ZARZĄDZENIE NR 691/2020
Burmistrza Miasta i Gminy Ogrodzieniec
z dnia 4 grudnia 2020 roku

w sprawie: wprowadzenia Polityki ochrony danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec

Na podstawie art.33 ust.3 ustawy z dnia 08 marca 1990 r. o samorządzie gminnym (Dz.U. z 2020r. poz.713 z późn. zm.) oraz 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) – RODO /Dz.Urz. UE L 119, s.1 z poźn.zm./ zarządza się, co następuje:

§ 1.

1. W Urzędzie Miasta i Gminy Ogrodzieniec wprowadza się:
   1) Politykę ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec, stanowiącą **załącznik nr 1** do zarządzenia.
   2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec, stanowiącą **załącznik nr 2** do zarządzenia.

§ 2.

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy Ogrodzieniec do zapoznania się z niniejszym zarządzeniem i przestrzegania zasad zawartych w załącznikach określonych w § 1.
2. Potwierdzeniem zapoznania się z dokumentacją o której mowa w § 1 będzie pisemne oświadczenie pracownika złożone do akt osobowych.

§ 3.

Załączniki do niniejszego zarządzenia określone w § 1 są dokumentami wewnętrznymi i nie podlegają publikacji.

§ 4.

Wykonanie zarządzenia powierza się Sekretarzowi Miasta i Gminy Ogrodzieniec oraz Inspektorowi Ochrony Danych.

§ 5.

Traci moc:

- **Zarządzenie Nr 577/2018** Burmistrza Miasta i Gminy Ogrodzieniec z dnia 30 maja 2018 r. w sprawie: Polityki ochrony danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec.
- **Zarządzenie Nr 89/2019** Burmistrza Miasta i Gminy Ogrodzieniec z dnia 01 kwietnia 2019 r. w sprawie: Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy
Anna Pilarczyk

RADCA PRAWNY
mgr Arkadiusz Janeczko
Kr 1683

„W Z Ó R"

Zgoda na przetwarzanie danych osobowych

Ja niżej podpisana(-ny) oświadczam, iż zgodnie z art. 6 ust.1 lit.a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO /Dz.Urz. UE L 119, s.1 z późn.zm./, wyrażam wyraźną i dobrowolną zgodę (art.7) na przetwarzanie przez **Burmistrza Miasta i Gminy Ogrodzieniec z siedzibą 42-440 Ogrodzieniec Pl.Wolności 25** (Administrator danych) moich danych osobowych zawartych w ..... / w zakresie ..... , w celu .....
.

Jestem świadoma(-my) przysługującego mi prawa do wycofania zgody w dowolnym momencie, jak również faktu, że wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Zgodę mogę odwołać poprzez wysłanie maila opatrzonego podpisem kwalifikowanym na adres **ogrodzieniec@ogrodzieniec.pl** lub za pośrednictwem potwierdzonego profilu **e-PUAP** z informacją o jej odwołaniu, w treści maila wskażę swoje imię i nazwisko, a w tytule wiadomości wpiszę ..... * lub listownie na adres Urzędu Miasta i Gminy Ogrodzieniec.

Miejscowość, dnia ..... r.

.....
(czytelny podpis osoby wyrażającej zgodę)

* w tym miejscu należy podać nazwę czynności, w ramach której udzielono zgody, np. udział w konferencji

Procedura postępowania w przypadku naruszenia ochrony danych osobowych

CEL PROCEDURY

Sprecyzowanie i wdrożenie w Urzędzie jednolitej i przejrzystej procedury postępowania w przypadku naruszenia ochrony danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **IOD** – w zakresie:
   1) oceny czy zgłoszenie stanowi naruszenie ochrony danych osobowych:
      a) jeżeli tak – czy może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych i w związku z tym wymaga zgłoszenia organowi nadzorczemu,
      b) czy zidentyfikowane naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co wiąże się z obowiązkiem zawiadomienia osób, których dane dotyczą,
   2) dokumentowania spraw z zakresu naruszeń.

2. **Pracownik Referatu OR** (pracownik wyznaczony przez Burmistrza)
   1) ewentualne zgłaszanie naruszeń w imieniu administratora do organu nadzorczego, w porozumieniu z IOD;
   2) ewentualne informowanie (zawiadamianie) osób, których dane dotyczą o wystąpieniu naruszenia, w imieniu administratora, w porozumieniu z IOD;
   3) ewentualne podejmowanie odpowiednich czynności zabezpieczających, w porozumieniu z administratorem oraz IOD;
   4) prowadzenie dokumentacji z zakresu naruszeń *(raport o naruszeniu, rejestr naruszeń ochrony danych, zgłoszenie naruszenia, informacja o wystąpieniu naruszenia itp.)*

3. **Administrator systemu informatycznego** (ASI) – w sytuacji gdy naruszenie dotyczy systemów informatycznych, współdziała z IOD.

4. **Pracownicy Urzędu** – w zakresie zgłaszania podejrzenia naruszenia lub naruszenia danych osobowych.

POSTANOWIENIA OGÓLNE PROCEDURY

Procedura dotycząca postępowania w przypadku naruszeń ochrony danych osobowych realizowana jest w dwóch etapach:

1) **wewnętrznym**, którego celem jest ustalenie, czy zgłoszone zdarzenie jest naruszeniem oraz w jaki sposób zidentyfikowane zdarzenie wpłynie na ryzyko dla praw i wolności osób fizycznych,

2) **zewnętrznym**, którego celem jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego oraz poinformowanie osoby, której dane dotyczą, w przypadku gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY
ROZDZIAŁ I – ETAP WEWNĘTRZNY

1. Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, którzy stwierdzili lub podejrzewają wystąpienie zdarzenia, które stanowi naruszenie ochrony danych osobowych, ma **obowiązek zgłoszenia** tego faktu na piśmie Burmistrzowi. W przypadku gdy zgłoszenie dotyczy systemów informatycznych stosowną informację należy przekazać również ASI.

2. Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:
   1) opisanie symptomów naruszenia ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

3. **Stwierdzenie naruszenia** następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych. [1]

4. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, ASI w porozumieniu z IOD podejmuje niezbędne działania zabezpieczające niezwłocznie po otrzymaniu informacji, o której mowa w ust. 3.

5. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego i ma związek z naruszeniem zabezpieczeń fizycznych, odpowiednie czynności zabezpieczające, w porozumieniu z IOD, podejmuje wyznaczony przez Burmistrza pracownik Urzędu, tj.:
   1) nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji Burmistrza;
   2) działa w celu wyjaśnienie okoliczności zdarzenia;
   3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

5. Odmowa udzielenia wyjaśnień lub współpracy z wyznaczonym przez Burmistrza pracownikiem Urzędu oraz IOD, traktowana będzie jako naruszenie obowiązków pracowniczych.

6. **Raport o naruszeniu danych osobowych** opracowuje IOD według wzoru stanowiącego część niniejszej procedury. Raport przedstawiany jest Burmistrzowi. Raport o naruszeniu danych osobowych jest przechowywany przez wyznaczonego przez Burmistrza pracownika Urzędu, wraz z pozostałą dokumentacją z zakresu naruszeń.

7. Każdy incydent związany z ochroną danych, przypadek naruszenia ochrony danych, odnotowywany jest w **rejestrze naruszeń ochrony danych** (załącznik do procedury), prowadzonym przez wyznaczonego przez Burmistrza pracownika Urzędu.

ROZDZIAŁ II – ETAP ZEWNĘTRZNY

1. W przypadku gdy naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych [2], musi być ono zgłoszone organowi nadzorczemu bez zbędnej zwłoki, ale nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia.

2. W przypadku konieczności dokonania **zgłoszenia naruszenia** do organu nadzorczego pismo w tej sprawie przygotowuje wyznaczony przez Burmistrza pracownik Urzędu, w porozumieniu z IOD. W **zgłoszeniu** takim, zgodnie z art.33 RODO, należy w szczególności:
   1) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) wskazać imię i nazwisko oraz dane kontaktowe IOD;
   3) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisać środki zastosowane lub proponowane w Urzędzie w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

---

[1] Żeby zaistniało naruszenie, muszą być spełnione łącznie trzy przesłanki: □ naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie; □ skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych; □ naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

[2] Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.: □ dyskryminacja, □ kradzież tożsamości lub oszustwo dotyczące tożsamości, □ nadużycia finansowe, □ straty finansowe, □ nieuprawnione cofnięcie pseudonimizacji, □ utrata poufności danych osobowych chronionych tajemnicą zawodową, □ naruszenie dobrego imienia □ lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających: □ pochodzenie etniczne, □ poglądy polityczne, □ przekonania religijne lub światopoglądowe, □ przynależność do związków zawodowych, □ dane genetyczne, □ dane dotyczące zdrowia, □ dane dotyczące życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

(źródło: UODO „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" – wersja 1.0 czerwiec 2019, www.uodo.gov.pl)

3. Jeżeli informacji, o których mowa w ust. 2, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki w następujący sposób:
   1) po dokonaniu pierwszego zgłoszenia można przekazywać na bieżąco organowi nadzorczemu aktualne informacje;
   2) w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

4. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, **bez zbędnej zwłoki zawiadamia się** o tym osoby, których dane dotyczą. [3]

6. Za realizację obowiązku wskazanego w ust. 5 odpowiada wyznaczony przez Burmistrza pracownik Urzędu, w porozumieniu z IOD.

7. **Zawiadomienie** należy przygotować jasnym i prostym językiem (art.34 RODO). Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.

8. Zawiadomienie, o którym mowa w ust. 5, nie jest wymagane, w następujących przypadkach:
   1) w Urzędzie wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) w Urzędzie zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) wymagałoby ono niewspółmiernie dużego wysiłku, w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

9. Należy wykazać przed organem nadzorczym, że został spełniony przynajmniej jeden z warunków wskazanych
   w ust. 8 w przypadku braku powiadomienia osób, których dane naruszono.

---

[3] Przykładowa klasyfikacja powagi naruszeń praw i wolności osób fizycznych:
A. Poziom: - 1. ograniczone naruszenie, - 2. naruszenie, - 3. znaczące naruszenie, - 4. najwyższy stopień naruszenia.
B. Opis wpływu (bezpośredniego i pośredniego):
- 1. Osoba, której dane dotyczą, nie odczuje wpływu lub zetknie się z niewielką liczbą niedogodności, które łatwo może przezwyciężyć,
- 2. Osoba, której dane dotyczą, może napotkać znaczące niedogodności, które będzie w stanie przezwyciężyć mimo kilku trudności,
- 3. Osoby, których dane dotyczą, mogą napotkać znaczące konsekwencje, które powinny móc przezwyciężyć mimo realnych i dużych trudności,
- 4. Osoba, której dane dotyczą, może napotkać poważne i nieodwracalne konsekwencje, których może nie być w stanie przezwyciężyć.

(źródło: Ochrona Danych Osobowych Przewodnik po ustawie i RODO z wzorami, red. Maciej Gawroński, wyd. Wolters Kluwer, Warszawa 2018)

„W Z Ó R"

Miejscowość, dnia ..... r.

Raport o naruszeniu danych osobowych

1) Miejsce, dokładny czas i data naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych *(piętro, nr pokoju, obszar, godzina itp.)*
.....
.....

2) Osoba / osoby powodujące naruszenie *(które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych):*
.....
.....

3) Charakter naruszenia – stwierdzone nieprawidłowości *(tj. nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych, wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania, brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną):*
.....
.....

4) Informacje o danych, które zostały lub mogły zostać ujawnione *(nazwa czynności – procesu przetwarzania, w ramach którego doszło do naruszenia ochrony danych):*
.....
.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem: .....
.....

6) Kategorie danych osobowych, których dotyczy naruszenie *(zwykłe, szczególne):* .....

7) Kategorie osób, których dane dotyczą, dotkniętych naruszeniem: .....

8) Liczba osób, których dane dotyczą, dotkniętych naruszeniem: .....

9) Środki bezpieczeństwa zastosowane przed naruszeniem: .....

10) Krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacji, w tym ochrony danych osobowych *(przebieg zdarzenia, opis zachowania uczestników, podjęte działania ad hoc):* .....
.....
.....

11) Możliwe konsekwencje naruszenia:
   a) dla Urzędu:
   .....
   b) dla osób których dane dotyczą:
   .....

12) Zalecenia naprawcze w celu: – przywrócenia stanu zgodnego z prawem, – zminimalizowania negatywnych skutków naruszenia dla osób, których dane dotyczą, – zminimalizowania ryzyka wystąpienia analogicznego naruszenia w przyszłości:
.....
.....

13) Ocena pod kątem zgłoszenia naruszenia organowi nadzorczemu (art.33 RODO):
.....
.....

14) Ocena pod kątem zawiadomienia osób, których dane dotyczą, o naruszeniu (art.34 RODO):
.....

.....

Sporządzający raport *(imię i nazwisko, funkcja):*

.....

(czytelny podpis)

„Zapoznałem się"

(czytelny podpis Administratora)

„W Z Ó R"

REJESTR

naruszeń ochrony danych osobowych

L.p	Informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia			Okoliczności naruszenia		
	Data zdarzenia	Data i źródło uzyskania informacji	Data i godzina stwierdzenia naruszenia	Charakter naruszenia	Kategorie osób / Przybliżona Liczba osób, których dane dotyczą (jeżeli to możliwe)	Kategoria danych: zwykłe, szczególne i liczba wpisów (jeżeli to możliwe)
1.	2.	3.	4.	5.	6.	7.

Skutki naruszenia	Środki naprawcze i zaradcze			Zgłoszenie naruszenia organowi nadzorczemu PUODO			Uwagi
Opis konsekwencji naruszenia	Czy poinformowano osoby których dane dotyczą ? (jeśli tak, to w jaki sposób, jeśli nie, to dlaczego)	Działania naprawcze	Działania zaradcze	Czy dokonano zgłoszenia (jeśli nie, przyczyna niedokonania zgłoszenia)	Data zgłoszenia	Data zgłoszenia uzupełniającego	Np. o poinformowaniu CERT Polska, organów ścigania
8.	9.	10.	11.	12.	13.	14.	15.

Procedura postępowania w zakresie oceny skutków dla ochrony danych osobowych (OSOD) w angielskiej wersji Data Protection Impact Assessment (DPIA)

CEL PROCEDURY

Ocena jakie skutki dla systemu ochrony danych w Urzędzie, niesie ze sobą planowana, modyfikowana czynność/operacja przetwarzania danych osobowych, w nowych lub istniejących procesach, w szczególności z użyciem nowych technologii.

Wynikiem przeprowadzania procedury jest:

a) określenie konieczności wykonania oceny;
b) dokumentacja związana z oceną skutków dla ochrony danych;
c) decyzja o rozpoczęciu, modyfikacji lub zaniechaniu prowadzenia ocenianych operacji przetwarzania;
d) decyzja o uruchomieniu procedury uprzednich konsultacji z organem nadzorczym;
e) zapisy z ocenianych operacji przetwarzania.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach – w zakresie prawidłowej realizacji procedury oceny skutków dla ochrony danych osobowych, w tym przeprowadzania konsultacji z IOD kwestii dot.:

1) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych;
2) metodologii przeprowadzenia oceny skutków dla ochrony danych osobowych;
3) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń naruszenia praw i wolności osób, których dane dotyczą;
4) prawidłowości przeprowadzonej oceny skutków dla ochrony danych osobowych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy stosować).

IOD – w zakresie udzielania konsultacji pracownikom Urzędu oraz prowadzenia konsultacji z organem nadzorczym.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Procedura oceny skutków ma zastosowanie do wszystkich czynności i operacji przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Procedurą objęte są dane osobowe w rozumieniu art.4 pkt 1 RODO.
3. Procedura odnosi się do czynności/operacji przetwarzania dla których współczynnik ryzyka naruszenia lub ograniczenia praw lub wolności osób, których dane osobowe podlegają przetwarzaniu kwalifikuje dane operacje do przeprowadzenia niniejszej procedury. „Przetwarzanie" definiowane jest zgodnie z art.4 pkt 2 RODO.
4. Procedurę należy uruchomić w przypadku projektowania nowych czynności przetwarzania, modyfikacji lub zmiany istniejących czynności, w oparciu o *„Procedurę zarządzania ryzykiem"* – ***załącznik nr 13, 13a, 13b, 13c, 13d*** do zarządzenia.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

1. **Określenie konieczności przeprowadzenia oceny skutków dla ochrony danych**

   1) ze względu na fakt, że ocena ryzyka jest tylko jednym z czynników determinujących konieczność przeprowadzenia oceny DPIA niezbędne jest sprawdzenie, czy przeprowadzenie oceny DPIA nie wynika z innych przesłanek określonych w **art.35 RODO**.

   2) Po przeprowadzeniu procedury oceny ryzyka dla czynności/operacji przetwarzania należy określić czy przetwarzanie danych osobowych jest niezbędne do wypełnienia istniejącego obowiązku prawnego **(art.6 lit. c RODO)** lub przetwarzanie jest niezbędne do zadania realizowanego w interesie publicznym

lub w ramach sprawowania władzy publicznej powierzonej administratorowi (**art.6 lit e RODO**). Jeśli ocena ryzyka wskazuje, że jeden z powyższych warunków został spełniony – oceny DPIA nie wykonuje się (**art.35 ust.10 RODO**)

3) Jeśli żaden z powyższych warunków nie został spełniony, a poziom ryzyka określono jako **wysoki** (wymaga DPIA), konieczne jest zweryfikowanie czy badana czynność/operacja przetwarzania nie figuruje w ***„wykazie rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych."*** [1] W sytuacji, kiedy czynność/operacja figuruje we wskazanym wykazie – oceny DPIA nie wykonuje się. W sytuacji, kiedy czynności/operacje nie znajdują się we wskazanym wykazie należy wykonać ocenę DPIA zgodnie z niniejszą procedurą (**art.35 ust.5 RODO**).

4) Jeśli czynność/operacja spełnia warunki zwolnienia z wykonywania oceny DPIA na podstawie przesłanek wskazanych w pkt 2), a poziom ryzyka określono jako **niski** (nie wymaga DPIA), należy zweryfikować, czy czynność/operacja przetwarzania danych spełnia **co najmniej dwa kryteria** wskazane w ***„wykazie rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony".*** [2] Jeśli tak, należy wykonać ocenę DPIA (**art.35 ust.3 RODO**).

5) Jeśli wykonanie oceny DPIA nie wynika z pkt 4) należy sprawdzić, czy czynność/operacja nie figuruje w ***„wykazie rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony".*** W sytuacji, kiedy czynność/operacja figuruje we wskazanym wykazie wykonywana jest ocena DPIA bez względu na określony poziom ryzyka. Jeśli czynność/operacja nie znajdują się we wskazanym wykazie nie należy wykonywać oceny (**art.35 ust.4 RODO**).

2. Wykonanie oceny DPIA

1) Ocenę należy wykonać zgodnie z *„Arkuszem oceny DPIA"*, ***załącznik*** do procedury, wypełniając tabelę nr 1 i 2.
2) Arkusz oceny zawiera systematyczny opis planowanych czynności/operacji przetwarzania zawierający informacje dotyczące danych osobowych podlegających przetwarzaniu.
3) Ocenę, czy przetwarzanie jest niezbędne oraz proporcjonalne w stosunku do celów.
4) Informacje na temat przeprowadzonej analizy ryzyka dla przetwarzania.
5) Opis środków stosowanych w celu zaradzenia ryzyku (środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych oraz wykazać, że przestrzegane jest RODO – ***załącznik*** do procedury – tabela nr 2.
6) Dane z tabeli nr 2 z kolumny podsumowanie należy przenieść do *„Arkusza szacowania ryzyka"* – ***załącznik nr 13a*** do zarządzenia i określić w jakim stopniu zastosowane środki wpłynęły na jego obniżenie. Wynik oceny ryzyka z *„arkusza"* należy wpisać do kolumny *„czy ryzyko akceptowalne"* w tabeli nr 2.

3. Uruchomienie procedury uprzednich konsultacji z organem nadzorczym.

1) W sytuacji, kiedy poziom ryzyka po zastosowaniu opisanych w tabeli nr 2 środków, został obniżony do akceptowalnego poziomu, należy podjąć działania zmierzające do ich wdrożenia (plan postępowania z ryzykiem).
2) W sytuacji, kiedy pomimo zaplanowanych środków pomniejszających ryzyko jego poziom przekracza ustalony wskaźnik graniczny, należy uruchomić procedurę uprzednich konsultacji z organem nadzorczym (**art.36 RODO**).

4. Zapisy

W celu zapewnienia rozliczalności wynikającej z przepisów RODO należy skompletować wszystkie przeprowadzone analizy. Dokumenty należy wydrukować, podpisać przez osoby dokonujące analizy i zarchiwizować.

---

[1] Organ nadzorczy może taki wykaz ustanowić i podać do publicznej wiadomości.

[2] Publikowany przez organ nadzorczy (Monitor Polski – Dziennik Urzędowy RP – Komunikat Prezesa UODO).

„W Z Ó R"

Arkusz oceny DPIA

I. **Administrator** – Burmistrz Miasta i Gminy Ogrodzieniec z siedzibą 42-440 Ogrodzieniec, Pl.Wolności 25.

II. **Inspektor Ochrony Danych** – Pan/Pani .....

Tabela nr 1.

1.	Kryteria dla których wymagane jest przeprowadzenie oceny	
2.	Cel przetwarzania	
3.	Nazwa czynności/operacja	
4.	Opis czynności	
5.	Nowa, czy istniejąca operacja	
6.	Podstawa prawna przetwarzania	
7.	Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora	
8.	Opis danych osobowych podlegających przetwarzaniu	
9.	Kategorie osób których dane dotyczą	
10.	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów	
11.	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą z *„arkusza szacowania ryzyka"* (procedura zarządzania ryzykiem)	
12.	Czy, a jeśli tak to w jaki sposób, zapewniono realizację praw osób, których dane podlegają przetwarzaniu	

13.	Jeśli wymagana jest zgoda – w jaki sposób realizowane jest/będzie zbieranie zgód	
14.	Czy uwzględniono okres przechowywania danych	
15.	Czy w przetwarzaniu będzie brał udział podmiot przetwarzający ? Jeśli tak to czy spełnia warunki określone w RODO	
16.	Czy dane przekazywane poza EOG, a jeśli tak to jakie środki bezpieczeństwa zostaną zastosowane ?	

Tabela nr 2

Środki planowane w celu zaradzenia ryzyku				
Lista zidentyfikowanych ryzyk wraz z opisem	Opis środków technicznych (fizycznych i informatycznych) służących zaradzeniu ryzyku	Opis środków organizacyjnych służących zaradzeniu ryzyku	Podsumowanie	Czy ryzyko jest akceptowalne ?

Miejscowość, dnia ..... r.

Sporządził:

.....
(czytelny podpis)

Procedura postępowania w zakresie przeprowadzania i dokumentowania wyników analizy ryzyka - zarządzanie ryzykiem

PODSTAWOWE DEFINICJE

akceptacja ryzyka	– decyzja uprawnionej osoby o zaniechaniu działań mających na celu zmianę poziomu ryzyka
analiza ryzyka	– systematyczne podejście mające na celu zidentyfikowanie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości
estymacja	– proces przypisywania wartości poziomowi ryzyka
dostępność informacji uprawniony	– właściwość polegająca na tym, że informacja jest możliwa do wykorzystania przez podmiot na jego żądanie, w założonym czasie
identyfikowanie ryzyka	– proces znajdowania, zestawiania i charakteryzowania przyczyn ryzyka
incydent	– pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań organizacji i zagrażają bezpieczeństwu informacji
integralność informacji	– właściwość polegająca na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony
ocena ryzyka	– proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
podatność	– słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie
postępowanie z ryzykiem	– proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka
poziom ryzyka	– produkt operacji na wartości przypisanej skutkowi i wartości związanej z prawdopodobieństwem zaistnienia zdarzenia powodującego skutek
poufność informacji	– właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom
ryzyko	– skutek niepewności w odniesieniu do ustalonego celu
ryzyko szczątkowe	– ryzyko, którego poziom nie przekracza akceptowanej wartości
skutek	– negatywna zmiana w odniesieniu do zaplanowanego poziomu miernika celu w wyniku oddziaływania zagrożenia
szacowanie ryzyka	– całościowy proces analizy i oceny ryzyka
właściciel ryzyka	– osoba odpowiedzialna za zarządzanie danym ryzykiem
zagrożenie	– potencjalna przyczyna niepożądanego oddziaływania
zarządzanie ryzykiem	– skoordynowane działania mające na celu kierowanie i sterowanie ryzykiem

CEL PROCEDURY

Sprecyzowanie i wdrożenie w Urzędzie, jednolitej i przejrzystej procedury zarządzania ryzykiem, w celu zastosowania odpowiednich środków technicznych i organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku, wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Burmistrz** (Administrator) – w zakresie:
   1) kształtowania i wdrażania procedury zarządzania ryzykiem;
   2) nadzoru i monitorowania skuteczności procesu zarządzania ryzykiem;
   3) wyznaczania poziomu akceptowalnego dla każdego ryzyka;
   4) podejmowania decyzji dotyczących sposobu reakcji na poszczególne ryzyka – działania zaradcze.

2. **Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach** – w zakresie:
   1) identyfikacji ryzyk związanych z realizacją przydzielonych czynności przetwarzania danych osobowych;
   2) wskazywania właścicieli zidentyfikowanych ryzyk;
   3) przeprowadzania analizy zidentyfikowanego ryzyka;
   4) proponowania sposobu postępowania w odniesieniu do poszczególnych ryzyk – propozycja reakcji na ryzyko;
   5) wdrażania działań zaradczych w stosunku do zidentyfikowanego ryzyka;
   6) systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich Administratorowi.

3. **IOD** – w zakresie:
   1) koordynowania procesu zarządzania ryzykiem;
   2) udzielania konsultacji w zakresie dokonywania oceny, czy dana czynność przetwarzania danych osobowych, dla której wykonywana jest identyfikacja ryzyk, powoduje wystąpienie wysokiego ryzyka naruszenia praw i wolności osób fizycznych których dane są przetwarzane – czy wymaga przeprowadzenia oceny skutków dla ochrony danych (**OSOD**), w angielskiej wersji Data Protection Impact Assessment (**DPIA**).

POSTANOWIENIA OGÓLNE PROCEDURY

1. Procedura zarządzania ryzykiem obejmuje:
   1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
   2) zasady i tryb identyfikacji ryzyka;
   3) zasady i tryb dokonywania analizy ryzyka;
   4) zasady określania właściwej reakcji na ryzyko.

2. Zarządzanie ryzkiem jest procesem ciągłym i nie ogranicza się do działań określonych w pkt 1.

3. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:
   1) rozpoznanie, czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością Urzędu w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;
   2) ocenę ryzyka i jego istotności, przy pomocy **„Arkusza szacowania ryzyka"** dalej: „arkusz", określony w ***załączniku 13 a***;
   3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;
   4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

4. Procedura zarządzania ryzykiem ma zastosowanie do wszystkich:
   a) stanowisk pracy (wskazanych w **Regulaminie organizacyjnym UMiG Ogrodzieniec**) na których odbywa się przetwarzanie danych osobowych,
   b) czynności przetwarzania danych osobowych, zidentyfikowanych w Urzędzie i opisanych w prowadzonym ***„Rejestrze czynności przetwarzania danych"*** (RCPD).

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

1. **Identyfikacja ryzyka:**

1) identyfikacja ryzyk prowadzona jest dla wszystkich czynności przetwarzania danych;
2) w procesie identyfikacji ryzyka uwzględnia się kryteria podziału zagrożeń:
   a) lokalizacja źródła (wewnętrzne, zewnętrzne),
   b) przyczyna (działanie przypadkowe człowieka, działanie umyślne człowieka, naturalna),
3) każde zidentyfikowane ryzyko ujmuje się w arkuszu;
4) dla każdego zidentyfikowanego ryzyka ustala się jego właściciela;
5) każdy pracownik ma prawo i obowiązek zgłaszania Administratorowi, ryzyk zidentyfikowanych podczas wykonywania przydzielonych czynności przetwarzania danych osobowych.

2. Analiza ryzyka

1) Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

2) Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

5) W celu dokonania oceny ryzyka wykorzystuje się **„Matrycę ryzyka"**, którą stanowi macierz prawdopodobieństwo – skutek (R = P x S) – określona w ***załączniku 13 b***;

3) Mapa ryzyka definiuje ryzyka na:
   a) niski poziom,
   b) średni poziom,
   c) wysoki poziom,
   d) bardzo wysoki poziom.

4) Przy ocenie prawdopodobieństwa wystąpienia ryzyka, przyjmuje się skalę punktową od 1 do 4, wykorzystując **„Tabelę oceny prawdopodobieństwa wystąpienia ryzyka (zdarzenia/zagrożenia)"** – określona w ***załączniku 13 c***, gdzie:
   a) 1 – oznacza ryzyko mało prawdopodobne,
   b) 2 – oznacza ryzyko możliwe,
   c) 3 – oznacza ryzyko prawdopodobne,
   d) 4 – oznacza ryzyko prawie pewne.

5) Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 4, wykorzystując **„Tabelę punktowa – sposób oceny skutku ryzyka"** – określona w ***załączniku 13 d***, gdzie:
   a) 1 – oznacza niski skutek wystąpienia ryzyka;
   b) 2 – oznacza średni skutek wystąpienia ryzyka;
   c) 3 – oznacza wysoki skutek wystąpienia ryzyka;
   d) 4 – bardzo wysoki skutek wystąpienia ryzyka.

3. Reakcja na ryzyko

Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

a) akceptacja ryzyka (zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie) ;
b) akceptacja ryzyka, monitowanie (zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka);
c) modyfikacja ryzyka za pomocą działań które mogą być przesunięte w czasie, stałe monitorowanie (zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka);
d) ryzyko nieakceptowalne, modyfikacja ryzyka za pomocą działań natychmiastowych (działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do niższego poziomu).

Arkusz szacowania ryzyka [1]

I. va komórki organizacyjnej / samodzielne stanowisko: .....

II. Właściciel procesu (ryzyka) / stanowisko: ..... / .....

III. Nazwa procesu/operacji przetwarzania danych (źródło ryzyka): .....

IV. Cel przetwarzania: .....

L.p	**Opis zidentyfikowanego ryzyka – zagrożenia** [2] (źródło potencjalnej szkody, istnieje ryzyko, że ...)	**PRAWDOPODOBIEŃSTWO wystąpienia ryzyka** (skala 1-4 pkt) **P**	**SKUTEK wystąpienia ryzyka** (skala 1-4 pkt) **S**	**Poziom wpływu RYZYKA na bezpieczeństwo / wartość ryzyka** (skala 1-16 pkt) **R = P x S**	**Ocena ryzyka** (poziom: niski, średni, wysoki, bardzo wysoki) / **Reakcja na ryzyko** (akceptacja, monitorowanie, modyfikacja, ryzyko nieakceptowalne)	**Istniejące mechanizmy kontroli** (aktualne środki ograniczające ryzyko)	**Propozycje reakcji na ryzyko**	**UWAGI / Decyzja Administratora** (uzgodnione działania)
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**
1.								
2.								

Miejscowość, dnia : ..... r.

.....
(czytelny podpis właściciela ryzyka)

[1] Nie można wskazać, jednej uniwersalnej metody szacowania ryzyka. Każda organizacja w zależności od rodzaju prowadzonej działalności może opracować własną metodę szacowania ryzyka. GIODO. Jak stosować podejści a ryzyku ? Poradnik RODO podejście oparte na ryzyku /część 2/ – grudzień 2017 r.

[2] Przykładowe kryteria podziału zagrożeń: – lokalizacja źródła (wewnętrzne, zewnętrzne), – przyczyna (działanie przypadkowe człowieka, działanie umyślne człowieka, naturalna).

L E G E N D A :

I. wpisz nazwę komórki organizacyjnej / samodzielne stanowisko pracy (zgodnie z Regulaminem organizacyjnym)
II. wpisz imię i nazwisko / stanowisko służbowe (zgodnie z Regulaminem organizacyjnym)
III. wpisz konkretną czynność przetwarzania z RCPD np. ewidencja ludności, dowody osobiste - lub wpisz realizacja czynności opisanych w RCPD np. poz. od 4 do 8
IV. wpisz cel przetwarzania z RCPD np. prowadzenie rejestru mieszkańców, wydawanie, wymiana i unieważnianie dowodów osobistych - lub wpisz przetwarzanie danych osobowych w wersji papierowej i elektronicznej, wynikające z zadań realizowanych przez w/wym. komórkę organizacyjną / samodzielne stanowisko

1. **Kolumna** - Liczba porządkowa 1, 2, 3, 4 ... itd.

2. **Kolumna** - wpisz zagrożenia np.: możliwość zniszczenia/zagubienia/kradzieży nośnika danych, pozostawienie danych/pomieszczenia bez nadzoru, awaria systemu/sprzętu IT, zagrożenie zalaniem pomieszczenia archiwum/serwerowni, zagrożenie upublicznieniem danych, praca ASI w kilku podmiotach/możliwość porzucenia pracy, wykorzystywanie sprzętu służbowego do celów prywatnych bez zgody Administratora, zniszczenie danych w stopniu umożliwiającym ich odzyskanie, opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji, nie wykonywanie regularnie kopii zapasowych/bezpieczeństwa, przechowywanie identyfikatora (loginu) i hasła w niewłaściwy sposób, dopuszczenie do kopiowania danych i utraty kontroli nad kopią, pozostawienie wydruków danych na ogólnodostępnej drukarce, nieautoryzowane wykonanie kopii klucza do pomieszczenia biurowego, przypadkowe lub celowe działanie użytkownika (skasowanie danych), naruszenie podstawowych zasad bezpieczeństwa informacji, zagrożenie naruszenia praw autorskich, oprogramowanie złośliwe, zaniedbania służby ochrony obiektu, możliwość skorzystania z konta przez personel sprzątający, przełamanie zabezpieczeń, zagrożenie sabotażem komputerowym, cyberterroryzm, błędna lub brak podstawy prawnej przetwarzania danych, niewypełnienie obowiązku informacyjnego, brak przejrzystego przekazywania informacji o przetwarzaniu danych, brak zgody osoby której dane dotyczą, na przetwarzanie danych itp.

3. **Kolumna** - wpisz cyfrę wg skali 1-4 pkt z Tabeli oceny prawdopodobieństwa wystąpienia ryzyka (załącznik nr 13 c)

4. **Kolumna** - wpisz cyfrę wg skali 1-4 pkt z Tabeli punktowej - sposób oceny skutku ryzyka (załącznik nr 13 d)

5. **Kolumna** - wpisz cyfrę wg skali 1-16 z Matrycy ryzyka, gdzie R = P x S (załącznik nr 13 b)

6. **Kolumna** - wpisz ocenę ryzyka i reakcje na ryzyko z Matrycy ryzyka (załącznik nr 13 b)

7. **Kolumna** - wpisz istniejące mechanizmy kontroli np. Polityka ochrony danych, Instrukcja zarządzania systemem służącym do przetwarzania danych, Polityka prywatności, regulamin monitoringu, weryfikacja zapisów umowy, klauzule informacyjne w łatwo dostępnych miejscach, informowanie osób, których dane dotyczą o prawach im przysługujących, zasady bezpieczeństwa informacji i danych, polityka czystego biurka i ekranu, polityka kluczy, system kontroli dostępu, lokalny system alarmowy, ewidencja wejścia/wyjścia, system monitoringu wizyjnego, autoryzowane nośniki danych, program szyfrujący dane, regulamin ... , instrukcja ... , wytyczne .... , itp.

8. **Kolumna** - wpisz propozycję reakcji na ryzyko np. przeprowadzić szkolenie/instruktaż, przeprowadzić kontrolę/audyt, dokonać przeglądu i uaktualnienia stosowanych środków organizacyjnych i technicznych, wprowadzić obowiązek szyfrowania wszystkich danych, wprowadzić zakaz korzystania ze sprzętu IT do celów prywatnych, wprowadzić obowiązek noszenia identyfikatorów pracowniczych, wprowadzić elektroniczny system kontroli dostępu, wprowadzić system monitoringu na stanowisku pracy, zakupić większą ilość szaf, niszczarek lub zastosować tzw. „bezpieczne pojemniki" , zatrudnić dodatkowego pracownika, dokonywać systematycznej kontroli dokumentów, rozbudować system monitoringu, stworzyć bezpieczne warunki przechowywania dokumentów, wykonywać kopie zapasowe w formie elektronicznej, prowadzić okresowe kontrole, przeglądy, dokonywać bieżących napraw, zakupić nowy komputer, wymienić zamki w drzwiach, szafach, itp.

9. **Kolumna** - wypełnia Administrator

Matryca ryzyka (skala dopuszczalności ryzyka)

LEGENDA:

- **NISKI POZIOM** (1 - 2) - **akceptacja ryzyka** (zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie)
- **ŚREDNI POZIOM** (3 - 4) - **akceptacja ryzyka, monitowanie** (zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka)
- **WYSOKI POZIOM** (6 - 8) - **modyfikacja ryzyka** za pomocą działań które mogą być przesunięte w czasie, stałe monitorowanie (zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka)
- **BARDZO WYSOKI POZIOM** (9 - 16) - **ryzyko nieakceptowalne**, modyfikacja ryzyka za pomocą działań natychmiastowych (działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do niższego poziomu)

RYZYKO (R = P x S)			SKUTEK (S)			
			Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4
PRAWDOPODOBIEŃSTWO (P)	Prawie pewne	4	Ś (4)	W (8)	B.W (12)	B.W (16)
	Prawdopodobne	3	Ś (3)	W (6)	B.W (9)	B.W (12)
	Możliwe	2	N (2)	Ś (4)	W (6)	W (8)
	Mało prawdopodobne	1	N (1)	N (2)	Ś (3)	Ś (4)

Tabela oceny prawdopodobieństwa wystąpienia ryzyka (zdarzenia/zagrożenia)

Prawdopodobieństwo wystąpienia ryzyka	Skala / punkty	Opis / przesłanki
Mało prawdopodobne (0 – 20 %)	**1**	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się raz lub nie zdarzy się w ciągu roku
Możliwe (powyżej 20 do 60 %)	**2**	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się raz lub kilka razy w ciągu roku
Prawdopodobne (powyżej 60 do 80 %)	**3**	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku
Prawie pewne (powyżej 80 %)	**4**	Przewiduje się, że zdarzenie z pewnością wystąpi raz w miesiącu lub częściej

Tabela punktowa - sposób oceny skutku ryzyka

SKUTEK wystąpienia ryzyka	Skala / Punkty	Opis / przesłanki
Niski	**1**	– Naruszenie bezpieczeństwa aktywa w zakresie poufności, integralności, dostępności może w niewielkim stopniu utrudnić pracę z aktywem. – Główne zadania w zakresie danego aktywa mogą być nadal realizowane. – Brak znaczącego wpływu na wymagany poziom bezpieczeństwa informacji. – Osoby, których dane osobowe są objęte zdarzeniem, praktycznie nie odczuwają skutków.
Średni	**2**	– Naruszenie bezpieczeństwa aktywa w zakresie poufności, integralności, dostępności może utrudnić pracę z aktywem, jednak można przywrócić pracę łatwo dostępnymi środkami. – Naruszenie ma ograniczony wpływ na wymagany poziom bezpieczeństwa. – Występuje niewielka odpowiedzialność finansowa. Raczej nie występują kary pieniężne lub są stosunkowo niskie. – Osoby, których dane osobowe są objęte zdarzeniem, mogą odczuwać konsekwencje, które są w stanie rozwiązać pomimo kilku trudności.
Wysoki	**3**	– Naruszenie bezpieczeństwa aktywa w zakresie poufności, integralności lub dostępności może znacząco zakłócić pracę z aktywem. – Naruszenie ma istotny wpływ na bezpieczeństwo informacji. – Możliwa jest odpowiedzialność prawna. – Występuje średnia odpowiedzialność finansowa, w tym mogą występować średnie kary pieniężne. – Występuje negatywny rozgłos medialny na skalę lokalną. – Osoby, których dane osobowe są objęte zdarzeniem, mogą odczuwać istotne konsekwencje, które są w stanie rozwiązać z wieloma trudnościami.
Bardzo wysoki	**4**	– Naruszenie bezpieczeństwa aktywa w zakresie poufności, integralności, dostępności drastycznie zakłóca lub całkowicie uniemożliwia pracę z aktywem. – Naruszenie ma krytyczny wpływ na wymagany poziom bezpieczeństwa informacji. – Występuje poważna odpowiedzialność prawna. – Występuje poważna odpowiedzialność finansowa, w tym mogą występować wysokie kary pieniężne. – Występuje negatywny rozgłos medialny na skalę krajową. – Osoby, których dane osobowe są objęte zdarzeniem, mogą odczuwać istotne lub nawet nieodwracalne konsekwencje.

ZARZĄDZENIE NR ..... / 2020
Burmistrza Miasta i Gminy Ogrodzieniec
z dnia ..... 2020 roku

w sprawie: wprowadzenia Polityki ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec

Na podstawie art.33 ust.3 ustawy z dnia 08 marca 1990 r. o samorządzie gminnym (Dz.U z 2019 r. poz.506 z pożn.zm.) oraz 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) – RODO /Dz.Urz. UE L 119, s.1 z pożn.zm./ zarządza się, co następuje

§ 1.

1. W Urzędzie Miasta i Gminy Ogrodzieniec wprowadza się:
   1) Politykę ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec, stanowiącą *załącznik nr 1* do zarządzenia,
   2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec, stanowiącą *załącznik nr 2* do zarządzenia.

1. Określa się :
   1) wzór oświadczenia o zapoznaniu się z treścią Polityki ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec, stanowiący *załącznik nr 3* do zarządzenia;
   2) procedurę postępowania w zakresie udzielenia upoważnienia do przetwarzania danych osobowych, stanowiącą *załącznik nr 4* do zarządzenia;
   3) procedurę postępowania dot. sporządzania rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania danych, stanowiącą *załącznik nr 5* do zarządzenia;
   4) procedurę postępowania w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych, stanowiącą *załącznik nr 6* do zarządzenia;
   5) ramowy wzór klauzuli informacyjnej w przypadku zbierania danych osobowych od osoby, której dane dotyczą, stanowiący *załącznik nr 7* do zarządzenia;
   6) ramowy wzór klauzuli informacyjnej w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą, stanowiący *załącznik nr 8* do zarządzenia;
   7) procedurę postępowania dot. wpłynięcia wniosku obywatela w zakresie przysługujących mu praw oraz wniosku podmiotu o udostępnienie danych osobowych, stanowiącą *załącznik nr 9* do zarządzenia;
   8) ramowy wzór zgody na przetwarzanie danych osobowych, stanowiący *załącznik nr 10* do zarządzenia;
   9) procedurę postępowania w przypadku naruszenia ochrony danych osobowych, stanowiącą *załącznik nr 11* do zarządzenia;
   10) procedurę postępowania w zakresie oceny skutków dla ochrony danych osobowych, stanowiącą *załącznik nr 12* do zarządzenia;
   11) procedurę postępowania w zakresie przeprowadzania i dokumentowania wyników analizy ryzyka, stanowiącą *załącznik nr 13, 13a, 13b, 13c, 13d* do zarządzenia.

§ 2.

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy Ogrodzieniec do zapoznania się z niniejszym zarządzeniem i przestrzegania zasad zawartych w dokumentach określonych w § 1.
2. Potwierdzeniem zapoznania się z dokumentacją o której mowa w § 1 będzie pisemne oświadczenie pracownika złożone do akt osobowych.

§ 3.

Niniejsza Polityka oraz Instrukcja jest dokumentem o charakterze wewnętrznym i nie może być udostępniana osobom trzecim oraz innym podmiotom, w żadnej formie, bez zgody Burmistrza.

§ 4.

Wykonanie zarządzenia nadzoruje Sekretarz Gminy Ogrodzieniec.

§ 5.

Traci moc:

- **Zarządzenie Nr 577/2018** Burmistrza Miasta i Gminy Ogrodzieniec z dnia 30 maja 2018 r. w sprawie: Polityki ochrony danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec.
- **Zarządzenie Nr 89/2019** Burmistrza Miasta i Gminy Ogrodzieniec z dnia 01 kwietnia 2019 r. w sprawie: Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 3 do zarządzenia

„WZÓR"

.....
(stanowisko / jedn.org)

.....
(imię i nazwisko)

OŚWIADCZENIE
o zapoznaniu się z treścią Polityki i Instrukcji

Oświadczam, iż zapoznałam(-łem) się z obowiązującą treścią:

a) Polityki ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec,

b) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec,

zrozumiałam(-łem) ich treść i zobowiązuję się do przestrzegania zawartych w tych dokumentach zasad, reguł i postanowień.

.....
(miejscowość dnia)

.....
(czytelny podpis)

Procedura postępowania w zakresie udzielenia upoważnienia do przetwarzania danych osobowych /art. 29 RODO/

CEL PROCEDURY

Sprecyzowanie i wdrożenie w Urzędzie jednolitej i przejrzystej procedury udzielenia upoważnienia do przetwarzania danych osobowych oraz przedstawienie wzoru upoważnienia.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Burmistrz** (Administrator) – w zakresie wydawania upoważnień do przetwarzania danych osobowych na mocy przepisów prawa.
2. **Pracownik Referatu OR** (pracownik wyznaczony przez Burmistrza) – w zakresie przygotowania upoważnienia (na podstawie zatwierdzonego wniosku) i gromadzenia upoważnień, o których mowa w ww. procedurze oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
3. **Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach** – w zakresie występowania z wnioskiem o nadanie upoważnień do przetwarzania danych osobowych dla podległych pracowników oraz innych osób im podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej).
4. **Przewodniczący komisji** (np. socjalnej, innej) – w zakresie występowania z wnioskiem o nadanie upoważnień do przetwarzania danych osobowych dla podległych im członków komisji.
5. **Administrator Systemu Informatycznego** (ASI) – w zakresie przydzielenia identyfikatora w systemie IT.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Burmistrz wydaje upoważnienia do przetwarzania danych osobowych dla pracowników Urzędu oraz innych osób, w szczególności stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej, jeżeli realizowane przez nich zadania wiążą się z przetwarzaniem danych osobowych w Urzędzie.
2. Upoważnienia przygotowywane są przez pracownika wyznaczonego przez Burmistrza.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

1. Kierownik komórki organizacyjnej, pracownik zatrudniony na samodzielnym stanowisku, przewodniczący komisji, występuje do Burmistrza z wnioskiem o wydanie upoważnienia do przetwarzania danych osobowych dla pracowników oraz innych osób mu podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej) w związku z:
   1) podjęciem pracy w Urzędzie,
   2) zmianą zakresu obowiązków,
   3) zmianą stanowiska pracy lub komórki organizacyjnej Urzędu,
   4) organizacją stażu lub praktyki lub wolontariatu,
   5) realizacją umowy cywilnoprawnej,
   6) realizacją zadań wynikających z prac komisji,

   – jeżeli realizowane przez nich zadania wiążą się z przetwarzaniem danych osobowych w Urzędzie.

2. Wzór **wniosku** oraz **upoważnienia** do przetwarzania danych osobowych, znajduje się w niniejszej procedurze.

3. Upoważnienie do przetwarzania danych osobowych może być w każdym czasie odwołane przez Burmistrza na wniosek Sekretarza Gminy, IOD, ASI, przewodniczącego komisji lub kierownika komórki organizacyjnej oraz pracownika zatrudnionego na samodzielnym stanowisku.

4. Pracownik **Referatu OR** prowadzi *„Ewidencję osób upoważnionych w Urzędzie do przetwarzania danych osobowych”*, w której w szczególności odnotowuje się następujące informacje:
   1) imię i nazwisko upoważnionego;
   2) komórka organizacyjna;
   3) status osoby (pracownik, stażysta, praktykant, wolontariusz, umowa cywilnoprawna, członek komisji);
   4) data wydania upoważnienia;
   5) data ustania upoważnienia;
   6) wskazanie procesu przetwarzania danych osobowych, w którym upoważniony będzie uczestniczył (z rejestru czynności przetwarzania danych osobowych).

5. Wzór **ewidencji** znajduje się w niniejszej procedurze.

6. Mogą być prowadzone dodatkowe ewidencje osób upoważnionych do przetwarzania danych w sytuacji, gdy wynika to z zawartej umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych.

„WZÓR" **Burmistrz Miasta i Gminy Ogrodzieniec**

WNIOSEK
o wydanie upoważnienia do przetwarzania danych osobowych

1. Wniosek o wydanie upoważnienia dla:

L.p	Imię i nazwisko	Stanowisko / status (stażysta / praktykant / wolontariusz / realizacja umowy cywilnoprawnej / członek komisji)	Komórka organizacyjna / samodzielne stanowisko /	Uwagi

2. Wnioskuję o wydanie upoważnienia do przetwarzania danych osobowych w związku z: *
   1) aktualizacją posiadanego upoważnienia do przetwarzania danych osobowych;
   2) podjęciem pracy w Urzędzie;
   3) zmianą zakresu obowiązków;
   4) zmianą stanowiska pracy lub komórki organizacyjnej;
   5) zawarciem umowy cywilnoprawnej nr ..... z dnia ..... ;
   6) organizacją stażu / praktyki / wolontariatu;
   7) realizacją zadań wynikających z prac komisji (nazwa) .....

3. Przetwarzanie danych odbywać się będzie w postaci papierowej i elektronicznej. Główne systemy informatyczne w których następuje przetwarzanie danych to:
   1) ..... ;
   2) ..... ;
   3) ..... .

4. Dane osobowe będą przetwarzane w ramach następujących procesów (zgodnie z rejestrem czynności właściwym dla danej komórki organizacyjnej):
   1) ..... ;
   2) ..... ;
   3) ..... .

5. Okres na jaki ma być udzielone upoważnienie: *
   1) na czas trwania stosunku pracy (umowy z kodeksu pracy);
   2) do dnia ..... (w przypadku pozostałych osób, które będą przetwarzały dane osobowe w imieniu administratora).

6. Kategorie danych, które będą przetwarzane: *
   1) zwykłe;
   2) szczególne.

Miejscowość, **dnia** ..... r.

Pieczęć imienna, czytelny podpis osoby wnioskującej

Decyzja Burmistrza (administratora):

.....

Adnotacja ASI, o przydzieleniu identyfikatora w systemie IT

.....

•niewłaściwe usunąć / skreślić

„WZÓR" Ogrodzieniec, dnia ..... r.

.....
Pieczęć

UPOWAŻNIENIE nr .....
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz.UE L 119 z 04.05.2016, str. 1 z późn.zm.)

u p o w a ż n i a m

Panią/Pana .....

zatrudnioną(-nego), odbywającą(-cego) staż, realizującą(-cego) praktykę lub wolontariat na stanowisku ..... w referacie / samodzielne stanowisko .....
w Urzędzie Miasta i Gminy Ogrodzieniec (dalej UMiG) do przetwarzania danych osobowych w celach związanych z realizacją • :

- zadań służbowych powierzonych przez przełożonego lub w opisie stanowiska pracy lub w zakresie obowiązków oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych, lub
- programu stażu, praktyki lub wolontariatu oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych.

Upoważnienie obejmuje przetwarzanie danych osobowych zlokalizowanych w • :

- systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją powierzonych obowiązków pracowniczych,
- funkcjonujących systemach informatycznych, w zakresie niezbędnym do wykonywania obowiązków na ww. stanowisku.

Upoważnienie obejmuje przetwarzanie danych • :

1) zwykłych,
2) szczególnych.

Upoważnienie ważne jest od dnia ..... do dnia jego odwołania lub ustania Pani/Pana stosunku pracy, zakończenia stażu lub praktyki/wolontariatu. Wszelkie upoważnienia wydane poprzednio tracą ważność z dniem wprowadzenia niniejszego upoważnienia.

.....
Podpis Administratora

• Niewłaściwe skreślić

Oświadczenie

1. *Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).*
2. *Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.*
3. *Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabraniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego, Administratorowi lub Inspektorowi Ochrony Danych.*
4. *Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych.*
5. *Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-łem) upoważniona(-ny) oraz haseł i zasad dostępu do tych systemów także po ustaniu umowy wiążącej mnie z UMiG Ogrodzieniec. Z chwilą ustania umowy zobowiązuję się do niezwłocznego zwrócenia UMiG Ogrodzieniec wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.*

6. Przyjmuję do wiadomości, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej.

Data i czytelny podpis Upoważnionego

„WZÓR" Ogrodzieniec, dnia ..... r.

.....
Pieczęć

UPOWAŻNIENIE nr .....
DO PRZETWARZANIA DANYCH OSOBOWYCH
NA PODSTAWIE UMOWY CYWILNOPRAWNEJ

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz.UE L 119 z 04.05.2016, str. 1 z późn.zm.)

u p o w a ż n i a m

Panią/Pana .....

do przetwarzania danych osobowych w celach związanych z realizacją umowy cywilnoprawnej nr ..... zawartej w dniu ..... , dotyczącej ..... oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych.

Upoważnienie obejmuje przetwarzanie danych osobowych zlokalizowanych w * :

- systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją wyżej wskazanej umowy,
- funkcjonujących systemach informatycznych, w zakresie niezbędnym do wykonywania wyżej wskazanej umowy.

Upoważnienie obejmuje przetwarzanie danych * :
1) zwykłych,
2) szczególnych.

Upoważnienie ważne jest od dnia ..... do dnia jego odwołania lub wygaśnięcia umowy. Wszelkie upoważnienia wydane poprzednio tracą ważność z dniem wprowadzenia niniejszego upoważnienia.

.....
Podpis Administratora

* Niewłaściwe skreślić

Oświadczenie

1. Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.
3. Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabraniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego, Administratorowi lub Inspektorowi Ochrony Danych.
4. Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych.
5. Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-łem) upoważniona(-ny) oraz haseł i zasad dostępu do tych systemów także po ustaniu

umowy wiążącej mnie z UMiG Ogrodzieniec. Z chwilą ustania umowy zobowiązuję się do niezwłocznego zwrócenia UMiG Ogrodzieniec wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.

6. Przyjmuję do wiadomości, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej.

.....
Data i czytelny podpis Upoważnionego

„WZÓR" Ogrodzieniec, dnia ..... r.

.....
Pieczęć

UPOWAŻNIENIE nr .....
DO PRZETWARZANIA DANYCH OSOBOWYCH
w związku z udziałem w pracach Komisji

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz.UE L 119 z 04.05.2016, str. 1 z późn.zm.)

u p o w a ż n i a m

Panią/Pana .....

członka **Komisji socjalnej** Urzędu Miasta i Gminy Ogrodzieniec, do przetwarzania danych osobowych, w celach związanych z realizacją działań określonych w Regulaminie ZFŚS UMiG Ogrodzieniec, oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych.

Upoważnienie obejmuje przetwarzanie danych osobowych zlokalizowanych w * :

- systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją wyżej wskazanych działań,
- funkcjonujących systemach informatycznych, w zakresie niezbędnym do wykonywania wyżej wskazanych działań.

Upoważnienie obejmuje przetwarzanie danych * :

1) zwykłych
2) szczególnych

Upoważnienie ważne jest od dnia ..... do dnia jego odwołania lub na czas udziału w pracach Komisji socjalnej UMiG Ogrodzieniec. Wszelkie upoważnienia wydane poprzednio tracą ważność z dniem wprowadzenia niniejszego upoważnienia.

.....
Podpis Administratora

* Niewłaściwe skreślić

Oświadczenie

1. Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.

3. Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabraniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego, Administratorowi lub Inspektorowi Ochrony Danych.

4. Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych.

5. Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-łem) upoważniona(-ny) oraz haseł i zasad dostępu do tych systemów także po ustaniu

mojego udziału w pracach Komisji socjalnej. Z chwilą ustania mojego udziału w pracach Komisji socjalnej zobowiązuję się do niezwłocznego zwrócenia Komisji socjalnej UMiG Ogrodzieniec wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.

6. *Przyjmuję do wiadomości, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej.*

Data i czytelny podpis Upoważnionego

„WZÓR"

EWIDENCJA
osób upoważnionych do przetwarzania danych osobowych
- pracownicy, stażyści, praktykanci, wolontariusze -

L.p	Imię i nazwisko	Stanowisko / nazwa komórki, jednostki organizacyjnej	Data nadania upoważnienia	Data ustania upoważnienia	Sygnatura upoważnienia	Zakres upoważnienia / zakres czynności przetwarzania	UWAGI
1.	2.	3.	4.	5.	6.	7.	8.

„WZÓR"

EWIDENCJA
osób upoważnionych do przetwarzania danych osobowych
- członkowie komisji, umowa cywilnoprawna, inne -

L.p	Imię i nazwisko	Członek komisji / rodzaj usługi / inne	Data nadania upoważnienia	Data ustania upoważnienia	Sygnatura upoważnienia	Zakres upoważnienia / zakres czynności przetwarzania	UWAGI
1.	2.	3.	4.	5.	6.	7.	8.

Procedura postępowania dot. sporządzania rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania danych /art. 30 RODO/

CEL PROCEDURY

Zapewnienie przez administratora, zgodności z RODO (art. 5 ust. 2 RODO), czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach** – w zakresie aktualności i poprawności informacji zawartych w rejestrach cząstkowych w ramach realizowanych procesów przetwarzania danych osobowych w zarządzanej komórce organizacyjnej.

2. **Przewodniczący komisji** (np. socjalnej, innej) – w zakresie aktualności i poprawności informacji zawartych w rejestrach cząstkowych w ramach realizowanych procesów przetwarzania danych osobowych w kierowanej komisji.

3. **Pracownik Referatu OR** (pracownik wyznaczony przez Burmistrza) – w zakresie koordynowania, sporządzenia i prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania danych dla całego Urzędu, we współpracy z IOD.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

1. Rejestr czynności przetwarzania danych i rejestr kategorii czynności przetwarzania danych dla całego Urzędu tworzy się na podstawie **rejestrów cząstkowych** tworzonych przez każdą komórkę organizacyjną Urzędu, pracownika zatrudnionego na samodzielnym stanowisku oraz przewodniczącego komisji.

2. Pierwsze rejestry czynności przetwarzania i rejestry kategorii czynności przetwarzania danych cząstkowe sporządzane zostaną na podstawie przeprowadzonej **inwentaryzacji** czynności przetwarzania danych. Pracownik **Referatu OR** przekaże do komórek organizacyjnych, pracowników zatrudnionych na samodzielnych stanowiskach, przewodniczącego komisji, projekty rejestrów, o których mowa w ust. 1, zgodnie z właściwością celem ponownego uzgodnienia zapisów oraz ewentualnego uaktualnienia.

3. Pracownik **Referatu OR** nie rzadziej niż **raz w roku** będzie występował do komórek organizacyjnych, pracowników zatrudnionych na samodzielnych stanowiskach, przewodniczącego komisji, celem zapewnienia, że nie zmieniły się procesy przetwarzania oraz kategorie przetwarzanych danych w przypadku, gdy Urząd jest podmiotem przetwarzającym (procesorem).

4. Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach, przewodniczący komisji, mają obowiązek **na bieżąco** informować pracownika **Referatu OR** lub IOD o wszelkich zmianach w procesach przetwarzania danych osobowych realizowanych w swoich komórkach, na swoich stanowiskach, w komisji, w szczególności dotyczących:
   1) celów przetwarzania danych;
   2) kategorii osób, których dane są przetwarzane;
   3) zakresu przetwarzania danych;
   4) podmiotów przetwarzających, którym dane są powierzane;
   5) odbiorców danych, którym dane są udostępnione.

5. Wzór **rejestru czynności przetwarzania danych** oraz **rejestru kategorii czynności przetwarzania danych**, znajduje się w niniejszej procedurze.

„WZÓR"

Rejestr czynności przetwarzania danych osobowych
/art.30 ust.1 RODO/

1. **Administrator** (art.30 ust.1 lit. a) – Burmistrz Miasta i Gminy Ogrodzieniec, z siedzibą 42-440 Ogrodzieniec, Pl.Wolności 25, tel. +48 32 67 09 700, e-mail: ogrodzieniec@ogrodzieniec.pl
2. **Inspektor Ochrony Danych** (art.30 ust.1 lit a) – Pan/Pani ..... e-mail: ..... , tel. ..... ,
3. **Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej** (art.30 ust.1 lit. e) – NIE DOTYCZY
4. **Ocena skutków dla ochrony danych /DPIA/** (art.35) - NIE JEST WYMAGANA / Jeżeli tak lokalizacja raportu

L.p	Nazwa procesu – czynności przetwarzania	Informacja o przedstawicielu administratora / o współadministrowaniu w ramach procesu (nazwa i dane kontaktowe)	Cel przetwarzania danych	Kategorie osób, których dane dotyczą / opis kategorii danych osobowych (w tym dane: zwykłe, szczególne)
		Art.30 ust.1 lit. a	Art.30 ust.1 lit. b	Art.30 ust.1 lit. c
5.	6.	7.	8.	9.
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)				
1.				
2.				
3.				
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)				
4.				
5.				
6.				

Kategorie odbiorców danych (art.4 pkt 9)		Planowane terminy usunięcia poszczególnych kategorii danych, w ramach procesu (jeżeli jest to możliwe)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa o których mowa w art.32 ust.1 (jeżeli jest to możliwe)
– inni administratorzy (odbiorcy lub kategorie odbiorców którym dane mogą być przekazywane)	– podmiot przetwarzający (informacja o powierzeniu przetwarzania w ramach procesu, nazwa i dane kontaktowe)		
Art.30 ust.1 lit. d	Art.30 ust.1 lit. d	Art.30 ust.1 lit. f	Art.30 ust.1 lit. g
10.	11.	12.	13.
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)			
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)			

„WZÓR"

Rejestr wszystkich kategorii czynności przetwarzania danych dokonywanych w imieniu administratora

/art.30 ust.2 RODO/

1. **Nazwa i dane kontaktowe przetwarzającego** (art.30 ust.2 lit.a) – Burmistrz Miasta i Gminy Ogrodzieniec, z siedzibą 42-440 Ogrodzieniec, Pl.Wolności 25, tel. +48 32 67 09 700, e-mail: ogrodzieniec@ogrodzieniec.pl
2. **Inspektor Ochrony Danych** (art.30 ust.2 lit.a) – Pan/Pani ..... e-mail: ..... , tel. .....
3. **Przedstawiciel** (jeśli wyznaczono) (art.30 ust.2 lit.a) – .....
4. **Nazwy państw trzecich lub organizacji międzynarodowych**, do których dane są przekazywane (art.30 ust.2 lit.c) – .....
5. **Dokumentacja odpowiednich zabezpieczeń** danych osobowych przekazywanych na podstawie **art. 49 ust. 1** akapit drugi (art.30 ust.2 lit.c) – .....

L.p	ADMINISTRATOR			Kategorie przetwarzań dokonywanych w imieniu każdego z administratorów
	Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy) / Nazwa i dane kontaktowe przedstawiciela administratora (jeżeli wyznaczono)	Inspektor ochrony danych administratora (jeżeli powołano)	
	Art.30 ust.2 lit. a	Art.30 ust.2 lit. a	Art.30 ust.2 lit. a	Art.30 ust.2 lit b
6.	7.	8.	9.	10.
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)				
1.				
2.				
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)				
3.				
4.				

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa o których mowa w art.32 ust.1 (jeżeli jest to możliwe)	Czas trwania przetwarzania / podstawa powierzenia	PODPRZETWARZAJĄCY	
		Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
Art.30 ust.2 lit. d			
11.	12.	13.	14.
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)			
Nazwa komórki organizacyjnej / pracownik na samodzielnym stanowisku / komisja ... (stanowisko przetwarzające)			

Procedura postępowania w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych /art. 28 RODO/

CEL PROCEDURY

Zapewnienie zgodności z RODO (art. 5 ust. 2 RODO), czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach** – w przypadku:
   1) zamiaru powierzenia przetwarzania danych osobowych – za wybór podmiotu przetwarzającego spełniającego wymogi wskazane w art.28 RODO,
   2) zamiaru przyjęcia powierzenia przetwarzania danych osobowych – odpowiada za realizację umowy w zakresie powierzenia przetwarzania danych.

2. **IOD** – odpowiada za czynności monitoringowe oraz kontrolne w zakresie przestrzegania przepisów RODO przez podmiot przetwarzający.

3. **Pracownik Referatu OR** (pracownik wyznaczony przez Burmistrza) – w zakresie prowadzenia rejestru podmiotów którym powierzono przetwarzanie danych osobowych oraz prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania danych dla całego Urzędu, we współpracy z IOD.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

Powierzenie przetwarzania danych przez Urząd

1. Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach obowiązani są informować IOD z tygodniowym wyprzedzeniem o zamiarze powierzenia przetwarzania danych osobowych i przekazać mu niezbędne informacje w tym zakresie, tj. szczegółowy opis na czym ma polegać przetwarzanie danych osobowych przez podmiot przetwarzający w celu uzgodnienia z IOD kryteriów wyboru podmiotu przetwarzającego.

2. Konsultacje z IOD, o których mowa w ust. 1, muszą odbyć się w szczególności przed złożeniem wniosku o wszczęcie postępowania na podstawie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz.U. 2018 r. poz. 1986), a jeżeli nie jest wymagane stosowanie ustawy – przed inną procedurą wyboru kontrahenta.

3. Każda umowa, porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych musi być **zaparafowany** przez IOD oraz wpisana do *„Rejestru podmiotów którym powierzono przetwarzanie danych"* prowadzonym w Urzędzie.

4. Wzór **rejestru**, znajduje się w niniejszej procedurze.

5. Informacje w zakresie umów lub porozumień (data zawarcia, podmiot) w sprawie przetwarzania danych osobowych muszą zostać zawarte w **rejestrze czynności** prowadzonym w Urzędzie.

6. IOD ma prawo do występowania do komórek organizacyjnych, pracowników zatrudnionych na samodzielnych stanowiskach, o przekazanie informacji na temat zawartych umów powierzenia przetwarzania danych.

7. Umowa w zakresie powierzenia przetwarzania danych osobowych powinna w szczególności zawierać:
   1) cel przetwarzania danych;
   2) oświadczenie procesora o zapewnieniu wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie powierzonych danych osobowych spełniało wymogi prawem przewidziane i chroniło prawa osób, których dane dotyczą;
   3) rodzaj i zakres przekazanych danych;
   4) informacje o zasadach dotyczących przeprowadzania kontroli w podmiotach przetwarzających dane osobowe w imieniu Urzędu;
   5) informacje o sposobie upoważniania osób, które w imieniu procesora będą przetwarzały dane osobowe;

6) informacje o sposobach zgłaszania naruszeń z zakresu ochrony danych osobowych;
7) informacje o sposobach postępowania z danymi osobowymi po zakończeniu realizacji umowy.

8. Jeżeli powierzenie przetwarzania danych jest zadaniem drugorzędnym w stosunku do umowy głównej, elementy wskazane w ust. 7 mogą być również ujęte w tej umowie (np. w przypadku umów o realizację szkoleń, ewaluacji itd.). Przepis ust. 3 stosuje się.

9. Ramowy wzór **umowy powierzenia**, znajduje się w niniejszej procedurze.

Urząd jako podmiot przetwarzający (procesor)

1. Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach mają obowiązek informowania IOD o planowanym powierzeniu Urzędowi przetwarzania danych osobowych w drodze umowy lub porozumienia z tygodniowym wyprzedzeniem, aby umożliwić IOD zajęcie stanowiska w przedmiotowej kwestii.

2. Każda umowa lub porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych musi być **zaparafowany** przez IOD.

3. Kategorie czynności, które zostały Urzędowi powierzone do przetwarzania, muszą zostać zawarte w **rejestrze kategorii czynności** prowadzonym w Urzędzie.

„WZÓR"

REJESTR
podmiotów, którym powierzono przetwarzanie danych osobowych

L.p	Nazwa podmiotu przetwarzającego, dane kontaktowe	Data powierzenia, zawarcia umowy powierzenia	Przedmiot i czas trwania przetwarzania (okres powierzenia, umowa główna do której odnosi się umowa powierzenia lub inny instrument prawny)	Charakter i cel przetwarzania	Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą	Informacje dodatkowe np. weryfikacja lub audyt w podmiocie przetwarzającym, podpowierzenie przetwarzania, zgłoszenie naruszenia, itp.
1.	2.	3.	4.	5.	6.	7.

„W Z Ó R"

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia ..... pomiędzy:
(zwana dalej „Umową")

Gminą Ogrodzieniec z siedzibą Pl.Wolności 25, 42-440 Ogrodzieniec,
NIP 574-205-53-06, REGON 151398273
reprezentowaną przez:
Annę Pilarczyk – Burmistrza
zwanym w dalszej części umowy „Administratorem"

oraz

.....
.....
reprezentowanym przez:
.....
zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**

łącznie zwane **„Stronami"**, a odrębnie **„Stroną"**

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (EU) nr 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 (ogólnego rozporządzenia o ochronie danych), zwanego w dalszej części „Rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy następujące rodzaje danych osobowych:
   PRZYKŁAD:
   - ***Dane zwykłe (w tym: imię i nazwisko, adres zamieszkania, PESEL)***
   - ***Szczególne kategorie danych (w tym: informacje o stanie zdrowia)***
2. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:
   <podać kategorię osób, których dane dotyczą np.:
   - ***petenci administratora,***
   - ***mieszkańcy Gminy,***
   - ***pracownicy, praktykanci, stażyści, administratora,***
   - ***wnioskodawcy,***
   - ***podatnicy, dłużnicy,***
   - ***kandydaci do pracy,***
   - ***właściciele nieruchomości, gruntów,***
   - ***producenci rolni,***

- ***najemcy, użytkownicy.***

3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Podstawowej („głównej"), tj.:
   ..... *<nazwa>* z dnia: ..... nr: .....
   w zakresie: .....
4. Przetwarzanie, o którym mowa w ust. 1 dotyczy wykonywania operacji:
   <podać rodzaj 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.***
5. Zakres danych osobowych wymienionych powyżej jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.
5. Podmiot przetwarzający na żądanie Administratora dostarcza Administratorowi wykaz upoważnionych osób oraz informuje Administratora o cofnięciu upoważnień.
   (ten punkt należy pozostawić, jeśli dotyczy)
6. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
8. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w czasie nie przekraczającym *24 h*.
   Powiadomienie o stwierdzeniu naruszenia powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.
10. Podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 Rozporządzenia.
11. Ze względu na obowiązek powierzenia przetwarzania danych przez Administratora podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymagania rozporządzenia i chroniło prawa osób, których dane dotyczą Podmiot Przetwarzający zobowiązany jest do wypełnienia ***„Ankiety bezpieczeństwa danych osobowych"*** *(załącznik do niniejszej umowy).*

§ 4
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy Podstawowej.
3. Zobowiązanie do zachowania poufności trwa przez cały okres obowiązywania Umowy Podstawowej, o której mowa w § 2 punkt 3 powyżej oraz po upływie okresu przedawnienia roszczeń wynikających z Umowy Podstawowej.

§ 5
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy lub Rozporządzenia.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum *7 dniowym* uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż *7 dni.*
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 6
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy Podstawowej po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający może powierzyć dane osobowe objęte niemniejszą umową podmiotom świadczącym usługi w zakresie zarządzania systemami informatycznymi, świadczącymi usługi hostingu dostawcom poczty elektronicznej oraz systemów informatycznych w celu administracji tymi systemami.
3. Podmiot przetwarzający zawarł umowy powierzenia przetwarzania danych osobowych w celu realizacji umowy z:
   a) .....
   b) .....
   (ten punkt należy pozostawić, jeśli dotyczy)
4. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
5. Podwykonawca, o którym mowa w § 6 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
6. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków w zakresie ochrony danych.
7. W przypadku dalszego powierzenia przetwarzania danych osobowych Podmiot Przetwarzający zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi postanowień, zgodnie z którymi, umowy dalszego przetwarzania będą ulegały automatycznemu rozwiązaniu w chwili zakończenia obowiązywania niniejszej Umowy.

§ 7

Oświadczenia Stron

1. Administrator oświadcza, że jest Administratorem danych osobowych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Podmiot Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
3. Przetwarzający na żądanie administratora danych powinien przedstawić dokumentację potwierdzająca przetwarzanie danych osobowych zgodnie z wymogami RODO, mogą to być między innymi: certyfikat potwierdzający wdrożenie normy PN-EN ISO/IEC 27001, raporty z przeprowadzonych przez niezależne podmioty audytów, dokumentacja potwierdzająca przeprowadzenie szkoleń, dokumentacja potwierdzająca wdrożenie zabezpieczeń technicznych i organizacyjnych.

§ 8

Odpowiedzialność Podmiotu przetwarzającego

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

§ 9

Czas obowiązywania umowy

1. Niniejsza umowa zostaje zawarta na czas trwania Umowy Podstawowej, o której mowa w § 2 pkt 3 powyżej.
2. Rozwiązanie umowy, o której mowa w § 2 pkt 3 powyżej skutkować będzie ustaniem niniejszej Umowy.
3. Zamawiający może rozwiązać umowę, o której mowa w § 2 pkt 3 powyżej ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia, gdy Wykonawca narusza zobowiązania wynikające z niniejszej Umowy.

§ 10

Rozwiązanie umowy

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową lub Rozporządzeniem;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 11

Inspektor Ochrony Danych Osobowych

1. Kontakt z Inspektorem Ochrony Danych [IOD] w **Urzędzie Miasta i Gminy Ogrodzieniec**: Pan/Pani ..... , e-mail: ..... , tel. .....
2. Kontakt z Inspektorem Ochrony Danych [IOD] w Podmiocie Przetwarzającym lub pełnomocnikiem Podmiotu Przetwarzającego właściwym z uwagi na przedmiot Umowy: Pan/Pani ..... , e-mail: ..... , tel. .....

§ 12

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Każdorazowo przez pojęcie „dni" rozumie się dni kalendarzowe.
3. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

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

ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Załącznik do umowy powierzenia danych osobowych nr: ..... z dnia: ..... .

Podmiot przetwarzający:	
Imię I Nazwisko osoby wypełniającej	
Stanowisko	
Adres e-mail i nr tel. do kontaktu	

Lp.	Pytanie	Odpowiedź	Uwagi
1	Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe.		
2	Czy Państwa personel został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
3	Czy personel przetwarzający powierzone dane osobowe w pozostałych krajach został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
4	Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych?		
5	Jeśli tak to w jakim kraju?		
6	Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych?		
7	Czy w Państwa organizacji przeprowadzane są okresowe audyty bezpieczeństwa IT?		
8	Czy posiadają Państwo wdrożoną politykę bezpieczeństwa przetwarzania danych osobowych zgodną z zasadami RODO?		
9	Czy prowadzą Państwo rejestr czynności przetwarzania, w tym dla procesora, zgodnie z art. 30 RODO?		
10	Czy jesteście Państwo zobowiązani do wyznaczenia IOD, zgodnie z art. 37 RODO?		
11	Jeśli tak, to czy wyznaczono IOD?		
12	Jeśli nie, to czy wyznaczyli Państwo osobę, która będzie odpowiedzialna za zapewnienie zgodności przetwarzania danych z przepisami i bezpieczeństwa danych?		
13	Czy do przetwarzania danych w Państwa organizacji są dopuszczone wyłącznie osoby posiadające upoważnienia?		
14	Czy osoby te zostały zobowiązane do zachowania poufności danych oraz informacji o stosowanych przez Państwa zabezpieczeniach?		
15	Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych?		

16	Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO?		
17	Czy wdrożyli Państwo instrukcję postępowania w przypadku sytuacji naruszenia ochrony danych osobowych?		
18	Jeśli tak, to czy zgodnie z tą instrukcją zdołają Państwo przekazać administratorowi danych informacje o incydencie w ciągu 24 godzin od stwierdzenia naruszenia?		
19	Czy w celu zaplanowania środków bezpieczeństwa przeprowadzono analizę ryzyka?		
20	Czy wdrożyli Państwo system zarządzania bezpieczeństwem informacji np. ISO 27001?		
21	Czy do przetwarzania danych w Państwa pomieszczeniach, stosuje się fizyczne zabezpieczenia przed dostępem osób nieuprawnionych? Proszę krótko opisać jakie np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny.		
22	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO w Państwa organizacji?		
23	Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów		
24	Czy posiadają Państwo wdrożoną instrukcję zarządzania systemami IT służącymi do przetwarzania danych osobowych lub inne dokumenty wewnętrzne regulujące zasady zarządzania infrastrukturą IT?		
25	Czy Państwa systemy IT zapewniają rozliczalność operacji wykonywanych na danych osobowych, tzn. czy istnieje odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
26	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
27	Czy stosują Państwo pseudonimizację i szyfrowanie danych?		
28	Czy podjęli Państwo środki, aby zapewnić zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania?		
29	Czy w Państwa organizacji są stosowane środki służące ochronie systemów IT przed działaniem tzw. złośliwego oprogramowania?		
30	Jeśli tak, to czy podlegają one cyklicznej aktualizacji?		
31	Czy podjęli Państwo środki, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Np. regularny backup		
32	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
33	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		

Załącznik nr 2 do zarządzenia nr .....
Burmistrza Miasta i Gminy Ogrodzieniec
z dnia ..... 2020 r.

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w

Urzędzie Miasta i Gminy Ogrodzieniec

Rozdział I
Podstawowe pojęcia

1) **Administrator** – Burmistrz Miasta i Gminy Ogrodzieniec (Gmina Ogrodzieniec, Urząd Miasta i Gminy w Ogrodzieńcu – reprezentowane przez Burmistrza), który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych;

2) **Administrator systemu informatycznego** (ASI) – osoba fizyczna lub pracownik Urzędu, który realizuje zadania administratora systemów informatycznych, określone w zarządzeniu Burmistrza, oraz inne zadania i obowiązki, jeżeli nie powodują konfliktu interesów;

3) **baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera (baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe);

4) **hasło** – ciąg znaków literowych, cyfrowych lub innych znaków specjalnych, znany jedynie użytkownikowi;

5) **identyfikator** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie;

6) **Inspektor Ochrony Danych** (IOD) – osoba fizyczna lub pracownik Urzędu, który realizuje zadania określone w art. 39 RODO oraz inne zadania i obowiązki, jeżeli nie powodują konfliktu interesów;

7) **Instrukcja** – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec.

8) **naruszenie ochrony danych osobowych** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

9) **nośnik komputerowy** (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dyski flash, pendrive.

10) **ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

11) **Polityka** – Polityka ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec;

12) **profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

13) **pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

14) **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

15) **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 (ogólne rozporządzenie o ochronie danych) Dz.U. L 119 z 04.05.2016 r. s 1 z późn.zm. (sprostowanie, Dz.U. L 127 z 23.5.2018, s. 2 (2016/679);

16) **system informatyczny** (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

17) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U 2018 poz. 1000 z pożń.zm.);

18) **usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

19) **Urząd** – Urząd Miasta i Gminy Ogrodzieniec;

20) **użytkownik** – pracownik Urzędu Miasta i Gminy Ogrodzieniec, posiadający uprawnienia (upoważnienie) do pracy w systemie informatycznym, zgodnie z zakresem obowiązków służbowych;

21) **zabezpieczenie systemu informatycznego** – wdrożenie stosownych środków organizacyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

22) **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji.

Rozdział II
Postanowienia ogólne

§ 1.

1. Niniejsza Instrukcja stanowi jeden ze **środków organizacyjnych**,[1] mających na celu wykazanie, że Urząd przetwarzając dane w systemach informatycznych, stosuje odpowiednie środki techniczne i organizacyjne, wynikające z przeprowadzonej analizy ryzyka przetwarzania danych dla praw lub wolności osób fizycznych, wypełniając obowiązek wynikający z art.32 RODO tj. **zapewnienia bezpiecznego przetwarzania danych.**

2. Instrukcja określa **zasady** eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

3. Za stosowanie niniejszej Instrukcji odpowiedzialni są **wszyscy użytkownicy**, zapoznani z zasadami ochrony danych i upoważnieni do ich przetwarzania, w systemach informatycznych.

4. ASI prowadzi, **wykaz systemów informatycznych** *(oprogramowania),* w tym programów służących do przetwarzania danych osobowych, dopuszczonych do użytkowania przez Administratora. Wzór wykazu określa ***załącznik nr 1*** do niniejszej Instrukcji.

5. Wymagania, zasady i regulacje dot. ochrony danych, jakie są stosowane przez Administratora określa **Polityka**, która stanowi dokument związany z niniejszą Instrukcją.

Rozdział III
Podstawowe zasady bezpieczeństwa danych

[1] Art.24 ust.1 RODO

§ 2.

1. Przetwarzanie danych w systemie informatycznym, realizujemy wyłącznie poprzez dopuszczone przez Administratora, licencjonowane oprogramowanie.
2. Na bieżąco aktualizujemy systemy operacyjne.
3. Systematycznie aktualizujemy programy antywirusowe, antymalware i antyspyware.
4. Systematycznie skanujemy stacje robocze programami antywirusowymi, antymalware i antyspyware.
5. Pobieramy oprogramowanie wyłącznie ze stron producentów.
6. Nie otwieramy załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
7. Nie zapamiętujemy haseł w aplikacjach webowych.
8. Nie zapisujemy haseł na kartkach.
9. Nie używamy tych samych haseł w różnych systemach informatycznych.
10. Zabezpieczamy serwery plików, czy inne zasoby sieciowe.
11. Zabezpieczamy sieci bezprzewodowe – Access Point.
12. Dostosowujemy złożoność haseł odpowiednio do zagrożeń.
13. Unikamy wchodzenia na nieznane, czy przypadkowe strony internetowe.
14. Nie logujemy się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
15. Wykonujemy regularne kopie zapasowe.
16. Korzystamy ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
17. Szyfrujemy dane przesyłane pocztą elektroniczną.
18. Szyfrujemy dyski twarde w komputerach przenośnych.
19. Przy pracy zdalnej korzystamy z szyfrowanego połączenia VPN.
20. Odchodząc od komputera blokujemy stację komputerową.
21. Nie umieszczamy w komputerze przypadkowo znalezionych nośników USB (może znajdować się na nich złośliwe oprogramowanie).

Rozdział IV
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności

§ 3.

1. Dostęp użytkownika do sprzętu i aplikacji, służących do przetwarzania danych osobowych w systemie informatycznym Administratora, może mieć miejsce wyłącznie po nadaniu indywidualnego **identyfikatora** (login)[2] oraz przydzieleniu w sposób poufny **hasła** (pierwotnego).

2. W uzasadnionych przypadkach, Administrator w uzgodnieniu z ASI może wyrazić użytkownikowi zgodę na udzielenie **dostępu zdalnego** do systemu informatycznego, z komputera osobistego / notebooka. Wzór wniosku o udzielenie dostępu zdalnego określa ***załącznik nr 2*** do niniejszej Instrukcji.

3. Przyznanie, zmiana, odebranie (anulowanie) uprawnień użytkownikowi do przetwarzania danych w systemie informatycznym realizowane jest przez **ASI**, na podstawie pisemnego **wniosku**, a następnie

[2] Zalecane jest aby identyfikator nadawany użytkownikowi, umożliwiał łatwe jego zidentyfikowanie.

upoważnienia [3] nadanego przez Administratora (o których mowa w Polityce), odnotowaniu tego faktu w prowadzonej **bazie użytkowników** systemu informatycznego prowadzonej przez ASI.

4. W przypadku nadania uprawnień, Administrator egzekwuje aby użytkownik:
   a) zapoznał się z zasadami ochrony danych osobowych (udokumentowane szkolenie), w tym z niniejszą Instrukcją oraz Polityką,
   b) złożył **oświadczenie** (o którym mowa w Polityce) i zobowiązał się do przestrzegania zawartych w tych dokumentach zasad, reguł i postanowień.

5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwienie innym osobom pracy na koncie innego użytkownika (zasada ta obowiązuje również administratora systemu).

6. Użytkownikowi uprzywilejowanemu (Administratorowi) nadawane jest indywidualne konto administracyjne – zobowiązany on jest do bieżącej pracy na koncie roboczym, użycie tzw. konta administracyjnego (np."root" lub „admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub istotnych zmian wprowadzanych w administrowanym systemie.

7. Uprawnienia do pracy w systemie informatycznym, mogą być odbierane czasowo, poprzez zablokowanie konta np. w przypadku zawieszenia w pełnieniu obowiązków służbowych.

8. Uprawnienia do przetwarzania danych odbierane są trwale, w przypadku ustania stosunku pracy, łączącego użytkownika z Administratorem.

9. Odebranie uprawnień użytkownikowi polega na skutecznym wyrejestrowaniu go z systemu, przez ASI.

10. Identyfikator (login) i hasło użytkownika po wyrejestrowaniu z systemu informatycznego, nie może być przydzielone innej osobie (powtórnie wykorzystane).

Rozdział V
Polityka haseł, stosowane metody i środki uwierzytelnienia

§ 4.

1. **Ogólne zasady postępowania z hasłami**
   1) Użytkownik systemu, w momencie pierwszego logowania, zobowiązany jest do zmiany przydzielonego hasła (**system wymusza zmianę hasła**).
   2) Użytkownik systemu w trakcie pracy w aplikacji może zmieniać swoje hasło, w razie takiej potrzeby.
   3) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać nazw własnych tj. np.: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów itp.
   4) Użytkownik zobowiązany jest do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich oraz zachowania hasła w poufności, nawet po utracie przez nie ważności.
   5) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie, ujawnianie ich osobom trzecim, w tym innym użytkownikom.
   6) W przypadku „zapomnienia" hasła lub zadziałania mechanizmu blokady dostępu do konta, **po 3 krotnej** próbie nieudanego logowania się, użytkownik zgłasza ASI, potrzebę zmiany (przydzielenia) hasła.[4]
   7) Nowoutworzone hasło przez użytkownika, musi się różnić od **10 haseł** używanych poprzednio (opcja: system odrzuca użyte ostatnio hasło).
   8) W przypadku ujawnienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych, użytkownik obowiązany jest **niezwłocznie powiadomić** Administratora oraz ASI, który dokonuje zablokowania konta użytkownika. [5]

2. **Hasło użytkownika**

---

[3] Obowiązuje zasada minimalizacji uprawnień.

[4] Przydzielenie przez ASI, użytkownikowi hasła (wtórnego) odbywa się również w sposób poufny (ze względów bezpieczeństwa nie powinno ono odbywać się przy użyciu telefonu).

[5] Powyższe podlega udokumentowaniu w rejestrze naruszeń ochrony danych, prowadzonym przez Administratora.

1) Hasło składa się, z zestawu co najmniej **8 znaków** (opcja ocena hasła: **„słabe", „średnie", „mocne"**).
2) Hasło nie może być identyczne z identyfikatorem użytkownika.
3) Hasło składa się z dużych i małych liter oraz z cyfr i znaków specjalnych.
4) Zmiana hasła winna odbywać się nie rzadziej niż co **30 dni** (opcja **„zmień hasło"** w ustawieniach).
5) Administrator lub ASI może w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

3. **Hasła administratora**
   1) Hasło administratora składa się co najmniej z **12 znaków.**
   2) Hasło składa się z dużych i małych liter oraz z cyfr i znaków specjalnych.
   3) Zmiana hasła winna odbywać się nie rzadziej niż co **60 dni.**
   4) Aktualne hasła dostępu do wszystkich systemów informatycznych (w tym **hasła „root"** lub **„admin"**), **ASI** wraz z **metryką hasła** przekazuje, za potwierdzeniem odbioru, Administratorowi lub upoważnionej przez niego osobie, która przechowuje je w tzw. „bezpiecznej kopercie", w sejfie lub metalowej szafie zamykanej na klucz, w pomieszczeniu objętym systemem kontroli dostępu. Wzór metryki hasła przedstawia ***załącznik nr 3*** do niniejszej Instrukcji.
   5) W przypadku utraty uprawnień przez osobę administrującą systemem (ASI), Administrator niezwłocznie zleca upoważnionej osobie, zmianę hasła, do którego miał dostęp ASI.
   6) W przypadkach awaryjnych (np. dłuższa nieobecność ASI), hasło może być przekazane (udostępnione) decyzją Administratora osobie przez niego upoważnionej.
   7) Po ustaniu sytuacji awaryjnej, ASI jest zobowiązany do zmiany hasła i odnotowaniu tego faktu w metryce hasła.

4. **Uwierzytelnianie**
   W uzasadnionych przypadkach (obowiązek prawny lub wynikający z zawartej umowy przez Administratora), użytkownik stosuje system uwierzytelniania, dla aplikacji i systemów (np. karta procesorowa, terminal i kod PIN).

Rozdział VI
Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

§ 5.

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
   1) zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie, **identyfikatora** (login) i **hasła** w sposób uniemożliwiający ich ujawnienie osobom postronnym;
   2) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
   3) powiadomienia Administratora oraz ASI, w razie stwierdzenia fizycznej ingerencji w systemie (np. próba logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje) lub innych podejrzeń dot. naruszenia bezpieczeństwa systemu.

2. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest niezwłocznie powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.

3. Użytkownik jest zobowiązany do zabezpieczenia danych wyświetlanych przez system na monitorze komputera, przed osobami nie mającymi uprawnień (np. pracownicy, współpracownicy, osoby postronne), wglądu do danych wyświetlanych przez system na monitorze komputera (np. poprzez odpowiednie ustawienie monitora, zastosowanie nakładki na monitor itp.) – obowiązuje tzw. ***„Polityka czystego pulpitu".***

4. Przerywając przetwarzanie danych w ciągu godzin pracy, użytkownik powinien:
   1) skorzystać z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie **wygaszacza ekranu** odblokowywanego hasłem (w przypadku braku stosowania opcji automatycznego włączania się wygaszacza po określonym czasie /np. 3-5 minut/ bezczynności użytkownika, odblokowywanego hasłem),
   2) lub zakończyć pracę w systemie informatycznym, wylogowując się skutecznie z systemu. Obowiązuje tzw. ***„Polityka czystego ekranu".***

5. Po zakończeniu pracy w systemie informatycznym w danym dniu, użytkownik zobowiązany jest do:
   1) skutecznego wylogowania się z systemu informatycznego – pamiętając, by do wylogowania się używać linku **"Wyloguj"** (nie używać w tym celu przycisku X /„Zamknij"/, wbudowanego w okno przeglądarki);
   2) wyłączenia i zabezpieczenia sprzętu komputerowego;
   3) zabezpieczenia stanowiska pracy, w szczególności wszelkiej **dokumentacji** oraz **elektronicznych nośników informacji** (w tym komputer przenośny) na których utrwalone są dane, poprzez ich umieszczenie w meblu biurowym lub metalowej szafie zamykanych na klucz – tzw. ***„Polityka czystego biurka"***;
   4) opuszczenia i zamknięcia (zabezpieczenia zgodnie z obowiązującą wewnętrzną procedurą – system kontroli dostępu) pomieszczenia.

6. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane, przechowywany jest w obszarze przetwarzania danych osobowych (w pomieszczeniach) zabezpieczonym przed dostępem osób nieuprawnionych (stosowane zabezpieczenia fizyczne).

7. Przebywanie osób nieuprawnionych w obszarze (np. korzystanie z pomieszczeń biurowych oraz ich wyposażenia w celach niezwiązanych z przetwarzaniem danych), w którym przetwarzane są dane osobowe jest dopuszczalne tylko za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych.

8. Osoba użytkująca komputer przenośny, zawierający dane, jest zobowiązana do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe oraz stosowania **środków ochrony kryptograficznej** wobec przetwarzanych danych osobowych.

Rozdział VII
Procedura tworzenia kopii zapasowych, sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane

§ 6.

1. Za tworzenie i przechowywanie kopii zapasowych oraz niezwłoczne usuwanie po ustaniu ich użyteczności, odpowiedzialny jest **ASI.**

2. Zasady tworzenia **kopii zapasowych** systemów przetwarzających dane osobowe oraz **okres przechowywania** poszczególnych nośników z kopiami zapasowymi (w zależności od celu przetwarzania danych osobowych zapisanych na kopiach zapasowych), określa prowadzona przez ASI tabela, której wzór stanowi ***załącznik nr 4*** do niniejszej Instrukcji.

3. Tworzone kopie bezpieczeństwa są **opisywane** datą jej sporządzenia (oznaczane), w sposób pozwalający na określenie ich zawartości.

4. Wykonane kopie zapasowe winny gwarantować Administratorowi, odtworzenie danych, w przypadku ich utraty lub uszkodzenia.

5. ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana **nie rzadziej niż raz na pół roku.**

6. ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego w Urzędzie. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

7. **Nośniki informacji** (elektroniczne, wydruki papierowe), zawierające dane są przechowywane w meblu biurowym lub metalowej szafie zamykanych na klucz (w pomieszczeniach objętych systemem kontroli dostępu), w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

8. **Zabronione jest** wynoszenie poza obszar siedziby Administratora nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi, bez zgody Administratora.

9. Administrator w uzgodnieniu z ASI, w uzasadnionych przypadkach stosuje procedurę **autoryzacji** przenośnych nośników zawierających dane osobowe, użytkowanych przez pracowników Urzędu. Wzór wniosku o autoryzację przenośnego nośnika danych określa ***załącznik nr 5*** do niniejszej Instrukcji.

Rozdział VIII
Procedura czyszczenia danych oraz niszczenia (utylizacji) elektronicznych nośników informacji, oraz wydruków zawierających dane

§ 7.

1. Użytkownicy są zobowiązani do bieżącego, niezwłocznego i **trwałego usuwania / kasowania danych** z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).

2. Przyjmuje się trzy poziomy utylizacji danych:
   1) zniszczenie wskazanych danych na nośniku, wykluczających ich odtworzenie (bez naruszenia pozostałej zawartości nośnika);
   2) całkowite zniszczenie całej zawartości nośnika, bez możliwości odtworzenia danych (po przeprowadzeniu procedury nośnik jest w pełni sprawny i nadaje się do dalszego użytkowania);
   3) fizyczne zniszczenie nośnika (po takiej operacji nośnik nie nadaje się do dalszego użytkowania).

3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, przeznaczone do:
   1) **likwidacji** – pozbawia się wcześniej zapisu tych danych, w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający odczytanie,
   2) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** (np. sprzedaż, darowizna) – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

4. Nośniki danych, w tym zawierające kopie zapasowe (bezpieczeństwa), które stały się niepotrzebne, **pozbawia się zapisu danych** w sposób uniemożliwiający ich odtworzenie (odzyskanie) np. wymazanie danych poprzez wielokrotne nadpisanie (co najmniej trzykrotnie), zastosowanie specjalistycznego oprogramowania, czy też poddanie dysku silnemu impulsowi elektromagnetycznemu.

5. **Niszczenie** (utylizacja) wszelkich użytkowanych przez Administratora, elektronicznych nośników danych, w tym dysków (zawierających kopie zapasowe), które uległy uszkodzeniu lub stały się nieprzydatne do dalszej pracy, odbywa się komisyjnie – protokolarnie (w składzie komisji powinien być ASI lub upoważniona przez niego osoba), w sposób uniemożliwiający ich odzyskanie np. poprzez fizyczne zniszczenie (zmiażdżenie, pocięcie, nawiercenie, młotkowanie).

6. Przeznaczone do zniszczenia, nośniki informacji zawierające dane osobowe, w postaci wydruków papierowych, są niszczone przez użytkowników na bieżąco, w sposób uniemożliwiający ich odczytanie (odzyskanie), przy użyciu odpowiednich **niszczarek paskowych** – w przypadku gdzie jest to wymagane przepisami prawa w niszczarce o podwyższonym standardzie bezpieczeństwa (**klasa DIN**).

7. Administrator w uzgodnieniu z ASI, może dokonać zniszczenia nośników informacji (elektronicznych, papierowych), za pośrednictwem **specjalistycznej firmy** (posiadającej certyfikat ISO 27001) świadczącej usługi w zakresie niszczenia nośników danych, potwierdzonym otrzymaniem np. protokołu / certyfikatu zniszczenia, nagrania procesu transportu i utylizacji, karty przekazania odpadu.

Rozdział IX
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

§ 8.

1. Urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych, zasilane energią elektryczną, są zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej.

2. Za wdrożenie i korzystanie z oprogramowania antywirusowego oraz oprogramowania firewall odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.

3. System informatyczny, przed działaniem wirusów komputerowych, jest chroniony (zabezpiecza), oprogramowaniem antywirusowym, aktualizowanym na bieżąco, który jest stosowany u Administratora.

4. W systemie informatycznym stosowane jest oprogramowanie firewall, zapewniające kontrolę przepływu informacji oraz działań inicjowanych z zewnątrz i od wewnątrz systemu.

5. Użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI.

6. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik jest zobowiązany niezwłocznie powiadomić Administratora oraz ASI.

7. Próba naruszenia, czy też fakt naruszenia bezpieczeństwa systemu informatycznego, winny zostać udokumentowane w rejestrze incydentów (rejestr naruszeń ochrony danych).

8. **Wykaz zabezpieczeń** (aktualizowany na bieżąco), stosowanych przez Administratora, prowadzi ASI.

Rozdział X
Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 9.

1. **Przeglądy i konserwacja urządzeń:**
   1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego są wykonywane w terminach określonych przez producenta sprzętu,
   2) nieprawidłowości ujawnione w trakcie tych działań są niezwłocznie usuwane, a ich przyczyny analizowane.
2. **Przegląd programów i narzędzi programowych:**
   1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów,
   2) zapisy logów systemowych opisujących pracę systemu, logowania i wylogowania użytkowników nadzoruje ASI i przegląda je każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy – **pozbawia się wcześniej zapisu tych danych** w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI lub osoby przez niego upoważnionej.

4. Wszelkie prace konserwacyjne i naprawcze sprzętu z danymi osobowymi na nośniku oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, odbywają się na zasadach określonych szczegółowo w zawartej **umowie** z Administratorem, która powinna gwarantować bezpieczną naprawę, przestrzeganie przepisów dot. ochrony danych osobowych, czy też zawierać kary umowne za niewywiązywanie się z realizacji umowy (należy na to zwracać uwagę dokonując zakupu).

5. **Rekomendowane jest:**
   1) przekazywanie do naprawy sprzętu z nośnikami informacji, z danymi **zaszyfrowanymi** na dysku / karcie pamięci (bez podawania hasła),
   2) korzystanie z serwisu / producenta, który zobowiązuje się do usunięcia usterki w miejscu instalacji (u klienta) produktu objętego gwarancją (tzw. **„gwarancja on-site"**).

6. Czynności konserwacyjne i naprawcze, wykonywane doraźnie przez osoby nie posiadające upoważnienia do przetwarzania danych (np. specjalistów z firm zewnętrznych), są wykonywane pod nadzorem ASI lub osoby przez niego upoważnionej.

7. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:
   1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany **protokołem**,
   2) przekazanie sprzętu potwierdzane jest **protokołem**, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

8. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia **protokołu serwisowego**, zawierającego, co najmniej poniższe informacje:
   1) imienne wskazanie osoby przeprowadzającej prace serwisowe oraz dane teleadresowe podmiotu, którego osoba ta jest pracownikiem,
   2) imienne wskazanie osoby nadzorującej przebieg prac serwisowych (dot. sytuacji, gdy prace realizowane są w siedzibie Urzędu),
   3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dot. sprzętu),
   4) zakres prac serwisowych i ich wynik oraz zalecenia,
   5) czas (data, godziny od do) i miejsce przeprowadzania prac serwisowych.

9. **Protokoły** (egzemplarz lub kopia), o których mowa w punkcie 7 i 8, przechowywane są przez ASI.

Rozdział XI
Postanowienia Końcowe

§ 10.

1. Wszyscy pracownicy Urzędu są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych na swoim stanowisku pracy.

2. Wszystkie osoby upoważnione do przetwarzania danych, zobowiązane są do stosowania zasad zawartych w niniejszej Instrukcji.

3. Nieprzestrzeganie przepisów o ochronie danych osobowych grozi odpowiedzialnością pracowniczą, karną i cywilną, wynikającą z powszechnie obowiązujących przepisów prawa.

4. W sprawach nieuregulowanych w niniejszej Instrukcji, mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz.1781 tekst jednolity) i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO /Dz.Urz. UE L 119, s.1 z późn.zm./

5. Niniejsza Instrukcja jest dokumentem o charakterze wewnętrznym i nie może być udostępniana osobom trzecim oraz innym podmiotom, w żadnej formie, bez zgody Administratora.

6. Żadna część niniejszej Instrukcji nie może być zmieniana ani kopiowana bez wiedzy i zgody Administratora.

Załącznik nr 1 do Instrukcji

W Y K A Z
systemów informatycznych (oprogramowania)

L.p	Nazwa oprogramowania / systemu	Producent	Wersja	Nr i typ licencji / termin ważności	Użytkownicy	Podpis Administratora Systemu Informatycznego (ASI)
1.	2.	3.	4.	5.	6.	7.

Załącznik nr 2 do Instrukcji

.....
(miejscowość i data)

.....
(imię i nazwisko)

Burmistrz Miasta i Gminy Ogrodzieniec
w / miejscu

.....
(stanowisko / jednostka.org.)

WNIOSEK O UDZIELENIE DOSTĘPU ZDALNEGO

Uprzejmie proszę o zezwolenie na korzystanie z dostępu zdalnego do systemu informatycznego (nazwa) ..... Urzędu Miasta i Gminy Ogrodzieniec (dalej: Administrator), z komputera osobistego / notebooka.

Uzasadnienie:

.....
.....

Na okres od: ..... r. **do** ..... r.

Oświadczam, że:

1. Zestaw komputerowy wykorzystywany do nawiązywania połączenia zdalnego jest należycie chroniony i zabezpieczony przed dostępem osób niepowołanych, między innymi poprzez jego szyfrowanie, wykorzystywanie bezpiecznego połączenia VPN, stosowanie haseł dostępu.
2. Nie będę na tym zestawie użytkował/a oprogramowania nielegalnego, oraz oprogramowania którego licencja nie zezwala na użytkowanie komercyjne.
3. Nie będę na tym zestawie przechowywała(-ał) danych uzyskanych z zasobów informatycznych Administratora.
4. Będę stosowała(-ał) się do:
   - *Polityki ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec,*
   - *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec,*
   - *wewnętrznych aktów dot. zasad korzystania z oprogramowania i sprzętu komputerowego,*

   przyjętych i wdrożonych do stosowania przez Administratora.
5. Zapoznałam(-łem) się z przepisami obowiązującej ustawy krajowej o ochronie danych osobowych i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO /Dz.Urz. UE L 119, s.1 z późn.zm./ i biorę pełną odpowiedzialność za udostępnienie oraz utratę danych osobowych oraz szkody wynikłe z nieautoryzowanego dostępu do sieci Administratora, wynikające z nienależytego zabezpieczenia wykorzystywanego przeze mnie połączenia zdalnego oraz zestawu komputerowego.

Równocześnie przyjmuję do wiadomości, że w przypadku włączenia się do sieci informatycznej Administratora, moja aktywność w niej może być monitorowana i **wyrażam na to zgodę.**

.....
(podpis wnioskodawcy)

Decyzja Administratora:

Wyrażam zgodę / nie wyrażam zgody *

.....
(imienna pieczęć, data i podpis Administratora)

.....
(podpis Administratora Systemu Informatycznego)

Załącznik nr 3 do Instrukcji

Metryka hasła Administratora

L.p	Nazwa systemu / urządzenia	Treść hasła	Data wprowadzenia hasła do systemu	Data i powód awaryjnego udostępnienia hasła	Data zmiany hasła	Podpis Administratora Systemu Informatycznego (ASI)
1.	2.	3.	4.	5.	6.	7.

Załącznik nr 4 do Instrukcji

KOPIE ZAPASOWE
systemów informatycznych / zasobów danych

L.p	System Informatyczny / Zasób danych	Typ nośnika, na jaki wykonywana jest kopia	Lokalizacja składowania kopii	Użyte narzędzie lub oprogramowanie	Metoda sporządzania	Częstotliwość wykonywania kopii	Okres przechowywania
1.	2.	3.	4.	5.	6.	7.	8.

Załącznik nr 5 do Instrukcji

.....
(miejscowość i data)

.....
(imię i nazwisko)

Burmistrz Miasta i Gminy Ogrodzieniec
w / miejscu

.....
(stanowisko / jednostka.org.)

WNIOSEK O AUTORYZACJĘ PRZENOŚNEGO NOŚNIKA DANYCH

Uprzejmie proszę o zezwolenie na korzystanie w systemach informatycznych (nazwa) .....
..... Urzędu Miasta i Gminy Ogrodzieniec (dalej: Administrator), z przenośnego nośnika danych.

Uzasadnienie:
.....
.....

Numer seryjny przenośnika: .....

Producent: ..... **Pojemność:** .....

Zobowiązuję się:

1. Zabezpieczyć autoryzowany nośnik danych przed dostępem osób nieupoważnionych, w sposób zapewniający poufność i integralność tych danych.
2. Wykorzystywać autoryzowany nośnik danych jedynie do celów służbowych i zgodnie z podanym uzasadnieniem.
3. Niezwłocznie zgłosić Administratorowi oraz Administratorowi Systemu Informatycznego /ASI/, uszkodzenie lub utratę wykorzystywanego nośnika danych, z podaniem jakie dane były zapisane na nośniku w chwili jego utraty bądź uszkodzenia, oraz opisaniem okoliczności tego zdarzenia.
4. Dostarczyć nośnik danych do ASI przed przekazaniem nośnika innej osobie, bądź zaprzestania wykorzystywania go do celów służbowych, w celu bezpiecznego usunięcia danych, w sposób uniemożliwiający ich odzyskanie.
5. Przechowywać na nośniku dane, wyłącznie w stanie zaszyfrowanym.

Oświadczam, że:

1) Będę stosowała (-ał) się do:
   - *Polityki ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec,*
   - *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec,*
   - *wewnętrznych aktów dot. zasad korzystania z oprogramowania i sprzętu komputerowego,*

   przyjętych i wdrożonych do stosowania przez Administratora.
2) Zapoznałam(-łem) się z przepisami obowiązującej ustawy krajowej o ochronie danych osobowych i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO /Dz.Urz. UE L 119, s.1/ i biorę pełną odpowiedzialność za udostępnienie oraz utratę danych osobowych oraz szkody wynikłe z dostępu do nośnika danych przez osobę nieuprawnioną, wynikające z nienależytego zabezpieczenia wykorzystywanego przeze mnie przenośnego nośnika danych.

.....
(podpis wnioskodawcy)

Decyzja Administratora:

Wyrażam zgodę / nie wyrażam zgody *

.....
(podpis Administratora Systemu

.....
Informatycznego)
(imienna pieczęć, data i podpis Administratora)

Załącznik nr 1 do zarządzenia nr ..... / 2020
Burmistrza Miasta i Gminy Ogrodzieniec
z dnia ..... 2020 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urzędu Miasta i Gminy Ogrodzieniec

Rozdział I
Podstawowe pojęcia

1) **Administrator** – Burmistrz Miasta i Gminy Ogrodzieniec (Gmina Ogrodzieniec, Urząd Miasta i Gminy Ogrodzieniec – reprezentowane przez Burmistrza), który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych;

2) **Administrator systemu informatycznego (ASI)** – osoba fizyczna lub pracownik Urzędu, który realizuje zadania administratora systemów informatycznych, określone w zarządzeniu Burmistrza, oraz inne zadania i obowiązki, jeżeli nie powodują konfliktu interesów;

3) **bezpieczeństwo informacji** – zapewnienie poufności, integralności oraz dostępności informacji;

4) **Burmistrz** – Burmistrz Miasta i Gminy Ogrodzieniec;

5) **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, 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) **dostępność** – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna;

7) **Inspektor Ochrony Danych (IOD)** – osoba fizyczna lub pracownik Urzędu, który realizuje zadania określone w art. 39 RODO oraz inne zadania i obowiązki, jeżeli nie powodują konfliktu interesów;

8) **Instrukcja** – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ogrodzieniec;

9) **integralność** – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób;

10) **naruszenie ochrony danych osobowych** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

11) **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którym ujawnia się dane osobowe, niezależnie od tego, czy są stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców (przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania);

12) **ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

13) **organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych (PUODO);

14) **organizacja międzynarodowa** – organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

15) **państwo trzecie** – państwo niebędące członkiem Unii Europejskiej oraz nienależące do Europejskiego Obszaru Gospodarczego;

16) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którzy przetwarzają dane osobowe w imieniu administratora;

17) **Polityka** – Polityka ochrony danych osobowych Urzędu Miasta i Gminy Ogrodzieniec;
18) **poufność** – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych;

19) **profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

20) **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

21) **pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

22) **Referat OR** – Referat organizacyjny w Urzędzie Miasta i Gminy Ogrodzieniec;

23) **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 (ogólne rozporządzenie o ochronie danych) Dz.U. L 119 z 04.05.2016 r. s 1 z późn.zm. (sprostowanie, Dz.U. L 127 z 23.5.2018, s. 2 (2016/679);

24) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;

25) **Urząd** – Urząd Miasta i Gminy Ogrodzieniec;

26) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U 2018 poz. 1000 z pożń.zm.);

27) **zgoda** – 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.

Rozdział II
Postanowienia ogólne

§ 1.

1. Polityka ma zastosowanie do przetwarzania danych osobowych w Urzędzie, w szczególności w związku z realizacją:
   1) zadań wynikających z przepisów prawa krajowego oraz Unii Europejskiej i określonych szczegółowo w Regulaminie organizacyjnym Urzędu;
   2) obowiązków pracodawcy w rozumieniu Kodeksu pracy;
   3) umów o organizację staży, praktyk, wolontariatu;
   4) innych zadań niezbędnych do zapewnienia funkcjonowania Urzędu.

2. W Urzędzie dane osobowe przetwarzane są co do zasady na podstawie następujących przesłanek:
   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 (**art.6 ust.1 lit. b RODO**);
   2) przetwarzanie jest niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze (**art.6 ust.1 lit. c RODO**);

3) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (**art.6 ust.1 lit. e RODO**).

3. Dane osobowe mogą być przetwarzane w Urzędzie w postaci papierowej oraz przy użyciu systemów informatycznych, które zostały wskazane w Instrukcji, stanowiącej ***załącznik nr 2*** do zarządzenia.

Rozdział III
Podstawowe zasady bezpieczeństwa informacji

§ 2.

1. **Zasada zamkniętego pomieszczenia** – ostatnia osoba wychodząca z pomieszczenia na zakończenie dnia pracy jest zobowiązana zamknąć drzwi – klucz/karta dostępu. Niedopuszczalne jest pozostawianie kluczy w drzwiach na zewnątrz, otwartych pomieszczeń w godzinach pracy, gdy nikogo upoważnionego nie ma w środku. Zasada nie dotyczy pomieszczeń ogólnie dostępnych.

2. **Zasada nadzorowanych dokumentów** – po godzinach pracy w zamkniętych na klucz szafach, szafkach lub szufladach powinny być przechowywane wszystkie dokumenty.

3. **Zasada czystego biurka** – należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych, płyt CD, DVD lub innych elektronicznych nośników danych.

4. **Zasada czystej tablicy** – w pomieszczeniach przeznaczonych do przyjmowania petentów (gości) po zakończonym spotkaniu pozostawiana jest czysta tablica (flipchart, itp.)

5. **Zasada czystego ekranu** – każdy komputer musi mieć ustawiony wygaszasz ekranu wyłączany po podaniu hasła. Wygaszasz powinien włączać się automatycznie po określonym czasie bezczynności użytkownika. Użytkownicy powinni przed pozostawieniem włączonego komputera bez opieki zablokować komputer lub w przypadku dłuższej nieobecności wylogować się z systemu. Po zakończonym dniu komputer powinien zostać wyłączony i zabezpieczony (komputer przenośny) w zamykanym na klucz meblu biurowym.

6. **Zasada czystego pulpitu** – na pulpicie komputera mogą znajdować się jedynie standardowe ikony Windows, pakietu Office oraz skróty do folderów i aplikacji służbowych pod warunkiem, że w nazwie nie zawierają informacji o projektach lub klientach Administratora.

7. **Zasada czystych drukarek** – dokumenty zawierające informacje o charakterze poufnym, wrażliwym (plany, umowy, dane osobowe czy finansowe itp.) powinny być zabierane z urządzeń służących do wydruku natychmiast po ich wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za dane urządzenie (informatyk) lub zgłosić incydent Administratorowi.

8. **Zasada czystego kosza** – dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający ich odczytanie (np. w niszczarce) lub umieszczane w specjalnie przeznaczonych do tego pojemnikach itp.

i) **Zasada poufności** – należy unikać prowadzenia rozmów o sprawach służbowych z osobami, które nie muszą o nich wiedzieć oraz udzielania informacji o charakterze poufnym, wrażliwym przez telefon.

9. **Zasada bezpieczeństwa danych** – niedozwolone jest kopiowanie służbowych danych, w tym na prywatne elektroniczne nośniki danych, oraz wynoszenie służbowego sprzętu poza siedzibę, bez gody Administratora.

10. **Zasada bezpieczeństwa danych dostępowych** – niedozwolone jest udostępnianie danych dostępowych (login/hasło) do systemów wewnętrznych Administratora. Każdy zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych jemu kontach.

Rozdział IV
Ogólne zasady przetwarzania danych osobowych

§ 3.

1. Przetwarzanie danych osobowych w Urzędzie oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, innych niż zautomatyzowanych, tj.:
   1) zbieranie;
   2) utrwalanie;
   3) organizowanie;
   4) porządkowanie;
   5) przechowywanie;
   6) adaptowanie lub modyfikowanie;
   7) pobieranie;
   8) przeglądanie;
   9) wykorzystywanie;
   10) ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie;
   11) dopasowywanie lub łączenie;
   12) ograniczanie;
   13) usuwanie lub niszczenie.

2. Zbieranie danych osobowych należy rozumieć jako pozyskiwanie danych osobowych.

3. Za utrwalanie należy przyjąć wszelkie formy i postaci zarejestrowania (zapisania) informacji na materialnym nośniku – informacja utrwalona, co do zasady, nadawać się powinna do dalszego przetwarzania zgodnie z celem, w jakim ją zebrano.

4. Organizowanie danych to operacje nieodnoszące się do zmiany treści lub postaci przechowania samych danych, a polegające na nadaniu określonej struktury zbiorowi czy zestawowi, w jakim dane są przetwarzane, lub zmianie jego dotychczasowej struktury.

5. Porządkowanie to operacja, która ma poprawić funkcjonalność użytkowania danych, w szczególności poprzez
   wprowadzenie jakichkolwiek lub lepszych niż dotychczasowe kryteriów wyszukiwania dostępu do określonych kategorii informacji.

6. Operacja przechowania jest związana z uprzednim utrwaleniem danych osobowych na nośniku materialnym z możliwością ich odtworzenia w późniejszym czasie.

7. Adaptowanie lub modyfikowanie danych osobowych polega na uzyskaniu nowej wiedzy na temat osoby, której dane są przetwarzane. Adaptowanie danych osobowych jest zmianą wynikającą ze skorzystania przez osobę, której dane są przetwarzane, z przysługujących jej praw, w szczególności: ograniczenia przetwarzania, usunięcia części danych. Modyfikacja danych związana jest z ingerencją osoby, której dane dotyczą, tj. sprostowania danych.

8. Pobieranie danych osobowych jest operacją związaną z wykonywaniem kopii danych osobowych lub ich części pozyskanych za pośrednictwem sieci telekomunikacyjnej lub innego kanału przesyłu informacji.

9. Przeglądanie danych należy rozumieć jako wyszukiwanie danych poprzez wpisywanie odpowiednich haseł, które dzięki zastosowanemu mechanizmowi indeksującemu pozwalają na zapoznanie się z konkretnymi danymi.

10. Wykorzystywanie danych jest celowym działaniem zmierzającym do konkretnego celu.

11. Ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie należy rozumieć jako operacje, które prowadzą do zapoznania się z danymi przez podmioty zewnętrzne za zgodą administratora.

12. Dopasowywanie lub łączenie danych osobowych polega na aktywnym działaniu podjętym przez administratora w celu weryfikacji poprawności danych, uzyskanie dodatkowych informacji wynikających ze skali przetwarzania, czy usprawnienie procesów przetwarzania.

13. Ograniczenie oznacza każdą formę zawężenia możliwości przetwarzania. Dotyczy to zarówno zakresu przetwarzanych informacji, jak i celów dla jakich są one wykorzystywane.

14. Usuwanie lub niszczenie polega na trwałym kasowaniu danych.

§ 4.

1. Administrator przetwarza dane osobowe zgodnie z następującymi zasadami:
   1) legalności;
   2) rzetelności;
   3) przejrzystości;
   4) ograniczenia celu;
   5) minimalizacji danych;
   6) prawidłowości danych;
   7) ograniczenia przechowywania;
   8) integralności i poufności;
   9) ochrony danych osobowych w fazie projektowania;
   10) domyślnej ochrony danych osobowych.

2. Zasada legalności oznacza przetwarzanie danych zgodnie z prawem. Realizując tę zasadę, dane osobowe przetwarzane są na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych, określonych w **art. 6 i 9 RODO.**

3. Zasada rzetelności wymaga, by dane były przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane dotyczą.

4. Zasada przejrzystości wymaga by osoba, której dane dotyczą została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania, tj. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

5. Zasada ograniczenia celu polega na przetwarzaniu danych osobowych jedynie w celu zgodnym z odpowiednią przesłanką dopuszczalności przetwarzania danych osobowych.

6. Zasada minimalizacji danych oznacza, że administrator przetwarza tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

7. Zasada prawidłowości danych oznacza, że administrator przetwarza dane osobowe prawidłowe i uaktualnia je w razie potrzeby.

8. Zasada ograniczenia przechowywania oznacza, że administrator przechowuje dane osobowe w dokumentacji tworzącej akta spraw przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt, uzgodnionego w trybie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2018 r. poz. 217, z pożn. zm.), z właściwym archiwum państwowym.

9. Zasada integralności i poufności jest realizowana przez dopuszczenie do przetwarzania danych osobowych jedynie osób upoważnionych oraz zastosowanie takich środków technicznych i organizacyjnych, by dane nie były zmieniane przez osoby nieupoważnione lub by dane nie były udostępniane osobom nieupoważnionym.

10. Zasada ochrony danych osobowych w fazie projektowania oznacza, że ochrona prywatności jest realizowana na etapie projektowanych działań skutkujących przetwarzaniem danych osobowych.

11. Zasada domyślnej ochrony danych osobowych oznacza, że domyślne ustawienia przetwarzania danych osobowych umożliwią przetwarzanie jedynie danych niezbędnych do osiągnięcia każdego konkretnego celu przetwarzania. Jednocześnie ustawienia systemów przetwarzania danych nie powinny umożliwiać udostępnienia danych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której dane dotyczą.

ROZDZIAŁ V
Wydawanie upoważnień do przetwarzania danych osobowych

§ 5.

1. W Urzędzie przetwarzanie danych osobowych odbywa się na podstawie **upoważnień** (art.29 RODO).

2. Upoważnienie wydawane jest osobie, która:
   1) w ramach obowiązków służbowych przetwarza dane osobowe;
   2) złożyła oświadczenie o zachowaniu poufności;
   3) została przeszkolona w zakresie ochrony danych osobowych przez IOD;
   4) złożyła oświadczenie o zapoznaniu się z treścią Polityki oraz Instrukcji, wzór **oświadczenia** określa ***załącznik nr 3*** do zarządzenia.

3. Sposób wydawania upoważnień do przetwarzania danych osobowych określa ***załącznik nr 4*** do zarządzenia.

4. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana do:
   1) zapoznania się z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych;
   2) przechodzenia okresowych szkoleń z obszaru ochrony danych osobowych;
   3) stosowania określonych w Urzędzie procedur i środków przetwarzania;
   4) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym;
   5) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
   6) nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych, zawierających dane osobowe oraz bez zabezpieczania dostępu do danych osobowych przetwarzanych w systemie informatycznym;
   7) zaprzestania przetwarzania danych osobowych po ustaniu stosunku zatrudnienia.

ROZDZIAŁ VI
Rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych

§ 6.

1. W Urzędzie prowadzi się **rejestr czynności przetwarzania danych** (jako Administrator) oraz **rejestr kategorii czynności przetwarzania danych** (jako podmiot przetwarzający), których zawartość określa art.30 RODO.

2. Prowadzony rejestr czynności przetwarzania danych i rejestr kategorii czynności przetwarzania dla Urzędu może być udostępniany na żądanie organu nadzorczego.

3. Sposób tworzenia rejestru czynności przetwarzania danych oraz rejestru kategorii czynności przetwarzania danych określa ***załącznik nr 5*** do zarządzenia.

4. Rejestry, o których mowa w ust. 1 mają formę pisemną, w tym formę elektroniczną.

ROZDZIAŁ VII
Umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych

§ 7.

1. Kierownik komórki organizacyjnej Urzędu, pracownik zatrudniony na samodzielnym stanowisku, realizując zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, odpowiada za wybór podmiotu przetwarzającego, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.

2. Kierownik komórki organizacyjnej Urzędu, pracownik zatrudniony na samodzielnym stanowisku, który w imieniu administratora przyjmuje powierzenie przetwarzania danych (podmiot przetwarzający – „procesor"):
   1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
   2) podejmuje wszelkie środki bezpieczeństwa, w szczególności w stosownych przypadkach:
      a) pseudonimizację i szyfrowanie danych osobowych,
      b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
      c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
      d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
   3) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;
   4) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
   5) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków związanych z bezpieczeństwem danych, postępowaniem w przypadku wystąpienia naruszeń, przeprowadzania oceny skutków dla ochrony danych i uprzednich konsultacji;
   6) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
   7) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

3. Szczegółowy sposób postępowania w zakresie wskazanym w ust. 1 i 2 określa ***załącznik nr 6*** do zarządzenia.

ROZDZIAŁ VIII
Prawa osób, których dane są przetwarzane w Urzędzie, niewymagające wniosku obywatela oraz sposób ich realizacji

§ 8.

1. Podstawowym prawem osoby, której dane są przetwarzane w Urzędzie, jest bycie poinformowanym o fakcie przetwarzania danych osobowych.

2. Zakres realizacji prawa wskazanego w ust. 1 zależy od sposobu pozyskania danych osobowych, tj. bezpośrednio od osoby, której dane dotyczą, lub w sposób inny niż od osoby, której dane dotyczą.

§ 9.

1. W przypadku zbierania danych od osoby, której dane dotycza, administrator w momencie pozyskiwania danych ma obowiązek przekazać w szczególności następujące informacje o:
   1) tożsamość administratora danych;
   2) celach przetwarzania danych;
   3) przysługujących prawach osobie, której dane są przetwarzane.

2. Przepisu ust. 1 nie stosuje się, gdy i w zakresie w jakim osoba, której dane dotyczą, dysponuje już tymi informacjami.

3. Ramowy, zgodny z art.13 RODO, zakres **klauzuli informacyjnej** w przypadku zbierania danych od osoby, której dane dotyczą, określa ***załącznik nr 7*** do zarządzenia.

§ 10.

1. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, Administrator podaje osobie, której dane dotyczą w szczególności następujące informacje o:
   1) tożsamości administratora danych;
   2) celach przetwarzania danych;
   3) przysługujących prawach osobie, które dane są przetwarzane;
   4) od kogo otrzymał dane osobowe.

2. Informacje, o których mowa w ust. 1, podaje sie najpóźniej:
   1) nie później niż w terminie miesiąca od momentu pozyskania danych osobowych lub
   2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – przy pierwszej takiej komunikacji z tą osobą lub
   3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – przy ich pierwszym ujawnieniu.

3. Obowiązku, o którym mowa w ust. 1, nie stosuje się gdy i w zakresie w jakim:
   1) osoba, której dane dotyczą, dysponuje już tymi informacjami;
   2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń odpowiednich dla tych danych, lub o ile obowiązek, o którym mowa w ust. 1, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania; w takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
   3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem krajowym przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
   4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

4. Ramowy, zgodny z art.14 RODO, zakres **klauzuli informacyjnej** w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, określa ***załącznik nr 8*** do zarządzenia.

§ 11.

1. Za realizację obowiązku informacyjnego, o którym mowa w § 9 i 10, odpowiedzialni są pracownicy Urzędu, którzy dane osobowe danej osoby będą przetwarzali.

2. Informacje, o których mowa w § 9 i 10, mogą zostać przekazane na piśmie, w tym elektronicznie, a w szczególnych przypadkach mogą zostać odczytane.

3. Każdorazowo należy udokumentować przekazanie informacji, o których mowa w § 9 i 10.

4. Istnieje możliwość konsultowania sposobu realizowania obowiązków, o których mowa w § 9 i 10 z IOD.

ROZDZIAŁ IX
Prawa obywateli, których dane są przetwarzane w Urzędzie, wymagające wniosku

§ 12.

1. Obywatelowi, którego dane są przetwarzane, przysługuje prawo:
   1) dostępu do danych przetwarzanych w Urzędzie oraz uzyskania potwierdzenia, czy Urząd przetwarza jego dane;
   2) sprostowania dotyczących go danych osobowych, które są nieprawidłowe, z uwzględnieniem celów przetwarzania;
   3) do usunięcia danych (tzw. prawo do bycia zapomnianym);
   4) do ograniczenia przetwarzania;
   5) do przenoszenia danych;
   6) do sprzeciwu wobec przetwarzania dotyczących jego danych osobowych.

2. Realizacja praw, o których mowa w ust. 1, odbywa się na podstawie **pisemnego wniosku** osoby, której dane dotyczą.

3. Sposób realizacji praw osoby, której dane dotyczą, wymagających wniosku określa ***załącznik nr 9*** do zarządzenia.

ROZDZIAŁ X
Przetwarzanie danych osobowych na podstawie zgody osoby, której dane są przetwarzane w Urzędzie

§ 13.

1. W szczególnych przypadkach przewidzianych prawem lub w sytuacjach, gdy przetwarzanie jest wymagane dla prawidłowej realizacji zadania, a nie mają zastosowania przesłanki wskazane w § 1 ust. 2, przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą.

2. W celu realizacji zasady rozliczalności zgoda powinna być udokumentowana w formie pisemnej.

3. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy również innych kwestii, oświadczenie zgody musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii.

4. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

5. Ramowy wzór treści **zgody** określa ***załącznik nr 10*** do zarządzenia.

ROZDZIAŁ XI
Udostępnianie danych osobowych

§ 14.

1. Udostępnianie danych osobowych przez Urząd wynika jedynie z obowiązujących przepisów prawa.

2. Pracownicy, do których wpływają wnioski o udostępnienie danych, obowiązani są każdorazowo do przeanalizowania możliwości oraz zakresu udostępnienia danych osobowych w uzgodnieniu z IOD.

3. W celu zapewnienia przez Urząd kontroli nad tym, komu dane są przekazywane, udostępnienie danych powinno odbywać się co do zasady w **formie pisemnej**, co pozwoli w szczególności na udokumentowanie podstawy prawnej udostępnienia danych i podmiotu, który o to się zwróci.

4. Sposób realizacji wniosku o udostępnienie danych, określa ***załącznik nr 9*** do zarządzenia.

ROZDZIAŁ XII
Przekazanie danych osobowych do państw trzecich

§ 15.

1. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może odbywać się jedynie zgodnie z zasadami wskazanymi w rozdziale V RODO.

2. Kierownik komórki organizacyjnej Urzędu, pracownik zatrudniony na samodzielnym stanowisku, obowiązani są zweryfikować istnienie podstawy prawnej uprawniającej do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przed dokonaniem przekazania.

3. Przekazanie danych osobowych odbywa się tylko w formie pisemnej.

ROZDZIAŁ XIII
Naruszenia ochrony danych osobowych

§ 16.

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:
   1) zniszczenia lub
   2) utracenia, lub
   3) zmodyfikowania, lub
   4) nieuprawnionego ujawnienia, lub
   5) nieuprawnionego dostępu.

2. Pracownicy Urzędu obowiązani są zgłaszać każde zdarzenie zagrażające bezpieczeństwu, a ustalenie czy stanowi ono naruszenie ochrony danych osobowych należy do IOD.

3. Sposób postępowania w przypadku naruszeń ochrony danych osobowych oraz ich zgłaszanie i dokumentowanie określa ***załącznik nr 11*** do zarządzenia.

ROZDZIAŁ XIV
Przeprowadzenie oceny skutków dla ochrony danych osobowych

§ 17.

1. Ocenę skutków dla ochrony danych osobowych planowanych procesów przetwarzania przeprowadza się, 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 fizycznych.

2. Ocena skutków dla ochrony danych osobowych przeprowadzana jest przez komórkę organizacyjną Urzędu, w której będzie odbywało się lub odbywa się przetwarzanie danych osobowych wymagające przeprowadzenia oceny skutków dla ochrony danych osobowych.

3. Komórka organizacyjna realizująca proces wskazany w ust. 1 jest obowiązana skonsultować z IOD w szczególności kwestie dotyczące:
   1) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych;
   2) metodologii przeprowadzenia oceny skutków dla ochrony danych osobowych;
   3) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń naruszenia praw i wolności osób, których dane dotyczą;
   4) prawidłowości przeprowadzonej oceny skutków dla ochrony danych osobowych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy stosować).

4. Za przeprowadzenie oceny skutków dla ochrony danych osobowych odpowiedzialni są Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach.

§ 18.

1. Ocena skutków dla ochrony danych osobowych, zgodnie z art.35 ust.7 RODO, zawiera co najmniej następujące elementy:
   1) opis planowanych operacji przetwarzania i celów przetwarzania, w tym gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Urząd;
   2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3) ocenę ryzyka naruszenia praw lub wolności obywateli, których dane dotyczą;
   4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

2. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z procesu przetwarzania, Kierownik komórki organizacyjnej, pracownik zatrudniony na samodzielnym stanowisku, który odpowiada za dany proces, dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych osobowych.

3. W sytuacji o której mowa w ust. 2 Kierownik komórki organizacyjnej, pracownik zatrudniony na samodzielnym stanowisku sporządza notatkę, która zawiera w szczególności elementy wskazane w ust. 1 po uwzględnieniu zmian.

4. Kierownik komórki organizacyjnej, pracownik zatrudniony na samodzielnym stanowisku po sporządzeniu notatki, o której mowa w ust. 3, jest obowiązany do przekazania jej IOD.

§ 19.

1. Oceny skutków dla ochrony danych osobowych nie przeprowadza się, jeżeli przetwarzanie odbywa się na podstawie przesłanki wskazanej w § 1 ust. 2 pkt 2 i 3 oraz gdy spełniono łącznie poniższe warunki:
   1) ma podstawę prawną w prawie Unii Europejskiej lub w prawie polskim i prawo takie reguluje daną operację przetwarzania lub zestaw operacji;
   2) oceny skutków dla ochrony danych osobowych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej.

2. Nie stosuje się wyłączenia wskazanego w ust. 1, jeżeli państwa członkowskie Unii Europejskiej uznają za niezbędne, by przed rozpoczęciem przetwarzania w ramach danego procesu dokonać oceny skutków dla ochrony danych osobowych (Komunikat Prezesa UODO).

§ 20.

1. Jeżeli przeprowadzona ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.

2. Ocenę, o której mowa w ust. 1, prowadzi komórka organizacyjna, która odpowiada za dany proces przetwarzania, kontaktując się z UODO przez IOD.

3. Konsultując się z UODO, komórka organizacyjna przedstawia następujące informacje:
   1) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu;
   2) cele i sposoby zamierzonego przetwarzania;
   3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;
   4) gdy ma to zastosowanie – dane kontaktowe IOD;
   5) ocenę skutków dla ochrony danych;
   6) wszelkie inne informacje, których zażąda organ nadzorczy.

§ 21.

Sposób przeprowadzania i dokumentowania oceny skutków dla ochrony danych osobowych (**OSOD**), w angielskiej wersji Data Protection Impact Assessment (**DPIA**) określa ***załącznik nr 12*** do zarządzenia.

ROZDZIAŁ XV
Inspektor Ochrony Danych (IOD)

§ 22.

1. IOD posiada kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie
   ochrony danych oraz umiejętności niezbędne do wypełnienia następujących zadań:
   1) informowania Administratora oraz pracowników Urzędu (w tym stażystów, praktykantów, wolontariuszy, osób wypełniających zadania w ramach umów cywilnoprawnych) o obowiązkach spoczywających na nich z mocy RODO oraz wynikających z innych przepisów w zakresie ochrony danych osobowych;
   2) doradzania Administratorowi oraz pracownikom Urzędu (w tym stażystom, praktykantom, wolontariuszom, osobom wypełniającym zadania w ramach umów cywilnoprawnych) w zakresie obowiązków spoczywających na nich z mocy RODO oraz innych przepisów w zakresie ochrony danych osobowych;
   3) monitorowania przestrzegania RODO oraz innych przepisów o ochronie danych osobowych, polityk ochrony danych osobowych wdrożonych w Urzędzie;
   4) udzielania zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowania wykonania oceny skutków dla ochrony danych osobowych;

5) współpracy z UODO i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenia konsultacji we wszystkich innych sprawach;
6) pełnienia roli punktu kontaktowego dla osób, których dane dotyczą.

2. IOD może wykonywać inne zadania i obowiązki niż wskazane w ust. 1, pod warunkiem że nie będą one powodowały konfliktu interesów.

3. IOD podlega bezpośrednio Burmistrzowi.

§ 23.

1. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2. W ramach wykonywania zadań IOD obowiązany jest do ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko w zakresie ochrony danych osobowych.

3. IOD jest obowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

4. Kierownicy komórek organizacyjnych, pracownicy zatrudnieni na samodzielnych stanowiskach obowiązani są do informowania IOD:
   1) o wszystkich istniejących i planowanych procesach przetwarzania danych oraz konsultowania z IOD tych kwestii, przy czym niezbędne informacje powinny być przekazywane IOD odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;
   2) o każdym spotkaniu kadry kierowniczej oraz innych spotkaniach pracowników, podczas których będą omawiane sprawy związane z ochroną danych osobowych.

§ 24.

1. Zadanie dotyczące informowania Administratora oraz pracowników Urzędu o obowiązkach spoczywających na nich w ramach ochrony danych osobowych IOD wykonuje w szczególności poprzez:
   1) przeprowadzenie szkolenia wstępnego przed rozpoczęciem przez pracowników (w tym stażystów, praktykantów, wolontariuszy, osoby wypełniające zadania w ramach umów cywilnoprawnych) służbowych obowiązków;
   2) prowadzenie lub organizowanie cyklicznych wykładów, szkoleń, warsztatów;
   3) przekazywanie materiałów informacyjnych;
   4) udział w opracowywaniu regulaminów lub procedur związanych z przetwarzaniem danych.

2. Doradzanie Administratorowi oraz pracownikom Urzędu w zakresie obowiązków spoczywających na nich z mocy RODO oraz innych przepisów w zakresie ochrony danych osobowych IOD realizuje poprzez przygotowywanie opinii, notatek służbowych, udział w ocenie skutków dla ochrony danych osobowych.

3. Monitorowanie przestrzegania obowiązujących przepisów związanych z ochroną danych osobowych oraz procedur wewnętrznych IOD realizuje w szczególności poprzez przeprowadzanie czynności monitoringowych, w ramach których zbiera informacje w celu identyfikacji czynności przetwarzania oraz przeprowadza analizę zgodności tego przetwarzania.

4. W ramach współpracy z organem nadzorczym i pełnieniem funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, IOD:
   1) przygotowuje, we współpracy z Administratorem oraz pracownikami Urzędu, odpowiedzi na pisma i zapytania organu nadzorczego;
   2) kontaktuje się w celu uzyskania porady ze strony organu nadzorczego.

5. Szczegółowe zadania realizowane w ramach pełnienia przez IOD punktu kontaktowego dla osób, których dane dotyczą, zostały opisane w rozdziale IX.

ROZDZIAŁ XVI
Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Urzędzie

§ 25.

1. Środki techniczne i organizacyjne w systemach informatycznych stosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie są określone w Instrukcji.

2. Środki techniczne i organizacyjne dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe, są określone w regulacjach wewnętrznych Urzędu.

3. Środki techniczne i organizacyjne, o których mowa w ust. 1 i 2, zostały dobrane na podstawie przeprowadzonej **analizy ryzyka**, w której uwzględniono następujące elementy:
   1) stan wiedzy technicznej;
   2) koszt wdrożenia środków technicznych i organizacyjnych;
   3) charakter przetwarzania, przez który należy rozumieć sposób dokonywania przetwarzania, w tym częstotliwość, czasowość, długoterminowość, masowość;
   4) zakres przetwarzania (katalog operacji na danych osobowych);
   5) kontekst przetwarzania, czyli kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego przetwarzania, otoczenie i zagrożenia dla bezpieczeństwa i integralności danych;
   6) cele przetwarzania.

4. Analiza ryzyka przeprowadzana jest **raz w roku** i w szczególnie uzasadnionych przypadkach (w szczególności w związku z dodatkowymi zadaniami Urzędu, czy w związku z wystąpieniem naruszenia) poddawana przeglądowi pod kątem jej aktualności.

5. Sposób przeprowadzania i dokumentowania wyników analizy ryzyka określa ***załącznik nr 13, 13 a, 13 b, 13 c i 13 d*** do zarządzenia.

ROZDZIAŁ XVII
Odpowiedzialność za przetwarzanie danych osobowych

§ 26.

1. Wszyscy pracownicy Urzędu są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych na swoim stanowisku pracy.

2. Wszystkie osoby upoważnione do przetwarzania danych, zobowiązane są do stosowania zasad zawartych w niniejszej Polityce.

3. Nieprzestrzeganie przepisów o ochronie danych osobowych grozi odpowiedzialnością pracowniczą, karną i cywilną, wynikającą z powszechnie obowiązujących przepisów prawa.

4. W sprawach nieuregulowanych w niniejszej Polityce, mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz.1781 tekst jednolity) i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO /Dz.Urz. UE L 119, s.1 z późn.zm./

5. Niniejsza Polityka jest dokumentem o charakterze wewnętrznym i nie może być udostępniana osobom trzecim oraz innym podmiotom, w żadnej formie, bez zgody Burmistrza.

6. Żadna część niniejszej Polityki nie może być zmieniana ani kopiowana bez wiedzy i zgody Burmistrza.

Załącznik nr 7 do zarządzenia

„WZÓR"

KLAUZULA INFORMACYJNA
w przypadku zbierania danych od osoby, której dane dotyczą

Zgodnie z **art.13 ust.1 i 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) – RODO /Dz.Urz. UE L 119 z 04.05.2016, str.1 z późn.zm./ informuję:

Tożsamość i dane kontaktowe Administratora	Administratorem Pani/Pana danych osobowych jest **Burmistrz Miasta i Gminy Ogrodzieniec z siedzibą Pl.Wolności 25, 42-440 Ogrodzieniec,** tel. +48 32 67 09 700, e-mail: ogrodzieniec@ogrodzieniec.pl
Dane kontaktowe Inspektora Ochrony Danych	Administrator – wyznaczył Inspektora ochrony danych /IOD/ ..... z którym może się Pani/Pan skontaktować poprzez: • adres e-mail: **iod@ogrodzieniec.pl** • pisemnie pod adresem: **42-440 Ogrodzieniec Pl.Wolności 25** Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem.
Cele przetwarzania i podstawa prawna	Pani/Pana dane osobowe przetwarzane są w celu: .... Podstawą prawną przetwarzania Pani/Pana danych jest: • 1) art.6 ust.1 lit. b RODO, tj. 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) art.6 ust.1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze w związku z ..... ; 3) art.6 ust.1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z ..... .
Odbiorcy danych	Pani/ Pana dane mogą być udostępnione podmiotom: • upoważnionym na podstawie przepisów prawa tj. ..... , • przetwarzającym dane na zlecenie i w imieniu Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych, w celu świadczenia określonych w umowie usług np. ..... .
Okres przechowywania danych	Pani/Pana dane będą przechowywane: • • do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów prawa tj. ..... - przez okres: ..... , • przez okres niezbędny do realizacji określonego celu/celów, lecz nie krócej niż przez okres wskazany w przepisach o archiwizacji lub innych przepisach prawa, • do czasu cofnięcia zgody, w przypadku przetwarzania danych na podstawie wyrażonej zgody.
Pani/Pana prawa związane z przetwarzaniem danych osobowych	1) Do żądania od Administratora dostępu do swoich danych osobowych oraz prawo ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec ich przetwarzania oraz prawo do przenoszenia danych. 2) Jeśli przetwarzanie odbywa się na podstawie zgody, do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. 3) Do wniesienia skargi do organu nadzorczego tj. Prezes Urzędu Ochrony Danych Osobowych /PUODO/ ul. Stawki 2, 00-193 Warszawa, gdy uzna Pani/Pan, że przetwarzanie dotyczących jej(-jego) danych osobowych narusza przepisy RODO.
Informacja o zamiarze przekazywania danych osobowych do państwa trzeciego lub orgfanizacji międzynarodowej	Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
Informacja o dowolności lub obowiązku podania danych	Podanie danych osobowych jest: • • niezbędne i wynika z wyżej wskazanych przepisów prawa, • jest dobrowolne w przypadku ..... .
Informacja o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu	Przetwarzanie podanych przez Panią/Pana danych osobowych nie będzie podlegało zautomatyzowanemu poodejmowaniu decyzji, w tym profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO.

• niepotrzebne usunąć

Załącznik nr 8 do zarządzenia

„WZÓR"

KLAUZULA INFORMACYJNA

w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą

Zgodnie z **art.14 ust.1 i 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) – RODO /Dz.Urz. UE L 119 z 04.05.2016, str.1 z późn.zm./ informuję:

Tożsamość i dane kontaktowe Administra	Administratorem Pani/Pana danych osobowych jest **Burmistrz Miasta i Gminy Ogrodzieniec z siedzibą Pl.Wolności 25, 42-440 Ogrodzieniec,** tel. +48 32 67 09 700, e-mail: ogrodzieniec@ogrodzieniec.pl
Dane kontaktowe Inspektora Ochrony Danych	Administrator – wyznaczył Inspektora ochrony danych /IOD/ ..... z którym może się Pani/Pan skontaktować poprzez: • adres e-mail: **iod@ogrodzieniec.pl** • pisemnie pod adresem: **42-440 Ogrodzieniec Pl.Wolności 25** Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem.
Cele przetwarzania i podstawa prawna	Pani/Pana dane osobowe przetwarzane są w celu: .... Podstawą prawną przetwarzania Pani/Pana danych jest: • 1) art.6 ust.1 lit. b RODO, tj. 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) art.6 ust.1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze w związku z ..... ; 3) art.6 ust.1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z ..... .
Kategorie odnośnych danych osobowych	Nazwisko i imię, imiona rodziców, adres zamieszkania/przebywania, PESEL, seria i nr dowodu osobistego, nr telefonu (do kontaktu) ..... . •
Odbiorcy danych	Pani/ Pana dane mogą być udostępnione podmiotom: • upoważnionym na podstawie przepisów prawa tj. ..... , • przetwarzającym dane na zlecenie i w imieniu Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych, w celu świadczenia określonych w umowie usług np. ..... .
Źródło pochodzenia danych osobowych	Źródła: • – prywatne inna osoba np. właściciel nieruchomości, – publiczne inny administrator np. CEIDG, Urząd, rejestr ogólnodostępny.
Okres przechowywania danych	Pani/Pana dane będą przechowywane: • • do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów prawa tj. ..... - przez okres: ..... , • przez okres niezbędny do realizacji określonego celu/celów, lecz nie krócej niż przez okres wskazany w przepisach o archiwizacji lub innych przepisach prawa,
Pani/Pana prawa związane z przetwarzaniem danych osobowych	1) Do żądania od Administratora dostępu do swoich danych osobowych oraz prawo ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec ich przetwarzania oraz prawo do przenoszenia danych. 2) Do wniesienia skargi do organu nadzorczego tj. Prezes Urzędu Ochrony Danych Osobowych /PUODO/ ul. Stawki 2, 00-193 Warszawa, gdy uzna Pani/Pan, że przetwarzanie dotyczących jej/jego danych osobowych narusza przepisy RODO.
Informacja o zamiarze przekazywania danych osobowych do państwa trzeciego lub orgfanizacji międzynarodowej	Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
Informacja o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu	Przetwarzanie Pani/Pana danych osobowych nie będzie podlegało zautomatyzowanemu poodejmowaniu decyzji, w tym profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO.

• niepotrzebne usunąć

Procedura postępowania dot. wniosku obywatela w zakresie przysługujących mu praw /art.15, 16, 17, 18, 20, 21 RODO/ oraz wniosku podmiotu o udostępnienie danych osobowych

CEL PROCEDURY

Sprecyzowanie i wdrożenie w Urzędzie jednolitej i przejrzystej procedury postępowania w przypadku złożenia przez obywatela wniosku w zakresie przysługujących mu praw oraz wniosku podmiotu o udostępnienie danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Kierownicy komórek organizacyjnych Urzędu, pracownicy zatrudnieni na samodzielnych stanowiskach** – w zakresie realizacji wniosku obywatela lub podmiotu.

2. **Pracownik Referatu OR** (pracownik wyznaczony przez Burmistrza) – w zakresie koordynowania, przyjmowania i rozpatrywania wniosków obywateli oraz podmiotów, a także prowadzenia *„Rejestru wniosków i udostępnień danych osobowych"*, we współpracy z IOD.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Pracownik **Referatu OR** koordynuje przyjmowanie i rozpatrywanie **wniosków** obywateli w zakresie praw związanych z ochroną danych osobowych oraz **wniosków** podmiotów o udostępnienie danych osobowych, wpływających do Urzędu.

2. Korespondencję pisemną lub przesłaną za pośrednictwem **e-PUAP**, której treść wskazuje na wniosek obywatela w zakresie praw związanych z ochroną danych osobowych lub wniosek podmiotu o udostępnienie danych osobowych, Sekretariat Burmistrza rejestruje w elektronicznym systemie obiegu dokumentów i przekazuje do Pracownika **Referatu OR**.

3. Korespondencję przesłaną na adresy poczty elektronicznej: ogrodzieniec@ogrodzieniec.pl Sekretariat Burmistrza przekazuje do Pracownika **Referatu OR.**

4. W przypadku korespondencji, o której mowa w ust. 2 i 3, Pracownik **Referatu OR** we współpracy z IOD weryfikuje kompletność danych adresowych oraz informacji umożliwiających zidentyfikowanie komórki merytorycznej odpowiadającej za przetwarzanie tych danych.

5. W przypadku braku wystarczających informacji umożliwiających zidentyfikowanie komórki merytorycznej, do której powinien być przekazany wniosek, Pracownik **Referatu OR** występuje do obywatela lub danego podmiotu o uszczegółowienie informacji.

6. Pracownik **Referatu OR** przekazuje korespondencję do właściwej komórki, która jest zobowiązana do zrealizowania wniosku. W przypadku braku możliwości jego realizacji, informację o przyczynach braku realizacji komórka merytoryczna właściwa do obsługi wniosku przesyła danemu obywatelowi lub podmiotowi oraz Pracownikowi **Referatu OR**.

7. W przypadku gdy korespondencja, której treść wskazuje na wniosek obywatela w zakresie przysługujących mu praw związanych z ochroną danych osobowych, czy też wniosek podmiotu o udostępnienie danych osobowych, została przesłana bezpośrednio do komórki organizacyjnej Urzędu, komórka ta jest zobowiązana do niezwłocznego przekazania wniosku do Pracownika **Referatu OR**.

8. Komórka właściwa w sprawie rozpatrzenia wniosku, o którym mowa w ust. 1, informuje osobę, której wniosek dotyczy, oraz podmiot który skierował wniosek o udostępnienie danych, a także Pracownika **Referatu OR** o sposobie załatwienia wniosku.

9. Wzór **Rejestr wniosków i udostępnień danych osobowych** znajduje się w niniejszej procedurze.

10. Skargi i wnioski realizowane na podstawie Kodeksu postępowania administracyjnego (KPA) obsługiwane są zgodnie z odrębną procedurą obowiązującą w Urzędzie. W przypadku pierwszego kontaktu z Urzędem do każdej korespondencji dołącza się stosowną **klauzulę informacyjną** o przetwarzaniu danych zgodną z wymogami art.13 lub art.14 RODO.

PRAWA OBYWATELI, KTÓRYCH DANE SĄ PRZETWARZANE W URZĘDZIE, WYMAGAJĄCE WNIOSKU

Rozdział I
Prawo dostępu do danych
art.15 RODO

1. Obywatel, którego dane dotyczą, jest uprawniony do uzyskania potwierdzenia, czy w Urzędzie przetwarzane są jego dane osobowe. Jeżeli ma to miejsce, **jest uprawniony do uzyskania dostępu** do nich oraz pozyskania następujących informacji:
   1) w jakim celu są przetwarzane jego dane osobowe;
   2) jakich kategorii danych osobowych dotyczy przetwarzanie;
   3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
   5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   6) o prawie wniesienia skargi do organu nadzorczego;
   7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, obywatel, którego dane dotyczą, **ma prawo zostać poinformowany** o odpowiednich zabezpieczeniach związanych z przekazaniem (art.46 RODO).

3. Jeżeli obywatel, którego dane dotyczą, zwróci się z **wnioskiem** o **dostarczenie kopii** jego danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ten obywatel, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania. Cennik może być ustalony odrębnie dla każdej komórki organizacyjnej lub sporządzony dla całego Urzędu.

4. Jeżeli obywatel, którego dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej **weryfikacji tożsamości** osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie obywatel, którego dane dotyczą.

5. Kopię danych, o której mowa w ust. 3, wydaje się w postaci **wydruku** po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego. Nie wydaje się skanów dokumentów ani ich kserokopii, gdyż mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem.

6. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

Rozdział II
Prawo do żądania sprostowania danych
art.16 RODO

1. Obywatel, którego dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Ponadto obywatel, którego dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

3. Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres Urzędu. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 Kodeksu postępowania administracyjnego (KPA).

Rozdział III
Prawo do żądania usunięcia danych
art.17 RODO
(„prawo do bycia zapomnianym")

1. Obywatel, którego dane dotyczą, ma prawo żądania od Urzędu niezwłocznego usunięcia dotyczących go danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   2) obywatel, którego dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
   3) dane osobowe były przetwarzane niezgodnie z prawem;
   4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że obywatel, którego dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Przepisy ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:
   1) do korzystania z prawa do wolności wypowiedzi i informacji lub
   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega Urząd, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub
   3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub
   4) do ustalenia, dochodzenia lub obrony roszczeń.

Rozdział IV
Prawo do żądania ograniczenia przetwarzania
art.18 RODO

1. Obywatel, którego dane dotyczą, ma prawo żądania ograniczenia przetwarzania jego danych osobowych.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

3. Do ograniczenia może dojść w następujących przypadkach:
   1) obywatel, którego dane dotyczą, kwestionuje prawidłowość danych osobowych, w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;
   2) przetwarzanie jest niezgodne z prawem, a obywatel, którego dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   3) Urząd nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   4) obywatel, którego dane dotyczą, wobec przetwarzania wniósł sprzeciw. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każdy pracownik, który jest upoważniony do przetwarzania tych danych był świadomy że dane te można jedynie przechowywać.

5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

Rozdział V
Prawo do przeniesienia danych
art.20 RODO

1. Jeżeli przetwarzanie odbywa się na podstawie umowy, której stroną jest obywatel, którego dane dotyczą, oraz w sposób zautomatyzowany, obywatel ten ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe go dotyczące. Dotyczy to danych, które obywatel składający żądanie wcześniej dostarczył.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, obywatel, którego dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Urząd bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe i obywatel wykaże, że administrator, któremu mają zostać dane przekazane akceptuje taki sposób pozyskania danych.

3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

4. Wykonanie prawa, o którym mowa w ust. 1, pozostaje bez uszczerbku dla prawa do usunięcia danych.

5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Rozdział VI
Prawo do wniesienia sprzeciwu wobec przetwarzania danych
art.21 RODO

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym, jakim jest między innymi dostęp do informacji publicznej, w tym umieszczanie danych w Biuletynie Informacji Publicznej (BIP) obywatel, którego dane dotyczą z przyczyn związanych z jego szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących go danych osobowych.

2. Administratorowi nie wolno już przetwarzać danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku gdy uzasadniona jest przesłanka do zrealizowania żądania postępuje się zgodnie z ust 2.

„W Z Ó R"

R E J E S T R
wniosków i udostępnień danych osobowych

L.p	Data wpływu wniosku lub żądania (nr pisma)	Dane osoby żądającej lub podmiotu wnioskującego (dane kontaktowe)	Podstawa prawna żądania, wniosku	Przedmiot żądania (np. dostęp do danych, sprostowanie), zakres danych których dot. żądanie, wniosek	Osoba odpowiedzialna za realizację żądania, wniosku	Czy żądanie, zostało spełnione, wniosek zrealizowany ? Jeżeli nie, przyczyna odmowy	Czy odbiorcy danych zostali powiadomieni o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania ? (art.16, 17 ust.1, 18 RODO) Nazwa odbiorcy, data, jeżeli brak informacji - uzasadnienie	Termin odpowiedzi (sposób odpowiedzi e-mail. list, inne), nr pisma
1.	2.	3.	4.	5.	6.	7.	8.	9.