy PN-ISO/IEC 27005:2014-01 Zał. C

4. Organizacja identyfikuje zabezpieczenia zastosowane w organizacji w ten sposób, iż klasyfikuje je w Rejestrze Czynności Przetwarzania stanowiącym załącznik nr 1 do Polityki Ochrony Danych Osobowych. Administrator uwzględnia stosowane zabezpieczenia w rejestrze czynności przetwarzania z uwagi na konieczność dostosowania wymogów formalnych do art. 30 RODO (opis technicznych i organizacyjnych środków bezpieczeństwa).

5. Organizacja identyfikuje podatność (prawdopodobieństwo) wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą:

PRAWDOPODOBIEŃSTWO	SKALA	CZĘSTOTLIWOŚĆ WYSTĄPIENIA ZDARZENIA
Zdarzenie niemal pewne	4	zdarzenie występuje co najmniej raz w tygodniu
Zdarzenie wysoce prawdopodobne	3	zdarzenie występuje co najmniej raz w miesiącu
Zdarzenie mało prawdopodobne	2	zdarzenie występuje co najmniej raz na kwartał
Zdarzenie nieprawdopodobne	1	zdarzenie nie występuje lub występuje raz w roku

6. Organizacja identyfikuje skutek wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą:

SKUTEK	SKALA	OPIS NASTĘPSTW
zdarzenie wywołuje katastrofalny skutek	4	• strata finansowa powyżej 100,000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy wysokości 100,000 zł, • zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych, • orzeczenie wyroku skazującego w zakresie przetwarzania danych przez organizację.
zdarzenie wywołuje bardzo znaczący skutek	3	• strata finansowa powyżej 50,000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy powyżej 50,000 zł, • zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje znaczący skutek	2	• strata finansowa powyżej 3000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy powyżej 3000 zł,

SKUTEK	SKALA	OPIS NASTĘPSTW
		• zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje niewielki skutek	1	• strata finansowa poniżej 3000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy wywołuje niewielki skutek, • strata osobista dla osoby fizycznej, której przetwarzanie wywołuje niewielki skutek, • organ nadzorczy daje upomnienie i wzywa do naprawienia braków formalnych (przy założeniu, że organizacja wypełnia wskazania organu nadzorczego), • skutek nie powodujący utraty zaufania ze strony osób fizycznych, względem których jednostka wykonuje zadania publiczne.
zdarzenie nie powoduje skutku (nie występuje)	0	• nie ma straty finansowej, • po stronie osoby fizycznej, której przetwarzanie dotyczy nie występuje ani szkoda o charakterze majątkowym, ani osobistym, • zaufanie osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych nie doznaje żadnego uszczerbku.

§ 9

Dokonanie analizy ryzyka

1. Organizacja wykorzystuje następujący wzór analizy ryzyka w zakresie wykonywania:

1) Analizy Ryzyka Ogólnego,

2) Oceny Skutków Dla Przetwarzania Danych (DPIA).

WZÓR ANALIZY RYZYKA:

$R_P = P \times S$

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczanego ryzyka	
P	wartość przypisana prawdopodobieństwu materializacji zagrożenia niezrealizowania założonych celów przez organizację	1 - zdarzenie nieprawdopodobne, 2 - zdarzenie mało prawdopodobne, 3 - zdarzenie wysoce prawdopodobne, 4 - zdarzenie niemal pewne.
S	Skutki zdarzenia	0 – zdarzenie nie powoduje skutku (nie występuje), 1 – zdarzenie wywołuje niewielki skutek, 2 – zdarzenie wywołuje znaczący skutek, 3 – zdarzenie wywołuje bardzo znaczący skutek,- 4 - zdarzenie wywołuje katastrofalny skutek.

2. Organizacja przyjmuje następujący zakres macierzy:

			SKUTEK				
			0	1	2	3	4
PRAWDOPODOBIEŃSTWO	Zdarzenie nieprawdopodobne	1	0	1	2	3	4
	Zdarzenie mało prawdopodobne	2	0	2	4	6	8
	Zdarzenie wysoce prawdopodobne	3	0	3	6	9	12
	Zdarzenie niemal pewne	4	0	4	8	12	16

3. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Analizy Ryzyka Ogólnego:

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Poziom ryzyka nieakceptowany – wymaga bezwzględnej reakcji – cel: zredukowanie podatności

4. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków Dla Przetwarzania Danych (DPIA):

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Wymaga bezwzględnej reakcji – cel: zredukowanie podatności Konsultacja z organem nadzorczym konieczna w momencie, kiedy Administrator nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego mimo, że przewidział wprowadzenie środków bezpieczeństwa.

5. Wyniki analizy szacowania ryzyka zawarte są w:

1) Macierzy ryzyka analizy ryzyka ogólnego tj.: „Macierzy ryzyka do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" z

2) Macierzy ryzyka oceny skutków dla przetwarzania danych tj.: „Macierzy ryzyka do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 10

Ocena ryzyka dla przetwarzania danych osobowych

1. Ocena ryzyka składa się z następujących elementów:

1) określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,

2) aktyw, dla którego zostało zidentyfikowane ryzyko,

3) kategoria zagrożenia,

4) rodzaj zagrożenia,

5) atrybut, dla którego zidentyfikowano ryzyko,

6) poziom ryzyka przed wprowadzeniem działań naprawczych wraz ze skalą ryzyka po wstępnym procesie,

7) szacowania ryzyka,

8) podjęta przez Administratora decyzja wobec zidentyfikowanego ryzyka,

9) zalecenia wobec zidentyfikowanego ryzyka.

2. Administrator może podjąć cztery rodzaje decyzji wobec zidentyfikowanego ryzyka, a mianowicie:

1) redukcja ryzyka (modyfikowanie ryzyka) – polega na obniżeniu poziomu ryzyka poprzez na przykład zastosowanie dodatkowych zabezpieczeń,

2) akceptacja ryzyka (zachowanie ryzyka) – organizacja nie wprowadza żadnych zmian w zakresie zidentyfikowanego ryzyka (najczęściej do przyjęcia na poziomie niskim),

3) unikanie ryzyka – polega na unikaniu przez organizację działań determinujących powstanie określonych typów ryzyka,

4) dzielenie (transfer) ryzyka – polega na przeniesieniu ryzyka najczęściej poprzez scedowanie skutków ryzyka na podmiot zewnętrzny.

3. Ocena ryzyka dla przetwarzania danych osobowych zawarta jest w „Ocenie ryzyka dla przetwarzania danych osobowych do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)".

§ 11

Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń

1. Plan postępowania z ryzykiem określa:

1) określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,

2) aktyw, dla którego zostało zidentyfikowane ryzyko,

3) kategoria zagrożenia,

4) rodzaj zagrożenia,

5) atrybut, dla którego zidentyfikowano ryzyko,

6) zalecenia wobec zidentyfikowanego ryzyka,

7) komórka organizacyjna odpowiedzialna za wprowadzenie zaleceń,

8) termin realizacji wdrożenia zaleceń,

9) poziom ryzyka po wprowadzeniu działań naprawczych (wtórny proces szacowania ryzyka) wraz ze skalą ryzyka po wprowadzeniu tychże działań,

10) właściciel ryzyka.

2. Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka zawarty jest w „Planie postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)".

§ 12

Akceptacja ryzyka szczątkowego

Akceptacja ryzyka przez Administratora następuje poprzez złożenie formalnego oświadczenia, którego treść stanowi zawartość „Oświadczenia właściciela ryzyka".

§ 13

Konsultacje z organem nadzorczym

Jeżeli mimo zastosowania odpowiednich środków technicznych lub organizacyjnych, analiza następstw utraty poufności bądź integralności lub dostępności w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków Dla Przetwarzania Danych (DPIA) w dalszym ciągu powoduje wysokie ryzyko szczątkowe, Administrator konsultuje się z organem nadzorczym. Administrator ma świadomość, iż ryzyko wysokie nie może podlegać decyzji w formie akceptacji.

Podstawa prawna:

Zgodnie z art. 36 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 14

Monitorowanie i przegląd ryzyka

1) Administrator deklaruje chęć utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w organizacji poprzez:

1) przeprowadzanie nie rzadziej niż raz na rok przeglądów ryzyk,

2) przeprowadzanie nie rzadziej niż raz na 6 miesięcy przeglądów stanu bezpieczeństwa,

3) przeprowadzanie oceny skutków względem już poddanych przeglądowi w zakresie praw i wolności czynności przetwarzania, nie rzadziej, niż raz na trzy lata,

4) przeprowadzanie oceny skutków dla nowych kategorii przetwarzania czy zastosowania nowoczesnych technologii przetwarzania, przed rozpoczęciem ich przetwarzania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych,

5) stosowanie procedur postępowania w przypadku wystąpienia incydentu,

6) przeprowadzanie cyklicznie szkoleń z zakresu ochrony danych osobowych,

7) ustalenie odpowiedzialności za ciągły proces minimalizacji ryzyka.

2) Administrator uwzględnia fakt, iż prowadzanie Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.

Oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych - załącznik nr 5

Oświadczam, że zostałem zapoznany z:

- przepisami o ochronie danych osobowych,
- zasadami przetwarzania i ochrony danych osobowych opisanymi w Polityce ochrony danych, w tym w systemach służących do przetwarzania danych osobowych wdrożonymi do stosowania u administratora danych.

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

- dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych i informacji prawem chronionych,
- przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi administratora danych,
- zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, nieuprawnioną zmianą lub zniszczeniem, utratą, uszkodzeniem.
- zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.

.....

(podpis osoby składającej oświadczenie)

Polityka wypełniania obowiązku informacyjnego - załącznik nr 6

Wzór ogólny klauzuli informacyjnej

W związku z realizacją wymogów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych „RODO"), Urząd Miasta Jedlina-Zdrój informuje o zasadach przetwarzania Pani/Pana danych osobowych oraz o przysługujących Pani/Panu prawach z tym związanych.

Jeśli ma Pani/Pan pytania dotyczące sposobu i zakresu przetwarzania Pani/Pana danych osobowych przez Urząd, a także przysługujących Pani/Panu uprawnień, prosimy o kontakt z Urzędem Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina Zdrój lub z inspektorem ochrony danych drogą elektroniczną poprzez: iodo@jedlinazdroj.eu lub pisemnie na adres: Urząd Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina Zdrój.

I. Wskazanie administratora

Administratorem Pani/Pana danych osobowych jest Burmistrz Miasta Jedlina-Zdrój ul. Poznańska 2, 58-330 Jedlina Zdrój.

II. Wskazanie inspektora ochrony danych

Inspektorem ochrony danych, kontakt: tel.: 74 84 55 215, email: iodo@jedlinazdroj.eu adres do korespondencji: Urząd Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina-Zdrój.

III. Cele oraz podstawa prawna przetwarzania Pani/Pana danych osobowych

Urząd przetwarza Pani/Pana dane osobowe w celach:

1. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
2. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
3. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
4. w innych przypadkach Pani/Pana dane osobowe przetwarzane będą wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody.

IV. Obowiązek podania danych osobowych

Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym, wynika z realizacji obowiązków wynikających z przepisów prawa.

V. Informacje o odbiorcach Pani/Pana danych osobowych

W związku z przetwarzaniem Pani/Pana danych osobowych w celach wskazanych w pkt. III, Pani/Pana dane osobowe mogą być udostępniane następującym odbiorcom bądź kategoriom odbiorców: organom władzy publicznej oraz podmiotom wykonującym zadania publiczne lub działającym na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa np. policja, sąd, prokuratura, urząd skarbowy, komornik sądowy.

VI. Okresy przetwarzania danych osobowych

Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanych w pkt. III celów, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy prawa.

VII. Prawa osoby, której dane dotyczą

Administrator pragnie zapewnić Panią/Pana, że wszystkim osobom, których danych osobowe są przetwarzane w Urzędzie Miasta Jedlina-Zdrój, przysługują odpowiednie prawa wynikające z 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. W związku z tym przysługują Pani/Panu następujące prawa:

1. prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2. prawo do żądania sprostowania (poprawiania) danych osobowych - w przypadku, gdy dane są nieprawidłowe lub niekompletne;
3. prawo do żądania usunięcia danych osobowych (tzw. „prawo do bycia zapominanym");
4. prawo do żądania ograniczenia przetwarzania danych osobowych;
5. prawo do wniesienia sprzeciwu wobec przetwarzania;
6. prawo do przenoszenia danych.

VIII. Prawo do cofnięcia zgody na przetwarzanie danych osobowych

W zakresie, w jakim udzieliła Pani/Pan zgody na przetwarzanie danych osobowych, przysługuje Pani/Panu prawo do jej cofnięcia. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych, którego dokonano na podstawie zgody przed jej wycofaniem.

IX. Prawo wniesienia skargi do organu nadzorczego

W przypadku uznania, iż przetwarzanie przez Urząd Pani/Pana danych osobowych narusza przepisy 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, przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Wzór klauzuli informacyjnej stosowanej w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Informuję, że:
administratorem Pani/Pana danych osobowych jest Urząd Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina-Zdrój, zwany dalej Administratorem; Administrator prowadzi operacje przetwarzania następujących kategorii Pani/Pana danych osobowych:

- ...,
- ...,

inspektorem danych osobowych u Administratora email: iodo@jedlinazdroj.eu adres do korespondencji: Urząd Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina-Zdrój.

1) Pani/Pana dane osobowe przetwarzane będą w celu ..... i nie będą udostępniane innym odbiorcom,
2) podstawą przetwarzania Pani/Pana danych osobowych jest .....,
3) posiada Pani/Pan prawo do:
   - żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
   - wniesienia sprzeciwu wobec takiego przetwarzania,
   - przenoszenia danych,
   - wniesienia skargi do organu nadzorczego,
   - cofnięcia zgody na przetwarzanie danych osobowych.
4) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu,
5) Pani/Pana dane osobowe będą przechowywane przez okres .....

Wzór klauzuli zgody na przetwarzanie danych osobowych zgodnej z RODO

1. Wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora danych Urząd Miasta Jedlina-Zdrój ul. Poznańska 2 58-330 Jedlina-Zdrój w celu .....
2. Podaję dane osobowe dobrowolnie i oświadczam, że są one zgodne z prawdą.
3. Zapoznałem(-am) się z treścią klauzuli informacyjnej, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiania.

.....

Data i podpis

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych – załącznik nr 7

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych na co może wskazywać: stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej należy niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych.
2. Inspektor Ochrony Danych Osobowych dokonuje niezwłocznie zabezpieczenia zbiorów danych osobowych oraz logów systemów operacyjnych komputerów celem analizy.
3. Inspektor Ochrony Danych Osobowych dokona sprawdzenia czy naruszenie miało faktycznie miejsce na podstawie zebranych dowodów i wyjaśnień oraz niezwłocznie powiadamia organ nadzoru nie później niż 72 godziny od momentu naruszenia i podejmuje próbę powiadomienia osób których to naruszenie dotyczy zgodnie z poniższym schematem i sporządza raport z naruszenia ochrony danych stanowiący i odnotowuje w rejestrze naruszeń wg poniższego wzoru.

Wzór rejestru naruszeń ochrony danych osobowych

Rejestr naruszeń ochrony danych osobowych					
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze
1.					
2.					
…					

Wzór umowy powierzenia przetwarzania danych osobowych - załącznik nr 8

UMOWA POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH Nr .....

w dniu ..... pomiędzy:

Gmina Jedlina-Zdrój , z siedzibą w Jedlinie-Zdroju przy ul. Poznańskiej 2

reprezentowaną przez Leszka Orpla – Burmistrza Miasta

zwaną dalej „Powierzającym",

a

..... z siedzibą

przy ....., zwanym dalej „Przetwarzającym",

wspólnie zwanymi dalej „Stronami",

w związku z zawarciem pomiędzy Stronami

Umowy .....,

w celu wykonania postanowień powyższej umowy, Strony zawierają niniejszą umowę, zwaną dalej Umową.

§ 1.

Użyte w Umowie określenia oznaczają:

1) RODO - 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 (Dz. Urz. UE z 2016 r. L 119/1);

2) dane osobowe - dane osobowe dotyczące osób fizycznych .....

3) przetwarzanie danych osobowych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, o których mowa w RODO.

§ 2.

Powierzający oświadcza, że jest administratorem danych w rozumieniu art. 4 pkt. 7 RODO o nazwie: „.....",

§ 3.

Przetwarzający powierzone dane osobowe będzie przetwarzał w okresie niezbędnym do realizacji Umowy; Umowa ulega rozwiązaniu z dniem .....r.

§ 4.

1. Powierzający, na podstawie art. 28 ust. 3 RODO, w celu realizacji postanowień umowy Nr ....., powierza Przetwarzającemu przetwarzanie danych osobowych zawartych w zbiorze,

o którym mowa w § 2 w imieniu i na rzecz Powierzającego, na warunkach opisanych w Umowie.

2. Przekazane przez Powierzającego Przetwarzającemu do przetwarzania dane osobowe zawarte w zbiorze, o którym mowa w § 2 mogą być przetwarzane wyłącznie w celu realizacji Umowy .....

§ 5.

Maksymalny zakres danych osobowych powierzonych Przetwarzającemu do przetwarzania obejmuje:

1) imię i nazwisko osoby.

2) adres zamieszkania osoby, o której mowa w pkt 1,

3) .....

§ 6.

1. Przetwarzający zapewnia, że do przetwarzania danych osobowych będą dopuszczone jedynie osoby, które:

1) posiadają imienne upoważnienie do przetwarzania danych osobowych,

2) zobowiążą się, przed rozpoczęciem przetwarzania danych, do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia, także po ustaniu zatrudnienia u Przetwarzającego.

2. Imienne upoważnienia, o których mowa w ust. 1 są ważne do dnia odwołania, nie później jednak niż do dnia rozwiązania lub wygaśnięcia Umowy. Upoważnienia te zachowują jednak ważność w okresie koniecznym do usunięcia danych z nośników Przetwarzającego w sposób uniemożliwiający ich odczytanie lub wykorzystanie w możliwie najkrótszym technologicznie i organizacyjnie uzasadnionym terminie (wynikającym z technologii stosowanej przez Przetwarzającego) nie wymagającym niszczenia nośników, przy czym wyłącznie w zakresie dotyczącym tych czynności.

§ 7.

1. Powierzający nie wyraża zgody na powierzenie przez Przetwarzającego przetwarzania zbioru danych osobowych, o którym mowa w § 2 innym podmiotom

§ 8.

1. Powierzający lub upoważniony przez niego audytor zewnętrzny ma prawo do przeprowadzenia audytu przestrzegania przez Przetwarzającego zasad przetwarzania danych osobowych, o których mowa w niniejszej umowie oraz w obowiązujących przepisach prawa, w szczególności poprzez żądanie udzielenia informacji dotyczących przetwarzania przez Przetwarzającego powierzonych danych osobowych, stosowanych środków technicznych i organizacyjnych, lub dokonywania audytu w miejscach, w których są przetwarzane powierzone dane osobowe.

2. Powierzający może wystosować do Przetwarzającego prawnie uzasadnione zalecenia z audytu, o którym mowa w ust. 1 dotyczące zasad przetwarzania powierzonych danych osobowych.

3. Powierzający przekaże Przetwarzającemu zalecenia organu nadzorczego powstałe w wyniku ewentualnych uprzednich konsultacji, o których mowa w art. 36 ust. 2 RODO, jeśli Przetwarzający nie otrzymałby ich bezpośrednio od organu nadzorczego, gdy mają zastosowanie do Przetwarzającego.

§ 9.

1. Przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych w zgodzie z przepisami RODO oraz postanowieniami zawartymi w Umowie.

2. Przetwarzający będzie niezwłocznie informować Powierzającego, jeżeli zdaniem Przetwarzającego wydane mu polecenie lub zalecenie stanowi naruszenie RODO lub innych przepisów dotyczących ochrony danych.

3. Przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie powierzonych danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO. W związku z powyższym będzie w szczególności:

1) stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, zapewniające ich poufność,

2) przetwarzać powierzone dane osobowe w taki sposób, aby zabezpieczyć je przed udostępnianiem ich osobom nieupoważnionym do ich przetwarzania, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów RODO oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem,

3) oceniać regularnie skuteczność zastosowanych środków technicznych i organizacyjnych zapewniających bezpieczeństwo powierzonych danych osobowych,

4) zachowywać w poufności wszystkie powierzone dane osobowe, a także zachowywać w poufności informacji o stosowanych sposobach zabezpieczenia danych osobowych, również po wygaśnięciu Umowy ..... .

§ 10.

1. Przetwarzający niezwłocznie w ciągu 24 godzin od wystąpienia zdarzenia poinformuje Powierzającego o:

1) wszelkich przypadkach naruszenia obowiązków dotyczących ochrony powierzonych do przetwarzania danych osobowych, naruszenia tajemnicy tych danych osobowych lub ich niewłaściwego wykorzystania;

2) wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony powierzonych do przetwarzania danych osobowych prowadzonych w szczególności przez organ właściwy ds. ochrony danych osobowych, policję lub sąd.

2. Przetwarzający zobowiązuje się do udzielenia Powierzającemu, na każde jego żądanie, informacji na temat przetwarzania powierzonych do przetwarzania danych osobowych.

3. Przetwarzający biorąc pod uwagę charakter przetwarzania, będzie pomagać Powierzającemu, poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO.

4. Przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagać będzie Powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO; w szczególności, Przetwarzający zgłasza Powierzającemu, bez zbędnej zwłoki, naruszenie ochrony powierzonych danych osobowych zgodnie z art. 33 ust. 2 oraz przekazuje informacje niezbędne Powierzającemu do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o którym mowa w art. 33 ust. 3 RODO.

§ 11.

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

2. Umowa zaczyna obowiązywać z dniem jej podpisania przez prawidłowo umocowanych przedstawicieli Stron, na czas nieokreślony.

3. W związku rozwiązaniem lub wygaśnięciem Umowy, Przetwarzający zobowiązuje się do zaprzestania wszelkich czynności przetwarzania powierzonych danych osobowych oraz usunięcia tych danych z nośników Przetwarzającego w sposób uniemożliwiający ich odczytanie lub wykorzystanie w możliwie najkrótszym technologicznie i organizacyjnie uzasadnionym terminie (wynikającym z technologii stosowanej przez Przetwarzającego) nie wymagającym niszczenia nośników.

4. Strony przystąpią do wykonania umowy niezwłocznie po jej zawarciu.

5. W sprawach nieuregulowanych Umową zastosowanie mają przepisy Kodeksu cywilnego, RODO i innych właściwych przepisów prawa.

6. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Powierzający **Przetwarzający**

....

Rejestr udostępnień danych osobowych - załącznik nr 9

Rejestr udostępnień danych osobowych

Lp.	Data udostępnienia danych	Podmiot, któremu dane udostępniono (nazwa, adres)	Nazwa zbioru z którego udostępniono dane	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Imię i nazwisko pracownika dokonującego udostępnienia

Obszar przetwarzania danych – załącznik nr 10

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych	
Adres:	Pomieszczenia:
Urząd Miasta ul. Poznańska 2, 58-330 Jedlina-Zdrój	**Piwnica:** – pokój 5A i B - Referat Gospodarki Przestrzennej i Mieszkaniowej, – pokój 5C - Referat Gospodarki Przestrzennej i Mieszkaniowej, Samodzielne Stanowisko ds. Gminnego Utrzymania Porządku, Zieleni i Cmentarza **Parter:** – pokój 1 i 2 - Referat Finansów i Budżetu, – pokój 3 - Referat Spraw Obywatelskich i Ogólnoorganizacyjnych (Ewidencja Ludności), – pokój 3 - Urząd Stanu Cywilnego, – pokój 4 - Biuro Obsługi Klienta, Kasa Urzędu, – pokój 5 - Biuro Gminnych Inwestycji i Infrastruktury Miejskiej, Referat Gospodarki Przestrzennej i Mieszkaniowej **I piętro:** – pokój 6 - Sekretarz Miasta, – pokój 6 - Sekretariat, – pokój 7 - Samodzielne stanowisko ds. Zamówień Publicznych, Zaopatrzenia i Obsługi Urzędu, Referat Spraw Obywatelskich i Ogólnoorganizacyjnych (Kadry), – pokój 8 - Referat Spraw Obywatelskich i Ogólnoorganizacyjnych (Działalność gospodarcza), Samodzielne Stanowisko ds. Obronnych, Obrony Cywilnej i Działań Kryzysowych – pokój 9 - Samodzielne stanowisko ds. obsługi Rady Miasta, Samodzielne Stanowisko ds. Koordynacji Kultury, Sportu i Promocji Gminy **II piętro:** serwerownia, Archiwum Urzędu i Archiwum USC

UZASADNIENIE

Ogólne rozporządzenie o ochronie danych osobowych (RODO) wprowadza nowe obowiązki i zawiera wytyczne, w jaki sposób zabezpieczyć przetwarzane w organizacji dane osobowe. Zgodnie z art. 24 ust. 1 i 2 niniejszego rozporządzenia administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem. Środki te obejmują wdrożenie odpowiednich polityk ochrony danych osobowych. W związku z powyższym Administrator danych osobowych, którym jest Burmistrz Miasta Jedlina-Zdrój, aby wykazać przestrzeganie niniejszego rozporządzenia powinien opracował i przyjąć wewnętrzną polityki ochrony danych.

Niniejsza Polityka ochrony danych osobowych stanowi zbiór wymogów, zasad i regulacji ochrony danych osobowych.

Polityka określa środki techniczne i organizacyjne zastosowane przez Administratora dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.

Mając na uwadze powyższe wydanie niniejszego zarządzenia jest uzasadnione.

Sporządził: A. Sobusiak

spr. 31.12.18r