POLITYKA OCHRONY DANYCH OSOBOWYCH wraz z Instrukcją zarządzania

systemem informatycznym przetwarzającym dane osobowe

w urzędzie Gminy radzanów

|  |  |
| --- | --- |
| **DIRECT GROUP SP. Z O.O.Ul. Krakowskie Przedmieście 4****00-333 Warszawa** | **Pieczęć firmowa:** |
| **Opracował:** | **Data:** | **Zatwierdził:** | **Data:** |
| **Inspektor Ochrony Danych****AGNIESZKA RADTKE** | **28.09.2018 r.** |  |  |

 [Tytuł dokumentu]

 Spis treści

Wstęp 2

Definicje 3

Zadania IOD 6

Ocena skutków (analiza ryzyka) 8

Opis operacji przetwarzania (inwentaryzacja aktywów). 8

Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO). 8

Analiza ryzyka 9

Definicje użyte w analizie ryzyka 9

Wyznaczenie zagrożeń 9

Reakcja na wartości ryzyka 9

Rejestr czynności przetwarzania 11

Polityka kluczy 11

Wykaz zbiorów danych osobowych 12

Opis struktury zbiorów danych wraz ze sposobem przepływu 12

Zabezpieczenia organizacyjne : 12

Zabezpieczenia fizyczne danych osobowych: 13

Kontrola systemu ochrony danych osobowych 14

Sprawozdanie roczne stanu systemu ochrony danych osobowych 14

Szkolenia pracowników 15

Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe 16

**Zarządzane uprawnieniami użytkowników** 16

Dostęp do systemów informatycznych przetwarzających dane osobowe - zabezpieczenia informatyczne 16

**Polityka haseł** 16

**Hasła do sieci i serwera** 17

**Hasła do programów przetwarzających dane osobowe** 17

**Hasła administratora** 18

Procedura rozpoczęcia, zawieszenia i zakończenia pracy - zabezpieczenia informatyczne 18

Procedura tworzenia kopii zapasowych - zabezpieczenia informatyczne 19

Przechowywanie elektronicznych nośników i dokumentów zawierające dane osobowe- zabezpieczenia informatyczne 21

Oprogramowania antywirusowe- zabezpieczenia informatyczne 22

**Ochrona antywirusowa** 22

Plan ciągłości działania 23

**Ochrona przed nieautoryzowanym dostępem do sieci lokalnej** 23

Postanowienia końcowe 24

# Wstęp

Celem Polityki Ochrony Danych Osobowych, zwana dalej Polityką, oraz Instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwana dalej Instrukcją, jest zapewnienie ochrony danych przetwarzanych przez Urząd Gminy Radzanów przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka wraz z Instrukcją jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia organizacyjne oraz zabezpieczenia informatyczne.

Zastosowane zabezpieczenia mają służyć ochronie danych osobowych i zapewnić:

1. **poufność danych** - dane nie są udostępniane nieupoważnionym osobom;
2. **integralność danych** - dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. **rozliczalność danych** - działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4. **integralność systemu** - nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

# Definicje

1. **Polityka** – rozumie się przez to Politykę Ochrony Danych Osobowych w Urzędzie Gminy Radzanów
2. **Administrator**– Urząd Gminy Radzanów, decydujący o celach i środkach przetwarzania danych osobowych;
3. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez Wójta Urzędu Gminy Radzanów odpowiedzialna za organizację ochrony danych osobowych.
4. **Administrator Systemów Informatycznych** (ASI) – osoba wyznaczona przez ADO odpowiedzialna za funkcjonowanie infrastruktury informatycznej (sprzęt, systemy, aplikacje), za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych.
5. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
6. **Dane osobowe (dane)** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.;
7. **Zbiór danych** - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
8. **Przetwarzanie danych osobowych**- to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
9. **Usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
10. **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
11. **Anonimizacja**- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych;
12. **Zgoda osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
13. **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;
14. **Ocena skutków w ochronie danych (analiza ryzyka) -** to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;
15. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **Administrator systemu** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
17. **Użytkownik** – pracownik Urzędu Gminy Radzanów posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
18. **Zabezpieczenie systemu informatycznego** - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, 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;
19. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;
20. **Podmiot przetwarzający (Procesor)-** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora;
21. **Pseudonimizacja** - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
22. **Szczególne kategorie danych osobowych (dane wrażliwe)** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;
23. **Profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która 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.

# Zadania IOD

Inspektor Ochrona Danych został powołany zgodnie z **Załącznikiem nr 1 Wyznaczenie IOD**

Do najważniejszych obowiązków Inspektora Ochrony Danych należy:

1. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów pranych o ochronie danych i doradzanie im w tej sprawie;
2. monitorowanie przestrzegania przepisów o ochronie danych przez Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe;
3. zapewnienie przetwarzania danych osobowych zgodnie z uregulowaniami Polityki Ochrony Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
4. wydawanie i anulowanie równolegle z Administratorem Upoważnień do przetwarzania danych osobowych;
5. prowadzenie równolegle z Administratorem Ewidencji osób upoważnionych do przetwarzania danych osobowych;
6. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
7. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
8. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
9. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
10. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
11. współpraca z organem nadzorczym.

Inspektor Ochrony Danych ma prawo :

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z

 ochroną danych osobowych w całej organizacji;

1. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z przepisami prawa;
2. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
3. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
4. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

# Ocena skutków (analiza ryzyka)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator / podmiot przetwarzający nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

Ocena skutków musi być wykonana z współudziałem Inspektora Ochrony Danych.

# Opis operacji przetwarzania (inwentaryzacja aktywów).

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w **Załączniku 2 Wykaz zbiorów danych osobowych.**

1. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
	1. nazwę zbioru (opis kategorii osób);
	2. opis celów przetwarzania;
	3. przekazanie danych;
	4. funkcjonalny opis operacji przetwarzania;
	5. aktywa służące do przetwarzania danych osobowych;
	6. informacja o konieczności wpisu do rejestru czynności przetwarzania;
	7. informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

# Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO).

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności:

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9);
2. dane te są adekwatne w stosunku do celów przetwarzania;
3. dane te są przetwarzane przez określony czas (retencja danych);
4. wobec osób, które dane są przetwarzane, wykonano tzw. obowiązek informacyjny (art. 12- 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody);
5. opracowano klauzule informacyjne dla powyższych osób;
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO);
7. prowadzony jest wykaz podmiotów przetwarzających powierzone dane **Załącznik 6 Ewidencja podmiotów zewnętrznych**;

# Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej).

# Definicje użyte w analizie ryzyka

1. **Aktywa** – środki materialne i niematerialne, zabezpieczenia organizacyjne, informatyczne i fizyczne mające wpływ na jakość ochrony danych.
2. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent).
3. **Wpływ** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
4. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

# Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania
2. Zagrożenia powinny być infekowane na podstawie obszaru działalności i adekwatne w stosunku do obszarów biznesowych.
3. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń.
4. Administrator określa Wpływ (W) wystąpienia zagrożenia.
5. Administrator określa Ryzyka (R).

# Reakcja na wartości ryzyka

1. **Akceptacja ryzyka** – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń;
2. **Działania łagodzące**, które może zastosować Administrator w celu zminimalizowania ryzyka:
	1. **Przeniesienie** –przerzucenie ryzyka (outsourcing, ubezpieczenie);
	2. **Unikanie** – eliminacja działań powodujących ryzyko;
	3. **Redukcja** – zastosowanie zabezpieczeń w celu obniżenia ryzyka
3. Analizę ryzyka przeprowadza się w arkuszu **Analiza ryzyka.**
4. Analizę ryzyka określa się za pomocą wzoru:

**P\*W= R**

1. Analiza ryzyka prowadzona jest w skali 3 i 6- stopniowej:
	1. Prawdopodobieństwo- skala 1-3, gdzie 1 to małe prawdopodobieństwo, 2 średnie prawdopodobieństwo, 3 duże prawdopodobieństwo;
	2. Wpływ- skala 1-3, gdzie 1 to mały wpływ, 2 średni wpływ, 3 duży wpływ;
	3. Ryzyko- skala 1-6, gdzie 1-3 to małe ryzyko, 4-5 średnie ryzyko, 6-9 duże ryzyko.

# Rejestr czynności przetwarzania

Zgodnie z art. 30 RODO Administrator (oraz gdy ma to zastosowanie - przedstawiciel administratora) prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiadają. Administrator realizuje obowiązek przez wypełnienie formularza **Rejestr czynności przetwarzania.** Administrator udostępnia rejestr na żądanie organu nadzorczego.

Art.30 ptk. 5 "Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10."

W związku z powyższym, Administrator spełnia przynajmniej jeden z punktów:

1. Liczba pracowników powyżej 250 osób;

2. Przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób;

3. Przetwarzanie danych nie ma charakteru sporadycznego;

4. Przetwarzane są dane wrażliwe.

# Polityka kluczy

1. Polityka kluczy obejmuje siedzibę Urzędu Gminy w Radzanowie; Radzanów 91A w szczególności dostęp do budynku oraz pomieszczeń.
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godzinach:
poniedziałek - piątek 7.30 - 15.30, a sprzątaczki codziennie 6.30-20.00
3. Dostęp do budynku odbywa się przy użyciu kluczy znajdujących się w posiadaniu i pod opieką upoważnionych pracowników.
4. Dostęp do poszczególnych odbywa się przy użyciu kluczy znajdujących się w posiadaniu i pod opieką upoważnionych pracowników.
5. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.

6.   Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.

7. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

8. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.

9. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.

10. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności:

* + wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
	+ wyłączenia oświetlenia,
	+ zabezpieczenia i zamknięcia okien i drzwi,
	+ zamknięcia szaf i szafek na klucz oraz zabezpieczenie kluczy
	+ zastosowania Polityki czystego biurka - zabronione jest pozostawianie niezabezpieczonych dokumentów zawierających dane osobowe po zakończeniu pracy.

11. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

# Wykaz zbiorów danych osobowych

Wykaz zbiorów danych osobowych to ewidencja zbiorów danych osobowych, z określoną lokalizacją w organizacji, określonymi zabezpieczeniami fizycznymi, organizacyjnymi i informatycznymi.

Zbiory danych osobowych występują w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

**Załącznik 2 Wykaz zbiorów danych osobowych.**

# Opis struktury zbiorów danych wraz ze sposobem przepływu

Opis systemów informatycznych, w których przetwarzane są dane osobowe oraz sposób przepływu danych pomiędzy programami został przedstawiony w **Załączniku 3 Opis struktury zbiorów danych w systemach informatycznych wraz ze sposobem przepływu danych pomiędzy nimi.**

# Zabezpieczenia organizacyjne :

1. został wyznaczony Inspektor Ochrony Danych nadzorujący przestrzeganie zasad ochrony danych osobowych **Załącznik 1 Wyznaczenie IOD**;
2. została opracowana i wdrożona Polityka Ochrony Danych Osobowych;
3. została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym;
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora **Załącznik 5 Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych;**
5. prowadzona jest Ewidencja osób upoważnionych do przetwarzania danych **Załącznik 4 Ewidencja osób upoważnionych do przetwarzania danych osobowych**;
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy (oświadczenie o poufności) **Załącznik 5 Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych;**
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
10. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe, których Administratorem jest Urząd Gminy Radzanów

# Zabezpieczenia fizyczne danych osobowych:

Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej:

1. drzwi zamykane na klucz;
2. zamknięte na klucz szafy;
3. niszczarki dokumentów;
4. Polityka kluczy;
5. Polityka czystego biurka;
6. alarm;
7. gaśnice;
8. Monitoring wizyjny
9. Kraty w oknach

**Zabezpieczenia informatyczne:**

Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji zarządzania systemem informatycznym.

# Kontrola systemu ochrony danych osobowych

Zgodnie z art. 32 RODO, Administrator będzie regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu opracował procedurę kontroli. IOD jest odpowiedzialny za przeprowadzenie audytu.

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych.
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych upoważniony jest IOD, wyznaczeni kontrolerzy wewnętrzni, najwyższe kierownictwo.
4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami Ustawy.
5. IOD przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
6. Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi. Na jego podstawie IOD inicjuje działania korygujące lub zapobiegawcze.

# Sprawozdanie roczne stanu systemu ochrony danych osobowych

1. Raz w roku IOD przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych
2. W spotkaniu sprawozdawczym uczestniczą: IOD, Kierownicy referatów w których przetwarzane są dane osobowe, Informatyk.

# Szkolenia pracowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada IOD, a za jego zorganizowanie odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Politykami, instrukcjami oraz Regulaminami obowiązującymi u Administratora, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje zakończone podpisaniem przez pracownika Oświadczenia o poufności.

Dokument ten jest przechowywany w aktach osobowych pracowników.

Po zakończonym szkoleniu Administrator nadaje pracownikowi Upoważnieni do przetwarzania danych osobowych. Dokument ten jest przechowywany w aktach osobowych pracowników.

# Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe

## **Zarządzane uprawnieniami użytkowników**

1. Pracownik przed podjęciem działań mających na celu przetwarzanie danych osobowych w systemie informatycznym lub w zbiorze papierowym otrzymuje od Administratora pisemne Upoważnienie do przetwarzania danych osobowych. Informacja o nadaniu upoważnienia przekazywana jest Inspektorowi Ochrony Danych.
2. W przypadku nadania bądź zmiany uprawnienia, IOD zobowiązany jest do sprawdzenia, czy użytkownik:
	1. odbył szkolenie z zakresu ochrony danych osobowych;
	2. podpisał oświadczenie o zachowaniu poufności;
	3. będzie przetwarzał dane osobowe w zakresie i celu określonym w Polityce i Instrukcji;
	4. zakres ustanowionego upoważnienia jest adekwatny do zakresu obowiązków służbowych.
3. W celu usunięcie uprawnień użytkownikowi Główny Informatyk (ASI) jest zobowiązany do wyrejestrowania go z systemu po uprzednim poinformowaniu o sytuacji IOD.
4. Usunięty identyfikator użytkownika nie może być przydzielany innej osobie.
5. Administrator bądź bezpośredni przełożony w imieniu Administratora, w sposób formalny, zgodnie z powyższą procedurą, nadaje upoważnienie do przetwarzania danych osobowych.
6. Upoważnienie do przetwarzania danych osobowych jest przechowywane w aktach osobowych pracownika.

# Dostęp do systemów informatycznych przetwarzających dane osobowe - zabezpieczenia informatyczne

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

## **Polityka haseł**

1. Bezpośredni przełożony pracownika informuje ASI oraz IOD o nadaniu upoważnienia do przetwarzania danych osobowych w wybranych systemach informatycznych, przed przystąpieniem pracownika do przetwarzania.
2. W upoważnieniu określony jest zakres możliwych działań pracownika w wyznaczonych systemach.
3. Zakres upoważnienia obejmuje: Wgląd, Archiwizację, Modyfikację, Usunięcie, Uprawnienia Administracyjne.
4. ASI informuje użytkownika o nadaniu pierwszego hasła do systemu.
5. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
6. Użytkownik systemu w trakcie pracy w systemie może zmienić swoje hasło.
7. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów (swoich oraz bliskich osób) oraz numerów rejestracyjnych samochodów, numerów telefonów.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabronione jest zapisywanie haseł w sposób jawny oraz udostępnianie ich innym osobom.

## **Hasła do sieci i serwera**

1. Hasło dostępu do (serwera / sieci) składa się co najmniej z 12 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 6 miesięcy i jest wymuszana przez system.

## **Hasła do programów przetwarzających dane osobowe**

**system pl.ID (aplikacja ŹRÓDŁO)**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

Program **EMUiA**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

Program **Selwin**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

Program **Xpertis**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

Program **WODA32**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

Program **PROBIT**:

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.

## **Hasła administratora**

1. Hasło administratora składa się co najmniej z 12 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 90 dni.
4. Administrator zobowiązany jest do prowadzenia metryk haseł administratora i umieszczenie ich w zamkniętych kopertach, odrębnych dla każdego z systemów w sejfie, w pokoju 17
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

# Procedura rozpoczęcia, zawieszenia i zakończenia pracy - zabezpieczenia informatyczne

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem loginu i hasła.
2. Użytkownik jest zobowiązany do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do podjęcia wszelkich działań w celu uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych – tzw.

**Polityka czystego ekranu**.

1. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 15 minut system automatycznie aktywuje wygaszacz.
2. Po zakończeniu pracy, użytkownik zobowiązany jest:
	1. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
	2. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe;
	3. dokumentacje oraz nośniki schować do szafy zamkniętej na klucz;
	4. klucze należy przechowywać w miejscu znanym jedynie pracownikowi;

# Procedura tworzenia kopii zapasowych - zabezpieczenia informatyczne

1. W celu zapewnienia optymalnego poziomu ochrony danych osobowych w systemach informatycznych Urzędu Gminy Radzanów stosuje się zasadę przetwarzania informacji zawartych w bazach danych Urzędu w oparciu o architekturę klient-serwer. Przetwarzanie danych odbywa się w bazach danych na dedykowanych dla systemu/aplikacji serwerach.
2. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Urzędu, stanowią jedynie końcówki klienckie systemu komputerowego.
3. Wszystkie informacje ( w tym dane osobowe) przetwarzane na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.
4. W szczególnych przypadkach za zgodą ADO, aplikacje oraz dane osobowe mogą być przechowywane lokalnie na stanowiskach komputerowych niepołączonych z siecią LAN/WAN. W takim przypadku obowiązek wykonywania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych i bezpiecznego przechowywania ciąży bezpośrednio na użytkowniku danej aplikacji.
5. Kopie baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:
	* + 1. w cyklu dobowym za pomocą aplikacji archiwizujących tworzone są pełne kopie baz danych aplikacji
			2. dane z serwera raz w miesiącu kopiowane są na płyty DVD. Płyty DVD są przechowywane w szafie pancernej w pomieszczeniu sekretariatu.
6. Wraz z kopią zbioru danych osobowych wykonywana jest kopia środowiska pracy (profile użytkowników domeny Radzanów).
7. Administrator systemu sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
8. Zasady przechowywania kopii:
9. kopie awaryjne danych osobowych oraz oprogramowania są przechowywane w przeznaczonej do tego celu metalowej szafie w wyznaczonym pomieszczeniu,
10. kopie bezpieczeństwa z systemów: Xpertis , Płatnik, Selwin przechowywane są na dysku wymiennym
11. dostęp do metalowej szafy mają tylko upoważnieni pracownicy, tj. administrator systemu i administrator bezpieczeństwa informacji.
12. Kopie zapasowe przechowuje się przez okres określony dla poszczególnych danych osobowych zgodnie z odrębnymi przepisami.
13. Kopie archiwalne miesięczne przechowywane są przez okres 3 miesięcy, po czym nośnik poddawany jest kolejnemu procesowi zapisania danych archiwalnych.
14. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie ( co najmniej metalowa szafa, w zabezpieczonym pomieszczeniu)
15. Administrator systemu przegląda okresowo kopie zapasowe i ocenia ich przydatność do odtworzenia systemu w wypadku jego awarii. Stwierdzenie utraty ich przydatności, upoważnia administratora systemu do ich natychmiastowego zniszczenia.
16. Wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce
17. Wydruki zawierające dane osobowe należy niszczyć w niszczarkach nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

# Przechowywanie elektronicznych nośników i dokumentów zawierające dane osobowe- zabezpieczenia informatyczne

Procedura określa sposób postępowania z nośnikami na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

**Elektroniczne nośniki informacji**

1. Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny administratora danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonym każdemu użytkownikowi przez administratora systemu.
2. Elektroniczne zewnętrzne nośniki informacji mogą być używane w wyjątkowych sytuacjach związanych z realizacją określonych zadań, a w innych przypadkach wyłącznie za zgodą Administratora Danych Osobowych.
3. W przypadku posługiwania się elektronicznymi nośnikami informacji pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do uprzedniego sprawdzenia go programem antywirusowym w celu wyeliminowania ewentualnych zagrożeń.
4. Zakazuje się przetwarzania zbiorów danych osobowych w całości na elektronicznych nośnikach informacji oraz ich przesyłania pocztą elektroniczną , nawet w postaci zaszyfrowanej. Dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
5. Elektroniczne zewnętrzne nośniki informatyczne przechowywane są w miejscach, zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem .
6. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych biurkach lub szafach biurowych.
7. Dane w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 3 dni, po wykorzystaniu tych danych, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania,
8. 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, nośnik niszczy się trwale w sposób uniemożliwiający odczytanie danych.
9. Nośniki informacji jednorazowego użytku takie jak płyty CD-R, DVD-R, zawierające nieaktualne lub zbędne kopie danych likwiduje się poprzez fizyczne zniszczenie w taki sposób, by nie można było odczytać ich zawartości.
10. Decyzję o likwidacji danych osobowych przetwarzanych bezpośrednio w systemie informatycznym oraz danych osobowych przechowywanych w kopiach zapasowych podejmuje osoba nadzorująca pracę na określonym zbiorze danych osobowych
w porozumieniu z Administratorem Danych Osobowych.
11. Przechowywane w systemie informatycznym kopie awaryjne lub w postaci wydruków dane osobowe, które przestały być użyteczne, podlegają usunięciu lub zniszczeniu w sposób trwały uniemożliwiający ich odczytanie.

# Oprogramowania antywirusowe- zabezpieczenia informatyczne

## **Ochrona antywirusowa**

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Za ochronę antywirusową odpowiada administrator systemu informatycznego.
2. Sprawdzanie obecności wirusów komputerowych, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła obywa się odbywa się za pomocą licencjonowanego oprogramowania antywirusowego zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora systemu.
3. Oprogramowanie antywirusowe jest instalowanie centralnie na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do sieci, także na komputerach nie podłączonych do sieci, na których przetwarzane są dane osobowe.
4. Aktualizacja oprogramowania antywirusowego odbywa się na bieżąco w sposób automatyczny.
5. Po każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić ASI.
6. Po usunięciu wirusa ASI przywraca aplikacje do pełnej funkcjonalności .

# Plan ciągłości działania

## **Ochrona przed nieautoryzowanym dostępem do sieci lokalnej**

1. Administrator systemu jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
2. sieci lokalnej i sieci rozległej,
3. stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej
4. Przed nieautoryzowanym dostępem do sieci i systemów zastosowano system zabezpieczeń firewall.
5. Połączenie z Internetem jest zabezpieczone na styku sieci firewall’em na bazie systemu Linux.
6. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości wystąpienia wirusów.
7. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

**Ochrona przed awarią zasilania**

1. System, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami
3. spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.
4. Dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych należy zabezpieczyć przed zanikiem napięcia wykorzystując centralny UPS i generator prądu.

# Postanowienia końcowe

1. Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy komórek organizacyjnych są obowiązani zapoznać się z zasadami wynikającymi z Polityki Ochrony Danych Osobowych.
3. Kierownicy komórek organizacyjnych są zobowiązani zapoznać z **Regulaminem Ochrony Danych Osobowych** każdego pracownika.
4. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Ochrony Danych Osobowych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
6. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
7. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r., o ochronie danych osobowych (tj. Dz.U. 24 maja 2018 poz. 1000) oraz wydanych na jej podstawie aktów wykonawczych oraz 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).