ZARZĄDZENIE NR 0050.64.2020
BURMISTRZA MIASTA I GMINY WLEŃ

z dnia 7 sierpnia 2020 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L 2016.119/1, sprostowanie, Dz.U. UE.L. 2018.127/2 ogólne), ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz.U. z 2019r. poz..1781 oraz art. 33 ust.3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (t.j. Dz.U. z 2020r. poz. 713) zarządzam, co następuje:

§ 1. Wprowadzam Politykę Bezpieczeństwa Ochrony Danych Osobowych stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Miasta i Gminy Wleń.

§ 3. Traci moc Zarządzenie Nr 26/2012 Burmistrza Miasta i Gminy Wleń z dnia 12 maja 2012r. w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę danych osobowych w Urzędzie Miasta i Gminy we Wleniu.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy
Wleń

Artur Zych

Załącznik Nr 1 do Zarządzenia Nr 0050.64.2020

Burmistrza Miasta i Gminy Wleń

z dnia 7 sierpnia 2020 r.

Polityka Bezpiestwa Przetwarzania Danych Osobowych.

Rozdział 1.
Przepisy ogólne

§ 1. 1. Polityka Bezpieczeństwa Przetwarazania Danych Osobowych, zwana dalej "Polityką", jest dokumentem określającym zasady bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Miasta i Gminy we Wleniu:

1) w zbiorach danych tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;

2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

2. Niniejszą Politykę stosuje się również do informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

1) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe;

2) dotyczące wdrożonych zabezpieczeń technicznych i organizacyjnych.

§ 2. Celem Polityki jest określenie i wdrożenie zasad bezpieczeństwa procesu przetwarzania danych osobowych, dystrybucji wewnątrz Urzędu Miasta i Gminy we Wleniu, ochrony przed nie uprawnionym dostępem i modyfikacją, utratą poufności.

§ 3. Urząd Miasta i Gminy we Wleniu, realizując Politykę, dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem;

2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;

3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;

4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewnią rozliczalność, integralność oraz poufność danych.

§ 4. Gwarancję realizacji zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych winny stanowić następujące założenia:

1) wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzania danych osobowych;

2) przeszkolenie pracowników przed dopuszczeniem do przetwarzania danych w zakresie bezpieczeństwa ochrony danych osobowych;

3) okresową kontrolę przestrzegania przez użytkowników wdrożonych zasad postępowania przy przetwarzaniu danych osobowych;

4) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (identyfikator, hasło), umożliwiających im dostęp do danych osobowych – stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.

§ 5. Zasady określone w niniejszej Polityce i dokumentach z nią powiązanych, powinny być znane i stosowane przez wszystkich pracowników, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.

§ 6. Za bieżącą ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych osobowych.

§ 7. 1. Zastosowanie niniejszej Polityki powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych oraz w systemach informatycznych urzędu.

2. Polityka dotyczy wszystkich danych przetwarzanych przez Urząd Miasta i Gminy Wleń niezależnie od formy przetwarzania danych oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych. Polityka reguluje w szczególności przetwarzanie danych w zbiorach ewidencyjnych prowadzonych w formie papierowej oraz systemach informatycznych.

§ 8. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.

Rozdział 2.
Cel polityki bezpieczeństwa

§ 9. Celem niniejszego dokumentu jest zabezpieczenie danych osobowych klientów, mieszkańców, pracowników.

§ 10. Urząd Miasta i Gminy we Wleniu, realizując Politykę, dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewnią rozliczalność, integralność oraz poufność danych.

§ 11. Gwarancję realizacji zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych winny stanowić następujące założenia:

1) wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzania danych osobowych;
2) przeszkolenie pracowników przed dopuszczeniem do przetwarzania danych w zakresie bezpieczeństwa danych osobowych;
3) okresową kontrolę przestrzegania przez użytkowników wdrożonych zasad postępowania przy przetwarzaniu danych osobowych;
4) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (identyfikator, hasło), umożliwiających im dostęp do danych osobowych – stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.

Rozdział 3.
Definicje

§ 12. Przez użyte w niniejszej Polityce pojęcia, wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz pozostałych dokumentów, przyjętych przez Urząd Miasta i Gminy we Wleniu w zakresie ochrony danych osobowych, należy rozumieć:

1) Administrator Danych Osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych

osobowych. Administrator Danych Osobowych to Urząd Miasta i Gminy Wleń reprezentowany przez Burmistrza Miasta i Gminy Wleń;

2) Inspektor Ochrony Danych Osobowych /IODO/ - pracownik wyznaczony przez Administratora, posiadający odpowiednie kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych;

3) Administrator Systemu Informatycznego - pracownik odpowiedzialny za prawidłową pracę systemów informatycznych, w tym utrzymanie ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej, inwentaryzowanie, okresowe sprawdzanie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych;

4) 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;

5) Dane osobowe – oznaczają informację o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię, 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) Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnienie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

8) Ograniczenie przetwarzania - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

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

10) Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, na podstawie umowy powierzenia przetwarzania danych osobowych;

11) Pseudonimizacja - odwracalne 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;

12) Anonimizacja – oznacza trwałe, nieodwracalne przekształcenie danych osobowych powodujące brak możliwości przyporządkowania informacji konkretnej osobie fizycznej;

13) Zgoda osoby, której dane dotyczą - rozumie się przez to dobrowolne, konkretne, świadome, i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

14) Naruszenie ochrony danych osobowych – 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;

15) Osoba upoważniona do przetwarzania danych osobowych – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator jeżeli dane są przetwarzane w systemie informatycznym;

16) System informatyczny – zespół współpracujących ze sobą urządzeń, programów oraz narzędzi programowych zastosowanych w celu przetwarzania danych;

17) Sieć lokalna – połączenie systemów informatycznych administratora wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

18) Użytkownik – każda osoba upoważniona przez ADO do przetwarzania danych, a w szczególności osoba fizyczna świadcząca na rzecz Administratora pracę lub usługi w oparciu o jakikolwiek stosunek prawny, jeżeli to świadczenie pracy lub usług wiąże się z przetwarzaniem danych;

19) Zabezpieczenie danych – zabezpieczenie danych poprzez wdrożenie i eksploatację środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

20) Identyfikator – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych w systemie informatycznym;

21) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Administratorowi oraz Użytkownikowi upoważnionemu do przetwarzania danych w systemie informatycznym;

22) Uwierzytelnianie – proces, którego celem jest weryfikacja tożsamości deklarowanej przez Użytkownika;

23) Rejestr Czynności Przetwarzania Danych (RCPD) – zbiór wszystkich związanych z przetwarzaniem danych działań. Jest to operacja lub zestaw powiązanych ze sobą operacji na danych wykonywanych przez administratora w związku z celem, w jakim te czynności zostają podjęte.

24) Rejestr kategorii przetwarzania danych – jest to spis umów powierzenia danych osobowych prowadzony przez administratora (podmiot, któremu dane są powierzane).

Rozdział 4.
Organizacja przetwarzania danych

§ 13. 1. Podmiotami odpowiedzialnymi za ochronę i przetwarzanie danych osobowych w Urzędzie Miasta i Gminy we Wleniu są:

1) Administrator Danych Osobowych;

2) Inspektor Ochrony Danych Osobowych;

3) Administrator Systemów Informatycznych;

4) Kierownicy komórek organizacyjnych.

2. Administrator Danych Osobowych może upoważnić Administrujących do wykonywania określonych czynności znajdujących się w zakresie zadań Administratora Danych Osobowych, w odniesieniu do danych przetwarzanych w podległych im komórkach organizacyjnych. Do zadań Administratora Danych należą:

1) wyznaczenie Inspektora Ochrony Danych i zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych;

2) wyznaczenie Administratora Systemów Informatycznych oraz określenie zakresu jego zadań i czynności w zakresie ochrony danych osobowych;

3) podejmowanie decyzji o celach i środkach przetwarzania danych osobowych;

4) podejmowanie decyzji dotyczących przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z Inspektorem Ochrony Danych;

5) wdrażanie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych;

6) upoważnienie poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie;

7) wdrożenie w wersji papierowej i elektronicznej również za pośrednictwem Biuletynu Informacji Publicznej rejestru czynności przetwarzania danych osobowych, rejestru upoważnień, rejestru umów powierzenia przetwarzania danych osobowych, rejestru naruszeń i innych rejestrów oraz procedur wynikających z niniejszej Polityki;

8) wdrożenie Polityki Bezpieczeństwa Ochrony Danych;

9) kontrola przestrzegania procedur przetwarzania danych osobowych w Urzędzie Miasta i Gminy Wleń;

10) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurami określonymi w niniejszej Polityce.

3. Inspektor Ochrony Danych Osobowych, do którego zadań należą:

1) nadzorowanie i monitorowanie przestrzegania przepisów prawa o ochronie danych osobowych oraz wewnętrznych procedur w dziedzinie ochrony danych osobowych;

2) sporządzanie raportu z funkcjonowania przyjętych procedur raz w roku w okresie sprawozdawczym tj. do 30 czerwca. Wzór sprawozdania ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi załącznik nr 1 do Polityki;

3) współpraca z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych;

4) informowanie Administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji;

5) prowadzenie rejestru upoważnień do przetwarzania danych;

6) prowadzenie i aktualizacja rejestru naruszeń zasad ochrony danych osobowych;

7) prowadzenie i aktualizacja rejestru czynności przetwarzania danych;

8) prowadzenie i aktualizacja rejestru czynności kategorii przetwarzania danych;

9) prowadzenie i aktualizacja rejestru umów powierzenia przetwarzania danych osobowych;

10) aktualizacje i sprawowanie nadzoru nad dokumentacją z zakresu ochrony danych osobowych;

11) wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe) wraz z administratorem systemu i właścicielem zasobu;

12) informowanie Administratora o wystąpieniu incydentu;

13) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych;

14) nadzorowanie i monitorowanie realizacji obowiązku informacyjnego zgodnie z wymogami RODO;

15) prowadzenie szkoleń z zakresu ochrony danych osobowych;

16) weryfikacja zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie minimum raz w roku sprawozdania dla Administratora.

4. Administrator Systemów Informatycznych, do którego zadań należą:

1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali;

2) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień;

3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;

4) zadania związane z utrzymaniem ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej;

5) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe;

6) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych;

7) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa, w tym instrukcji zarządzania system informatycznym;

8) utrzymanie systemu w należytej sprawności technicznej;

9) inwentaryzowanie oraz okresowe sprawdzenie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych;

10) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych;

11) dokumentowanie ustaleń i dokonywanie innych czynności związanych z ochroną danych osobowych;

12) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, która jest częścią ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i zasady ochrony danych osobowych w Urzędzie Miasta i Gminy Wleń;

13) kontrola przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej, a systemem informatycznym;

14) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków;

15) prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych.

5. Kierownicy komórek organizacyjnych nadzorują bezpieczeństwo przetwarzania danych osobowych w swoich działach/zespołach poprzez:

1) zapewnienie prawidłowego przetwarzania danych osobowych;

2) zapewnienie prawidłowego zabezpieczenia danych w formie papierowej;

3) zapewnienie prawidłowego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

§ 14. 1. Osoby upoważnione do przetwarzania danych osobowych to osoby dopuszczone przez Administratora Danych Osobowych do przetwarzania danych osobowych, na podstawie upoważnienia.

2. Do zadań tych osób należą m.in:

1) przetwarzanie danych zgodnie z zakresem udzielonego upoważnienia;

2) zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

3) przestrzeganie przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych;

4) niezwłoczne zgłaszanie incydentów dotyczących bezpieczeństwa danych osobowych.

Rozdział 5.
Przetwarzanie danych

§ 15. 1. Do przetwarzania danych osobowych w zbiorach danych osobowych mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez ADO. Wzór upoważnienia do przetwarzania danych osobowych określony jest w załączniku nr 2 do niniejszej Polityki.

2. Każdy pracownik mający dostęp do danych osobowych w Urzędzie jest wpisywany do ewidencji osób upoważnionych do przetwarzania danych osobowych, prowadzonej przez Inspektora Ochrony Danych. Wzór ewidencji osób upoważnionych stanowi załącznik Nr 3 do Polityki.

3. Upoważnienia przechowuje się w aktach osobowych pracownika.

4. Rozwiązanie stosunku pracy lub odwołania z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

5. Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia.

6. Zmiana stanowiska, zakresu obowiązków powoduje konieczność aktualizacji zakresu upoważnienia.

§ 16. 1. Każdy pracownik jest zobowiązany do zachowania tajemnicy i poufności danych osobowych oraz sposobów ich zabezpieczenia. W tym celu podpisują pisemne oświadczenie o zobowiązaniu się do zachowania poufności i w tajemnicy danych osobowych. Wzór oświadczenia stanowi załącznik Nr 4 do Polityki.

2. Osoby upoważnione do przetwarzania danych pod groźbą sankcji dyscyplinarnych wynikających z przepisów, mają obowiązek zachowania tajemnicy o przetwarzanych w Urzędzie danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych.

§ 17. Dopuszczenie do przetwarzania danych osobowych przez osoby nie będące pracownikami jest możliwe, po uzyskaniu pozytywnej opinii Inspektora Ochrony Danych oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych.

§ 18. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności, co najmniej jednego użytkownika odpowiedzialnego za te dane.

§ 19. Przetwarzane dane osobowe muszą być zabezpieczone przed udostępnieniem osobom nieupoważnionym.

§ 20. Pracownicy są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:

1) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych;
2) pisemnego zgłaszania nowych zbiorów danych osobowych do IODO;
3) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony.

§ 21. Pracownicy przetwarzający dane osobowe zobowiązani są do:

1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania zbiorami danych osobowych i ich obsługi;
2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych;
3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania zbiorami danych osobowych oraz ich obsługi;
4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
5) nieudzielania informacji o danych osobowych przetwarzanych w zbiorach danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
6) powiadomić o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzanie, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku;
7) bezzwłocznego zawiadamiania Inspektora Ochrony Danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych przetwarzanych w zbiorach danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe;
8) w razie wykrycia naruszenia ochrony danych osobowych każdy pracownik ma obowiązek postępować zgodnie z procedurami zawartymi w niniejszej Polityce.

Rozdział 6.
Pozyskiwanie danych osobowych

§ 22. 1. Dane osobowe przetwarzane w Urzędzie Miasta i Gminy Wleń mogą być pozyskiwane bezpośrednio od osób, których dane dotyczą. Administrator podczas pozyskiwania tych danych podaje informacje wynikające z obowiązku informacyjnego, o którym mowa w Rozdziale 7 niniejszej Polityki.

2. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych i również wypełnić obowiązek informacyjny określony w Rozdziale 7 niniejszej Polityki.

§ 23. Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać w postaci umożliwiającej identyfikację osób, których dotyczą.

§ 24. Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.

§ 25. Dane osobowe, które są zbierane powinny być merytorycznie poprawne.

§ 26. Zakres danych osobowych, które są zbierane powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.

§ 27. Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.

Rozdział 7.
Obowiązek informacyjny i dostęp do danych osobowych

§ 28. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą Administrator podaje następujące informacje:

1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie tożsamość i dane kontaktowe swojego przedstawiciela;
2) gdy ma to zastosowanie – dane kontaktowe Inspektora Ochrony Danych;
3) cel oraz podstawę prawną przetwarzania;
4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) rozporządzenia – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
5) informację o odbiorcach danych osobowych lub kategoriach odbiorców jeżeli istnieją;
6) gdy ma to zastosowanie – informację o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

1) okres przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria tego okresu;
2) informacje o prawie do żądania od administratora dostępu do danych osobowych ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
3) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) art. 9 ust. 2 lit. a) rozporządzenia;
4) informację o prawie wniesienia skargi do organu nadzorczego;
5) informację, czy przetwarzanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
6) informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia, oraz przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

4. Powyższy obowiązek administrator danych nakłada na osoby zatrudnione przy gromadzeniu i przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonania.

5. Obowiązek informacyjny jest realizowany zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak również z innych źródeł.

6. W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie tożsamość i dane kontaktowe swojego przedstawiciela;

2) gdy ma to zastosowanie – dane kontaktowe Inspektora Ochrony Danych;

3) cel przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

4) kategorie odnośnych danych osobowych;

5) informację o odbiorcach danych osobowych lub kategoriach odbiorców jeżeli istnieją;

6) gdy ma to zastosowanie – informację o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

7. Ponadto podczas pozyskiwania danych osobowych Administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:

1) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria tego okresu;

2) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) rozporządzenia – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

3) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

4) jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) rozporządzenia – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

5) informację o prawie wniesienia skargi do organu nadzorczego, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

6) informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia, oraz przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 29. Informacje dotyczące pozyskania danych administrator podaje osobie:

1) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;

3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

§ 30. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

§ 31. 1. Administrator nie podaje informacji o danych, gdy:

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 do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 rozporządzenia;

3) pozyskiwanie lub ujawnienie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, 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 lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy;

2. Powyższy obowiązek Administrator Danych Odobowych nakłada na osoby zatrudnione przy gromadzeniu i przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonania.

§ 32. Jedną z form spełniania obowiązku informacyjnego jest udostępnienie osobom, których dane osobowe są przetwarzane klauzul informacyjnych. Przykładowy wzór klauzuli określony został w załączniku nr 5 do niniejszej polityki. Klauzule informacyjne winny być każdorazowo dostosowane do celu przetwarzania, podstawy prawnej i okresu przechowywania danych.

§ 33. Obowiązek informacyjny należy spełnić w momencie zbierania danych.

§ 34. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

1) cel przetwarzania;

2) kategorie odnośnych danych osobowych;

3) informacja o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalenia tego okresu;

5) informację o prawie żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

6) informację o prawie wniesienia skargi do organu nadzorczego;

7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

8) informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia, oraz przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 35. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 rozporządzenia, związanych z przekazaniem.

§ 36. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopie drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Rozdział 8.
Udostępnianie danych

§ 37. 1. Do udostępniania posiadanych w zbiorach danych osobowych upoważniony jest kierownik komórki organizacyjnej lub pracownik posiadający wymagane upoważnienie.

2. Administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa wyłącznie na pisemny umotywowany wniosek.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik Nr 6 do Polityki.

4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

5. Udostępnienia są ewidencjonowane, wzór ewidencji stanowi załącznik Nr 7 do niniejszej Polityki. Ewidencje zawierają informacje o tym, komu udostępniono, datę kiedy zostały udostępnione oraz jaki zakres danych został udostępniony.

§ 38. Procedura przekazywania danych.

1. Podczas przekazywania dane zabezpiecza się przed ich nieuprawnionym dostępem.

2. Dane przesyłane drogą teleinformatyczną muszą być odpowiednio zabezpieczone przed utratą ich poufności i integralności za pomocą zabezpieczeń kryptograficznych, umożliwiających ich bezpieczne przesyłanie.

Rozdział 9.
Prawa osób, których dane dotyczą

§ 39. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w urzędzie gminy, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

§ 40. Zgodnie z RODO, osobom, których dane osobowe są przetwarzane przysługują następujące prawa:

1) prawo dostępu do danych;

2) prawo do sprostowania danych;

3) prawo do usunięcia danych („prawo do bycia zapomnianym”);

4) prawo do ograniczenia przetwarzania;

5) prawo do przenoszenia danych;

6) prawo wniesienia sprzeciwu;

7) prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

8) prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych, w przypadku przetwarzania danych osobowych z naruszeniem przepisów RODO.

§ 41. Na wniosek osoby, której dane dotyczą, Administrator Danych Osobowych jest zobowiązany do udzielenia informacji. Informacja powinna być udzielona w formie pisemnej oraz powszechnie zrozumiałej.

§ 42. W razie wniesienia żądania oraz wykazania przez osobę, które dane dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów albo są zbędne do realizacji celu dla którego zostały zebrane, Administrator Danych Osobowych bez zbędnej zwłoki dokonuje uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru chyba, że dotyczy to danych osobowych w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

Rozdział 10.
Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

§ 43. W Urzędzie Miasta i Gminy Wleń dane osobowe przetwarzane są w ramach zbiorów danych osobowych, a szczegółowe obszary przetwarzania danych osobowych określa załącznik Nr 8 do niniejszej Polityki. Wykaz obszarów podlega aktualizacji w zależności od potrzeb i zatwierdzeniu przez Administrator Danych Osobowych.

§ 44. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności sprzętu informatycznego oraz innych urządzeń.

§ 45. Wynoszenie zbiorów danych osobowych poza obszar przetwarzania możliwy jest za wyłączną zgodą Administratora Danych Osobowych.

§ 46. Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 9 do niniejszej Polityki. Rejestr prowadzony i na bieżąco aktualizowany jest przez Inspektora Ochrony Danych Osobowych. Każda aktualizacja rejestru podlega zatwierdzeniu przez Administratora Danych Osobowych.

Rozdział 11.
Przekazywanie danych do państwa trzeciego

§ 47. Administrator nie będzie przekazywał danych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek podmiotów takich jak sądy, urzędy, organy ścigania lub osoby, której dane dotyczą.

Rozdział 12.
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 48. Środki ochrony fizycznej danych.

1. Dane osobowe w Urzędzie są przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony przeciwpożarowej.

3. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części innych pomieszczeń.

4. Do pomieszczeń przetwarzania danych osobowych zalicza się:

a) serwerownię;

b) pomieszczenia biurowe, w których zlokalizowane są stacje robocze i/lub zbiory tradycyjne;

c) pomieszczenia, w których przechowywane są sprawne oraz uszkodzone nośniki informacji, kopie zapasowe;

d) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego.

5. Klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym.

6. Podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz.

7. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

8. Na stanowisku pracy, gdzie są przetwarzane dane osobowe w przypadku dłuższej nieobecności pracownika lub po zakończeniu pracy, pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, tj. w zamykanej szafie. Ma to uniemożliwić dostęp do nich osobom nieuprawnionym.Ważne jest to przede wszystkim wtedy, kiedy pomieszczenia są sprzątane po godzinach pracy.

9. Rolety w oknach powinny być całkowicie zasłonięte, jeżeli okna Urzędu skierowane są na okna sąsiadujących z Urzędem kamienic.

10. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

11. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych.

12. Zbiór danych osobowych w formie tradycyjnej jest przechowywany w zamkniętej szafie.

13. Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie.

14. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek do dokumentów.

§ 49. Środki sprzętowe, informatyczne i telekomunikacyjne:

1. Sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci poprzez zastosowanie firewalla programowego chroniącego zasoby Urzędu.

2. Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowania.

3. Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

4. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

5. Na stanowiskach, na których są przetwarzane dane osobowe, zainstalowano wygaszacze ekranu.

§ 50. Środki organizacyjne:

1. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

2. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.

3. Kopie zapasowe zbioru danych osobowych nie są przechowywane w tym samym pomieszczeniu co, komputer, na którym są na bieżąco przetwarzane dane osobowe.

Rozdział 13.
Powierzenie przetwarzania danych osobowych

§ 51. 1. Administrator Danych Osobowych:

1) przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego np. do Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, Sądów Powszechnych, Policji i Prokuratury;

2) powierza przetwarzanie danych innemu podmiotowi w drodze umowy powierzenia przetwarzania danych osobowych, zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

2. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz zgodnie z zasadami przetwarzania i zabezpieczeniami określonymi w umowie.

3. Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4. Umowy powierzenia przetwarzania danych osobowych podlegają ewidencji w Rejestrze Umów Powierzenia Przetwarzania Danych Osobowych, określonym w załączniku Nr 10 do niniejszej Polityki. Rejestr prowadzony jest przez Inspektora Ochrony Danych Osobowych.

Rozdział 14.
Rejestrowanie czynności przetwarzania danych

§ 52. 1. Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, za które odpowiada. Rejstr zawiera następujące informacje:

1) nazwę;

2) dane kontaktowe;

3) dane kontaktowe współadministratorów;

4) dane kontaktowe Inspektora Ochrony Danych;

5) nazwa czynności przetwarzania;

6) jednostka organizacyjna (departament, dział);

7) cele przetwarzania zgodnie z art. 30 ust. 1 pkt. b;

8) opis kategorii osób, których dane dotyczą zgodnie z art. 30 ust. 1 pkt. c rozporządzenia;

9) opis kategorii danych osobowych zgodnie z art. 30 ust. 1 pkt. c rozporządzenia;

10) podstawa prawna;

11) źródło danych;

12) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione zgodnie z art. 30 ust. 1 pkt. f rozporządzenia;

13) planowany termin usunięcia danych;

14) kategorie odbiorców (innych niż podmiot przetwarzający), którym dane osobowe zostały lub zostaną ujawnione w państwach trzecich zgodnie z art. 30 ust. 1 pkt. d rozporządzenia;

15) nazwa systemu lub oprogramowania;

16) kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych zgodnie z art. 30 ust.1 pkt. d rozporządzenia;

17) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, zgodnie z art. 32 ust. 1 rozporządzenia.

2. Rejestr prowadzi się w formie papierowej oraz elektronicznej.

3. Administrator udostępnia rejestr na żądanie Organu Nadzorczego.

4. Administrator prowadzi rejestr kategorii przetwarzania danych, zawierający wykaz umów powierzenia danych osobowych.

Rozdział 15.
Postępowanie w przypadku naruszenia ochrony danych

§ 53. 1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je Organowi Nadzorczemu właściwemu zgodnie z art. 55 rozporządzenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie powinno zawierać:

1) imię i nazwisko zgłaszającego;

2) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;

3) określenie wszelkich informacji mogących wskazywać na przyczynę naruszenia;

4) określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 54. Inspektor Ochrony Danych lub osoba upoważniona dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

§ 55. W przypadku stwierdzenia naruszenia zasad ochrony danych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych i dokonuje kwalifikacji naruszenia jako naruszenie niskie lub wysokie.

§ 56. W przypadku kwalifikacji naruszenia niskiego należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi załącznik Nr 11 do niniejszej Polityki.

§ 57. O fakcie naruszenia danych osobowych każdy pracownik Administratora jest zobowiązany do niezwłocznego poinformowania bezpośredniego przełożonego, Inspektora Ochrony Danych oraz w przypadku danych osobowych przetwarzanych z użyciem systemu informatycznego służącego do przetwarzania danych osobowych -Administratora Systemu Informatycznego.

§ 58. Po przywróceniu normalnego stanu systemu informatycznego należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych. Należy przedsięwziąć działania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

§ 59. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych.

§ 60. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

§ 61. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań obowiązujących w Urzędzie.

Rozdział 16.
Analiza ryzyka bezpieczeństwa informacji

§ 62. Celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykiem i zabezpieczeniem. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.

§ 63. Zarządzanie ryzykiem w bezpieczeństwie informacji powinno zapewnić:

1) zidentyfikowanie ryzyka;

2) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia;

3) informowanie o prawdopodobieństwie i następstwach ryzyka;

4) ustanowienie priorytetów postępowania z ryzykiem;

5) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka;

6) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem;

7) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem;

8) szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

Rozdział 17.
Dodatkowe elementy bezpieczeństwa ochrony danych osobowych

§ 64. Stosowanie zasady „czystego ekranu” - w przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.

§ 65. Stosowanie zasady „czystego biurka” - w trakcie pracy użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne w tym czasie do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony, powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy użytkownik poprzez zamknięcie na klucz w szafie zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych.

§ 66. Stosowanie zasady „czystej drukarki” mającej na celu uniemożliwienie osobom trzecim zabrania wydruków z drukarek (szczególnie ogólnodostępnych). Drukowane informacje powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania i podejrzenia, iż wydruk zostanie wydrukowany bez nadzoru, należy skontaktować się z osobą odpowiedzialną za eksploatację urządzenia.

§ 67. Stosowanie zasady „czystego kosza” oznacza ochronę niepotrzebnych dokumentów papierowych i miękkich nośników zawierających dane osobowe w sposób uniemożliwiający ich ponowne odczytanie poprzez bieżące korzystanie z niszczarek, umieszczanie w specjalnie przeznaczonych do tego celu zaplombowanych pojemnikach itp.

§ 68. Niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej.

§ 69. Stosowanie się do pozostałych wewnętrzych instrukcji i zarządzeń związanych z bezpieczeństwem informacji, w tym m.in. Instrukcji postępowania z kluczami, oraz zabezpieczenia pomieszczeń i budynku Urzędu Miasta i Gminy we Wleniu, Instrukcji Zarządzania System Informatycznym.

§ 70. Zachowanie w poufności wszelkich informacji w tym w szczególności przetwarzanych danych osobowych.

§ 71. Użytkownicy - osoby przetwarzające dane osobowe mogą korzystać wyłącznie z elektronicznych nośników (w szczególności pendrivy, dysków zewnętrznych, CD-R, DVD) oraz komputerów przenośnych przeznaczonych do użytku służbowego.

Rozdział 18.
Postanowienia końcowe

§ 72. Polityka Bezpieczeństwa Ochrony Danych Osobowych jest dokumentem wewnętrznym Urzędu Miasta i Gminy Wleń i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 73. Niniejsza Polityka Ochrony Danych obowiązuje na wszystkich stanowiskach oraz obszarach, gdzie dochodzi do przetwarzania informacji podlegających ochronie.

§ 74. Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia danych osobowych.

§ 75. Naruszenie przez pracownika postanowień niniejszej Polityki może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.

Załącznik nr 1

Wzór

Sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1) Oznaczenie administratora danych i adres jego siedziby:
……
……
(podać pełną nazwę oraz adres)

2) Wykaz czynności podjętych przez ADO w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:
3) Datę rozpoczęcia i zakończenia sprawdzenia:
……
……
4) Określenie przedmiotu i zakresu sprawdzenia:
……
……
5) Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:
……
……
6) Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:
……
……
7) Wyszczególnienie załączników stanowiących składową część sprawozdania:
……
……

……

Data i podpis ADO

Załącznik nr 2

Wzór

Wleń, dnia …….

……
(pieczęć jednostki organizacyjnej)
……
(nazwa administratora danych)

UPOWAŻNIENIE NR …….

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)

I Upoważniam Panią/Pana

……..

(imię i nazwisko)

zatrudnioną/zatrudnionego ……..

(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków na stanowisku:……

(zajmowane stanowisko)

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie papierowej i w systemach informatycznych, wg wykazu zbiorów podanych w pkt. II.

II Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:

1. ……
2. ……
3. ……

Jednocześnie zobowiązuję Panią/Pana do zachowania w tajemnicy (również po ustaniu zatrudnienia) danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczenia.
Upoważnienie jest ważne w okresie obowiązywania umowy o pracę.

……

(podpis ADO)

Załącznik nr 3

Wzór

Ewidencja osób upoważnionych

					Zakres upoważnienia		
Lp.	**Imię i nazwisko**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Stanowisko służbowe**	**Dostęp do oprogramowania** (nazwy systemów / zbiorów, do których użytkownik ma dostęp)	**Login/ Identyfikator**	**Uwagi**

Załącznik nr 4

Wzór

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych osobowych z którymi mam styczność podczas wykonywania zadań służbowych, a nie przeznaczonych do publicznego rozpowszechniania.

Potwierdzam, że zapoznałem się z Polityką Bezpieczeństwa Ochrony Danych Osobowych oraz wszelkimi regulacjami z tego zakresu, wprowadzonymi przez Administratora Danych.

Jednocześnie jestem świadomy/a, że osoby upoważnione do przetwarzania danych zobowiązane są zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia, także po ustaniu stosunku pracy lub po upływie ważności upoważnienia oraz podlegają odpowiedzialności karnej wynikającej z art. 266 kodeksu karnego.

Zobowiązuję się do nierozpowszechniania i niewykorzystywania informacji zdobytych w trakcie wykonywania obowiązków pracowniczych, a także po ustaniu zatrudnienia.

Z chwilą ustania zatrudnienia zobowiązuję się do niezwłocznego zwrócenia pracodawcy wszelkich dokumentów oraz innych materiałów dotyczących informacji chronionych.

Przyjmuję do wiadomości i akceptuję, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu przepisów Kodeksu pracy oraz, że strona poszkodowana ma prawo do dochodzenia na zasadach ogólnych odszkodowania odpowiadającego wysokości poniesionej szkody.

……..……

(czytelny podpis pracownika)

Załącznik nr 5

Wzór

Klauzula informacyjna **Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) informuję, iż:**	
TOŻSAMOŚĆ ADMINISTRATORA	Administratorem Pani/Pana danych jest: Burmistrz Miasta i Gminy Wleń z siedzibą w Urzędzie Miasta i Gminy, ul. Pl. Bohaterów Nysy 7 59-610 Wleń.
DANE KONTAKTOWE ADMINISTRATORA	• adres email burmistrz@wlen.pl, • pisemnie na adres: Pl. Bohaterów Nysy 7, 59-610 Wleń • tel. 75 71-36-438
DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	Maja Kodzis • Urząd Miasta i Gminy we Wleniu, Pl. Bohaterów Nysy 7,59-610 Wleń, • tel. 75 71-36-438, • email mkodzis@wlen.pl
CELE PRZETWARZANIA I PODSTAWA PRAWNA	Pani/Pana dane będą przetwarzane w celu realizacji ustawowych zadań: ……. ……..
ODBIORCY DANYCH	Dane będą udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa: …… ……
OKRES PRZECHOWYWANIA DANYCH	Dane będą przechowywane zgodnie Rozporządzeniem Prezesa Rady Ministrów z dnia 20 stycznia 2011r.w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania, a także danych osób, nad którymi sprawowana jest prawna opieka, np. danych dzieci.

Klauzula informacyjna **Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) informuję, iż:**	
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.
ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH	Dane są pozyskiwane od klientów Urzędu Miasta i Gminy we Wleniu oraz od organów publicznych.
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU	Obowiązek podania danych osobowych jest dobrowolny, ale niezbędny do realizacji wskazanych wyżej celów.

Potwierdzenie zapoznania się z klauzulą …….

(Data, podpis)

Załącznik nr 6

Wzór

Wleń, dnia …….

……

……
(wnioskodawca)

…….
(adres jednostki organizacyjnej)

..……..…….
(nazwa administratora danych)

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Podstawa prawna upoważniająca do pozyskania danych:

   ……

2. Wskazanie przeznaczenia dla udostępnionych danych:

   ……

3. Oznaczenie lub nazwa zbioru z którego mają być udostępnione dane:

   …….

4. Zakres żądanych informacji ze zbioru:

   ……

5. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

   ……

……
(podpis wnioskodawcy)

Załącznik nr 7

Ewidencja udostepnienia danych osobowych

Lp.	Imię i nazwisko osoby udostepniającej dane	Imię i nazwisko osoby dla której zostają udostępnione dane	Data udostępnia	Zakres udostępnionych danych

Załącznik nr 8

Obszary przetwarzania danych osobowych

w **Urzędzie Miasta i Gminy we Wleniu, pl. Bohaterów Nysy 7, 59-610 Wleń**

Lp.	**Nr pomieszczenia**	**Nazwa wydziału/samodzielnego stanowiska/nazwa pomieszczenia**
P A R T E R		
1.	2	Urząd Stanu Cywilnego, Ewidencja Ludności, Dowody Osobiste.
2.	3	Inwestycje, Nieruchomości, Gospodarka Przestrzenna, Ochrona Środowiska.
3.	4	Fundusze Unijne i Promocja.
4.	5	Gospodarka Komunalna.
I P IĘ T R O		
5.	6	Sekretariat.
6.	7	Burmistrz Miasta i Gminy Wleń.
7.	8	Zastępca Burmistrza Miasta i Gminy Wleń.
8.	9	Sekretarz Miasta i Gminy Wleń.
9.	10	Księgowość.
10.	12	Księgowość budżetowa.
11.	13	Skarbnik Miasta i Gminy Wleń.
12.	14	Księgowość podatkowa.
13.	15	Informatyk, Obsługa rady, Inspektor Ochrony Danych.
14.	16	Serwerownia.

Załącznik nr 9

Wzór

Rejestr Czynności Przetwarzania danych osobowych

Imię i nazwisko lub nazwa Administratora: Burmistrz Miasta i Gminy Wleń

Dane kontaktowe Administratora: ul. Plac Bohaterów Nysy 7, 59-610 Wleń

Dane Współadministratorów ……..

Dane Inspektora Ochrony Danych: Maja Kodzis, tel. 506-413-433

Nazwa czynności przetwarzania		
Jednostka organizacyjna (departament, dział)		
Cel przetwarzania Art. 30 ust. 1 pkt. b		
Kategoria osób których dane dotyczą Art. 30 ust. 1 pkt. c		
Kategorie danych osobowych Art. 30 ust. 1 pkt. c		
Podstawa prawna		
Źródło danych		
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione		
Planowany termin usunięcia danych Art. 30 ust. 1 pkt. f		
Kategorie odbiorców (innych niż podmiot przetwarzający), którym dane osobowe zostały lub zostaną ujawnione w państwach trzecich Art. 30 ust. pkt. d		
Nazwa systemu lub oprogramowania		
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych Art. 30 ust. 1 pkt. d		
Ogólny opis środków bezpieczeństwa zgodnie z art. 32 ust.1	techniczny	organizacyjny
Transfer do kraju trzeciego lub organizacji międzynarodowej Art. 30 ust. 1 pkt. e	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju lub podmiotu) Art. 30 ust. 1 pkt. e	Jeśli transfer i art. 49 ust. 1 akapit drugi dokumentacja odpowiednich zabezpieczeń Art. 30 ust. 1 pkt. e

Załącznik nr 10

Wzór

Ewidencja Rejestru Umów Powierzenia Przetwarzania Danych Osobowych

Lp.	**Nr umowy**	**Data zawarcia umowy**	**Oznaczenie podmiotu, z którym zawarta jest umowa powierzenia**	**Zakres powierzenia wynikający z umowy**	**Okres, na jaki została zawarta umowa lub termin jej wygaśnięcia**	**Cel powierzenia danych osobowych**

Załącznik nr 11

Wzór

REJESTR NARUSZEŃ

Zgłoszenie naruszenia kierowane do UODO / osoby, której dane dotyczą *

Numer kolejny incydentu ……

Data naruszenia …….. Data zgłoszenia ……..……

Imię i nazwisko lub nazwa administratora ……..

Dane Inspektora Ochrony Danych …….

Opis charakteru naruszenia ochrony danych osobowych **		
Konsekwencje naruszenia ochrony danych osobowych		
Środki naprawcze	zastosowane	
	proponowane	

……

(podpis administratora)

*(niepotrzebne skreślić)

**(nie dotyczy zgłaszania osobie, której dane dotyczą)