
	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	1 z 46
		Wydanie	1
		Data wydania	2020-09-01

POLITYKA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH W URZĘDZIE GMINY ŚWILTZA

WRZESIEŃ 2020


	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltcza	Strona	2 z 46
		Wydanie	1
		Data wydania	2020-09-01

METRYKA DOKUMENTU

Nazwa jednostki organizacyjnej	Urząd Gminy Świltcza		
Tytuł dokumentu	Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Świltcza(PBDO)		
System	System Ochrony Danych Osobowych (SODO)		
Rodzaj	Dokument wiodący		
Zarządzenie	Wójta Gminy Świltcza numer 140.2020 z dnia 01.09.2020 r.		
Zastosowanie	Urząd Gminy Świltcza, Gminna Komisja Rozwiązywania Problemów Alkoholowych		
Status	Dokument finalny	Liczba stron	65

HISTORIA ZMIAN

Wersja	Data wersji	Opis zmiany	Akcja	Rozdział	Zatwierdził
1.0	01.09.2020	Aktualizacja do wymagań ogólnego rozporządzenia o ochronie danych (RODO),	Ustanowienie nowej Polityki bezpieczeństwa danych osobowych	Wszystkie	Wójt Gminy Świltcza
-	-	-	-	-	-


	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	3 z 46
		Wydanie	1
		Data wydania	2020-09-01

SPIS TREŚCI

Rozdział I.	Postanowienia ogólne	4
Rozdział II.	Definicje i skróty użyte w Polityce	4
Rozdział III.	Zakresy odpowiedzialności za przetwarzanie i ochronę danych osobowych	6
Rozdział IV.	Uwzględnienie ochrony danych w fazie projektowania (privacy by desing) – tworzenie nowych zbiorów danych	9
Rozdział V.	Prawa i wolności osób, których dane dotyczą	10
Rozdział VI.	zasady dotyczące przetwarzania danych osobowych	13
Rozdział VII.	Domyślna ochrona danych osobowych	13
Rozdział VIII.	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	13
Rozdział IX.	Rejestr Czynności Przetwarzania	14
Rozdział X.	Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych	14
Rozdział XI.	Zarządzanie dostępem do danych osobowych	16
Rozdział XII.	Udostępnianie i powierzanie danych osobowych	17
Rozdział XIII.	Zarządzanie ryzykiem danych osobowych	19
Rozdział XIV.	Kontrola przetwarzania i stanu zabezpieczenia danych osobowych	20
Rozdział XV.	Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych	21
Rozdział XVI.	Postanowienia końcowe	22

SPIS ZAŁĄCZNIKÓW

Załącznik numer 1:	Wzór wniosku o utworzenie nowego zbioru danych lub czynności przetwarzania w ramach istniejącego zbioru danych
Załącznik numer 2:	Rejestr czynności przetwarzania
Załącznik numer 3:	Klauzula informacyjna – zbieranie danych od osoby
Załącznik numer 4:	Klauzula informacyjna – zbieranie danych z innych źródeł
Załącznik numer 5:	Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe
Załącznik numer 6:	Ogólna Polityka Informacyjna
Załącznik numer 7:	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik numer 7a:	
Załącznik numer 8:	Wniosek o udostępnienie danych osobowych
Załącznik numer 9:	Wzór ewidencji udostępnień danych osobowych
Załącznik numer 10:	Wzór umowy powierzenia przetwarzania danych
Załącznik numer 11:	Wzór ewidencji umów powierzenia przetwarzania danych osobowych
Załącznik numer 12:	Ankieta identyfikacji ryzyk
Załącznik numer 13:	Plan postępowania z ryzykiem
Załącznik numer 14:	Rejestr ryzyk bezpieczeństwa informacji
Załącznik numer 15:	Karta oceny naruszenia/podejrzenia wystąpienia naruszenia
Załącznik numer 16:	Rejestr Naruszeń
Załącznik numer 17:	Zawiadomienie osoby fizycznej o naruszeniu
Załącznik numer 18:	Wzór zgody na przetwarzanie danych osobowych razem z klauzulą informacyjną

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	4 z 46
		Wydanie	1
		Data wydania	2020-09-01


ROZDZIAŁ I. POSTANOWIENIA OGÓLNE

- Niniejsza „Polityka Bezpieczeństwa Danych Osobowych” zwana dalej Polityką, została opracowana w Urzędzie Gminy Świlcza. Polityka określa zasady i wymagania w zakresie bezpieczeństwa danych osobowych przetwarzanych w każdej formie (zarówno tradycyjnie jak i w systemach informatycznych).
- Polityka obejmuje swym zakresem Urząd Gminy Świlcza oraz Gminną Komisję Rozwiązywania Problemów Alkoholowych dla której Wójt Gminy Świlcza jest Administratorem Danych Osobowych na podstawie przepisów Ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.
- Polityka została opracowana proporcjonalnie do realizowanych w Urzędzie Gminy Świlcza czynności przetwarzania w oparciu o art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- Celem Polityki jest zapewnienie powszechnego stanu, w ramach którego przetwarzanie realizowane w Urzędzie Gminy Świlcza:
 - odbywa się w zgodzie z Rozporządzeniem;
 - chroni prawa i wolności osób, których dane dotyczą;
 - gwarantuje stopień bezpieczeństwa odpowiadający ryzyku poszczególnych czynności przetwarzania (zabezpiecza przed przypadkowym lub niezgodnym z prawem zniszczeniem danych, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych, które są przesyłane, przechowywane lub przetwarzane w inny sposób).
- Dla skutecznego realizowania założeń Polityki, Urząd Gminy Świlcza zapewnia:
 - zastosowanie rozwiązań organizacyjnych, proceduralnych i technicznych w formie zabezpieczeń przed zagrożeniami danych osobowych;
 - prowadzenie szkoleń pracowników w zakresie zasad przetwarzania i bezpieczeństwa danych osobowych;
 - okresowe szacowanie ryzyka występujących zagrożeń dla zbiorów danych osobowych lub poszczególnych czynności przetwarzania;
 - bieżącą kontrolę i nadzór nad przetwarzaniem danych osobowych;
 - monitorowanie skuteczności zastosowanych środków ochrony danych.

ROZDZIAŁ II. DEFINICJE I SKRÓTY UŻYTE W POLITYCE


W niniejszej Polityce następujące wyrażenia i określenia mają znaczenie zgodnie z podanymi poniżej definicjami:

- Administrator Danych Osobowych (Administrator, 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 oraz posiadają status Administratora Danych Osobowych dla danych przetwarzanych w ich bieżącej działalności. Ilekroć w Polityce będzie mowa o „ADO”, „Administratorze” lub „Administratorze Danych Osobowych” należy rozumieć, że jest to Urząd Gminy Świlcza oraz Wójt Gminy Świlcza.
- Inspektor Ochrony Danych (IOD)** – osoba, wyznaczona przez ADO, realizuje zadania wynikające z art. 39 Rozporządzenia, polegające na informowaniu, monitorowaniu przestrzegania Rozporządzenia, udzielaniu zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania, współpracy z organem nadzorczym (PUODO) oraz pełniąc funkcję punktu kontaktowego dla organu, a także realizująca inne zadania i obowiązki;
- Informatyk** – pracownik referatu organizacyjno-administracyjnego Administratora właściwy ds. informatyki. Szczegółowy zakres zadań wynika z Regulaminu Organizacyjnego;
- Pracownik** – każda osoba zatrudniona przez Administratora w jakiejkolwiek formie prawnej i upoważniona przez niego do przetwarzania danych osobowych, w szczególności pracownicy samorządowi w rozumieniu przepisów Ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, pracownicy w rozumieniu Ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy, a także zleceniobiorcy, przyjmujący, stażyści, praktykanci i wolontariusze.
- Gminna Komisja Rozwiązywania Problemów Alkoholowych** – gminna komisja rozwiązywania problemów alkoholowych, o której mowa w art. 4¹ ust. 3 Ustawy z dnia z dnia 26 października 1982 r. o wychowaniu

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	5 z 46
		Wydanie	1
		Data wydania	2020-09-01

w trzeźwości i przeciwdziałaniu alkoholizmowi, dla której organem powołującym oraz Administratorem jest Wójt Gminy Świlcza.

6. **Zespół Interdyscyplinarny** – zespół interdyscyplinarny, o którym mowa w art. 9a Ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie, dla którego organem powołującym jest Wójt Gminy Świlcza.
7. **Grupy Robocze** – grupy robocze, o których mowa w art. 9a ust. 10 Ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie tworzone przez Zespół Interdyscyplinarny.
8. **Członek Gminnej Komisji Rozwiązywania Problemów Alkoholowych** – każda osoba wchodząca w skład Gminnej Komisji Rozwiązywania Problemów Alkoholowych, niezależnie od tego czy jest pracownikiem Administratora czy też nie. Jeżeli Polityka nie stanowi inaczej, postanowienia dotyczące Członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych należy odnosić także do jej Przewodniczącego.
9. **Członek Zespołu Interdyscyplinarnego** – każda osoba wchodząca w skład Zespołu Interdyscyplinarnego niezależnie od tego czy jest pracownikiem Administratora czy też nie. Jeżeli Polityka nie stanowi inaczej, postanowienia dotyczące Członków Zespołu Interdyscyplinarnego należy odnosić także do jego Przewodniczącego.
10. **Członek Grupy Roboczej** – każda osoba wchodząca w skład Grupy Roboczej, niezależnie od tego czy jest pracownikiem Administratora czy też nie.
11. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
12. **Dane genetyczne** – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
13. **Dane biometryczne** – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
14. **Dane dotyczące zdrowia** – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
15. **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
16. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Świlcza;
17. **Komórka organizacyjna** – zgodnie ze znaczeniem przyjętym w Regulaminie Organizacyjnym;
18. **Kierownik** – zgodnie ze znaczeniem przyjętym w Regulaminie Organizacyjnym. Ilekroć w Polityce mowa jest o Kierowniku należy przez to rozumieć także jego zastępcę;
19. **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
20. **Powierzenie przetwarzania danych** – zlecenie wykonania czynności przetwarzania danych podmiotowi przetwarzającemu w drodze odrębnej umowy zawartej na piśmie lub stosownego pisemnego zapisu do umowy wyłącznie w zakresie i celu w nich przewidzianym;
21. **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
22. **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
23. **Rozporządzenie/RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1);

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	6 z 46
		Wydanie	1
		Data wydania	2020-09-01

24. **Zarządzanie ryzykiem** – skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń;
25. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
26. **Zgoda** – osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

ROZDZIAŁ III. ZAKRESY ODPOWIEDZIALNOŚCI ZA PRZETWARZANIE I OCHRONĘ DANYCH OSOBOWYCH

1. Postanowienia ogólne

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami, Rozporządzenia oraz Polityki Bezpieczeństwa Danych Osobowych odpowiadają:

- 1.1. Administrator Danych Osobowych lub osoba działająca w jego imieniu (ADO);
- 1.2. Inspektor Ochrony Danych (IOD);
- 1.3. Informatyk;
- 1.4. Każdy pracownik Administratora;
- 1.5. Członkowie Gminnej Komisji Rozwiązywania Problemów Alkoholowych.

2. Administrator Danych Osobowych


- 2.1. Administratorem Danych Osobowych jest Urząd w imieniu, którego kompetencje Administratora wypełnia Wójt Gminy Świlcza.
- 2.2. W imieniu ADO obowiązki określone w Rozporządzeniu pełni Wójt Gminy Świlcza – w przedmiocie podejmowania samodzielnych decyzji o celach i sposobach przetwarzania danych osobowych.

Do obowiązków Administratora należy:

- Ustanowienie i bieżąca aktualizacja odpowiednio do celów i zakresu przetwarzanych danych osobowych – polityki bezpieczeństwa i procedur zarządzania tym bezpieczeństwem.
- Nadzorowanie wdrożenia i stosowania środków przewidzianych w ustanowionej Polityce Bezpieczeństwa Danych Osobowych.
- Zapewnienie odpowiednich relacji z podmiotem, któremu powierzono przetwarzanie danych lub z osobą, której dane dotyczą.
- Zapewnienie właściwego i niezwłocznego włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych.

3. Inspektor Ochrony Danych (IOD)


- 3.1. IOD po przeprowadzeniu oceny (przeprowadzonej na podstawie aktu wydanego przez Grupę Roboczą art. 29: „Wytyczne dotyczące Inspektorów Ochrony Danych” z dnia 13 grudnia 2016 r., WP 243, rev. 01) został wyznaczony przez ADO na podstawie art. 37 ust. 1 lit. c Rozporządzenia i podlega bezpośrednio Administratorowi.
- 3.2. IOD realizuje następujące zadania przewidziane przez Rozporządzenie:
 - 3.2.1. informuje ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów o ochronie danych, a także doradza im w tej sprawie;
 - 3.2.2. monitoruje przestrzeganie Rozporządzenia, innych przepisów o ochronie danych oraz niniejszej Polityki Bezpieczeństwa Danych Osobowych,
 - 3.2.3. prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
 - 3.2.4. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 Rozporządzenia;
 - 3.2.5. współpracuje z organem nadzorczym;
 - 3.2.6. pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia,

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	7 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 3.2.7. w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach;
- 3.2.8. oraz inne zadania i obowiązki wyznaczone przez ADO, w warunkach w których te zadania i obowiązki nie powodują konfliktu interesów.
- 3.3. IOD jest osobą, wyznaczoną na podstawie posiadanych kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 Rozporządzenia.
- 3.4. IOD w zakresie swych czynności dotyczących ochrony danych osobowych posiada wyznaczony zakres czynności oraz stosowne uprawnienia udzielone przez Administratora do wydawania poleceń wszystkim użytkownikom systemów informatycznych oraz pracownikom przetwarzającym dane osobowe w systemach tradycyjnych, obejmujące wymagania wynikające z przepisów prawa oraz z zatwierdzonych przez ADO dokumentów systemu ochrony danych osobowych, tj. Polityki Bezpieczeństwa Danych Osobowych.
- 3.5. ADO zobowiązany jest zgłosić IOD do rejestracji lub wykreślić z rejestru prowadzonego przez organ nadzorczy, tj. Prezesa Urzędu Ochrony Danych Osobowych.
- 3.6. ADO korzystając z uprawnienia z art. 38 ust. 6 Rozporządzenia określa inne zadania i obowiązki IOD, do których w szczególności należą:
 - 3.6.1. Nadzór nad treścią Polityki Bezpieczeństwa Danych Osobowych oraz innych dokumentów związanych z ochroną danych osobowych stosowanych przez Administratora oraz ich aktualizacji.
 - 3.6.2. Prowadzenie i bieżące aktualizowanie Rejestru Czynności Przetwarzania (w oparciu o informacje własne lub przekazane przez pozostałych pracowników Administratora).
 - 3.6.3. Udział w kontrolach prowadzonych przez Organ Nadzorczy.
 - 3.6.4. Informowanie Administratora o prowadzonej przez Organ Nadzorczy kontroli i jej wynikach.
 - 3.6.5. Przedstawianie Administratorowi uwag i zastrzeżeń dotyczących przeprowadzonych przez organ kontroli oraz przedkładanie opinii w sprawie zatwierdzenia protokołu kontroli.
 - 3.6.6. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa danych osobowych;
 - 3.6.7. Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które prowadzą do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.
 - 3.6.8. Monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.
 - 3.6.9. Nadzór nad działaniami Informatyka w zakresie realizowanych obowiązków dotyczących ochrony danych osobowych.
 - 3.6.10. Nadzorowanie i realizacja procesu nadawania upoważnień pracownikom Administratora do przetwarzania danych osobowych.
 - 3.6.11. Nadzorowanie i organizacja realizacji obowiązku informacyjnego.
 - 3.6.12. Nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe.
 - 3.6.13. Opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych.
 - 3.6.14. Opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych podmiotom przetwarzającym.
 - 3.6.15. Wydawanie pisemnych zaleceń wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z Rozporządzeniem oraz Polityką Bezpieczeństwa Danych Osobowych.
 - 3.6.16. Opracowywanie planu kontroli lub audytów w zakresie ochrony danych osobowych przetwarzanych przez Administratora.

4. Informatyk

- 4.1. Podlega bezpośrednio IOD w zakresie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych. Jest odpowiedzialny za bieżące funkcjonowanie systemów i sieci teleinformatycznych, za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci, oraz za ochronę przetwarzanych w nich danych osobowych. Odpowiada za zadania wynikające z regulaminu organizacyjnego, tj.:
 - 4.1.1. koordynowanie prac związanych z komputeryzacją jednostek organizacyjnych Administratora,
 - 4.1.2. analiza stanu informatycznego jednostek organizacyjnych Administratora oraz opracowywanie raportów o stanie informatyki,

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	8 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 4.1.3. przygotowywanie wniosków oraz opiniowanie propozycji zakupu sprzętu i oprogramowania,
- 4.1.4. wdrażanie, rozpowszechnianie i administrowanie systemów i programów komputerowych,
- 4.1.5. administrowanie siecią komputerową,
- 4.1.6. archiwizacja danych komputerowych,
- 4.1.7. przygotowanie i aktualizacja strony internetowej Administratora,
- 4.1.8. wprowadzanie informacji i obsługa biuletynu informacji publicznej.

4.2. Ponadto Informatyk odpowiada za:


- 4.2.1. Opracowywanie projektów szczególnych wymagań bezpieczeństwa dla poszczególnych systemów i sieci z uwzględnieniem kluczowych urządzeń teleinformatycznych oraz przedstawianie propozycji ich uaktualnienia.
- 4.2.2. Wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemów i sieci teleinformatycznej.
- 4.2.3. Wdrażanie procedur ochrony antywirusowej oraz prowadzi profilaktykę antywirusową.
- 4.2.4. Opracowanie planów awaryjnych i planu napraw systemów i sieci teleinformatycznej.
- 4.2.5. Informowanie IOD (oraz ADO w przypadkach szczególnie istotnych dla bezpieczeństwa przetwarzanych danych) o stwierdzonych: incydentach bezpieczeństwa w zakresie funkcjonowania systemów i sieci teleinformatycznych, wykrytych podatnościach i zagrożeniach dla bezpieczeństwa informacji, bieżące prowadzenie ich ewidencji.
- 4.2.6. Proponowanie zmian mających na celu poprawę bezpieczeństwa systemów i sieci teleinformatycznej.
- 4.2.7. Systematyczne wykonywanie kopii bezpieczeństwa i kopii archiwalnych baz danych i zbiorów danych osobowych zgodnie z ustalonym planem.
- 4.2.8. W przypadku współpracy z zewnętrzną firmą informatyczną organizuje i nadzoruje pracę przedstawicieli tych firm, dba o przestrzeganie wymaganych zasad bezpieczeństwa.
- 4.2.9. Dbą o bezpieczeństwo oraz prawidłowe funkcjonowanie systemów informatycznych.
- 4.2.10. Utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu komputerowego uprawnionych do przetwarzania danych osobowych.
- 4.2.11. Prowadzi nadzór sprzętu oraz oprogramowania pod kątem kontroli nieuprawnionych zmian ich konfiguracji.
- 4.2.12. Dokonuje analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz, w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmuje odpowiednie kroki zaradcze zapewnienie strategii, uregulowań, instrukcji i procedur bezpieczeństwa.
- 4.2.13. Zabezpiecza niszczenie nośników zgodnie z obowiązującymi procedurami.
- 4.2.14. Doskonalą się z zakresu wiedzy o bezpieczeństwie systemów informatycznych.

5. Pracownicy Administratora

- 5.1. Każdy pracownik zobowiązany jest do ochrony danych osobowych w sposób zgodny z przepisami Rozporządzenia oraz Polityki Bezpieczeństwa Danych Osobowych.
- 5.2. Dostęp do określonego zbioru danych osobowych pracownik uzyskuje na podstawie pisemnego upoważnienia.
- 5.3. Pracownicy zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
- 5.4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy, stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.

6. Członkowie Gminnej Komisji Rozwiązywania Problemów Alkoholowych

- 6.1. Każdy członek Gminnej Komisji Rozwiązywania Problemów Alkoholowych, zobowiązany jest do ochrony danych osobowych w sposób zgodny z przepisami Rozporządzenia oraz Polityki Bezpieczeństwa Danych Osobowych.
- 6.2. Dostęp do określonego zbioru danych osobowych członkowie Gminnej Komisji Rozwiązywania Problemów Alkoholowych uzyskują na podstawie pisemnego upoważnienia.


	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	9 z 46
		Wydanie	1
		Data wydania	2020-09-01

6.3. Członkowie Gminnej Komisji Rozwiązywania Problemów Alkoholowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po zaprzestaniu sprawowania funkcji członka Gminnej Komisji Rozwiązywania Problemów Alkoholowych.

6.4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy może stanowić przesłankę odpowiedzialności karnej z art. 107 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

ROZDZIAŁ IV. UWZGLĘDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA (PRIVACY BY DESIGN) – TWORZENIE NOWYCH ZBIORÓW DANYCH


1. Zasady dotyczące zbierania i przetwarzania danych osobowych określone w tym rozdziale obowiązują dla sytuacji tworzenia nowych zbiorów danych osobowych lub nowych czynności przetwarzania w ramach zbioru.
2. Uprawnienie do podejmowania decyzji w sprawie tworzenia nowych zbiorów danych osobowych lub nowych czynności przetwarzania w ramach zbioru przysługuje wyłącznie Administratorowi.
3. Administrator może upoważnić pracowników do wydawania decyzji w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach zbioru.
 - 3.1. Każda decyzja o utworzeniu nowego procesu przetwarzania danych osobowych oraz doborze odpowiednich środków technicznych i organizacyjnych (wprowadzanych w celu skutecznej realizacji zasad ochrony danych, spełnienia wymogów RODO oraz ochrony praw osób, których dane dotyczą) poprzedzona jest procesem zarządzania ryzykiem, w ramach którego uwzględnia się:
 - 3.1.1. stan wiedzy technicznej,
 - 3.1.2. koszt wdrożenia,
 - 3.1.3. charakter, zakres, kontekst i cele przetwarzania danych,
 - 3.1.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
4. Pracownicy wnioskują na piśmie do Administratora o podjęcie decyzji w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach istniejącego zbioru. Wzór wniosku stanowi załącznik numer 1 do Polityki.
 - 4.1. Wniosek wymaga uzyskania uprzedniej pisemnej opinii IOD dotyczącej możliwości zbierania i utworzenia zbioru danych osobowych.
 - 4.2. IOD w szczególności rozstrzyga o formie i trybie wykonania obowiązku informacyjnego oraz o kwestii konieczności przeprowadzenia oceny skutków dla ochrony danych
 - 4.3. Opinia wydawana jest możliwie jak najszybciej, jednak nie dłużej niż w terminie 14 dni od daty otrzymania zapytania wraz z informacjami, określonymi w pkt. 5 niniejszego Rozdziału.
5. Osoby wnioskujące do Administratora w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach zbioru, w terminie 30 dni przed rozpoczęciem procesu zbierania danych osobowych i utworzeniu nowego zbioru zgłaszają swój zamiar IOD, podając jednocześnie informacje dotyczące:
 - 5.1. Nazwy zbioru oraz/lub nazwy czynności przetwarzania.
 - 5.2. Formy prowadzenia zbioru (papierowa czy elektroniczna).
 - 5.3. Istniejących w momencie składania wniosku regulacji wewnętrznych, które będą odnosić się do tworzonego zbioru;
 - 5.4. Podstawy prawnej zbierania danych lub pozostałych dopuszczeń określonych w art. 6 Rozporządzenia.
 - 5.5. Zakresu zbieranych danych (z zaznaczeniem czy przetwarzane będą szczególne kategorie danych lub dane biometryczne lub dane genetyczne).
 - 5.6. Celu zbierania danych.
 - 5.7. Podmiotu zbierającego dane.
 - 5.8. Źródła pochodzenia danych (od osoby lub z innych źródeł).
 - 5.9. Zamiaru udostępniania lub powierzania przetwarzania danych na zewnątrz z oznaczeniem podmiotów przetwarzających lub odbiorców danych.
 - 5.10. Wykazu stosowanych środków i mechanizmów zabezpieczeń.
 - 5.11. Infrastruktury systemu informatycznego służącego do przetwarzania danych osobowych.
 - 5.12. Obszaru przetwarzania danych osobowych.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	10 z 46
		Wydanie	1
		Data wydania	2020-09-01


- 5.13. Przewidywanego terminu usunięcia danych.
- 5.14. Ewentualnego przekazania danych osobowych do odbiorców z państw trzecich (z udokumentowaniem odpowiednich zabezpieczeń).
6. Osoby podejmujące decyzję o utworzeniu zbioru danych osobowych zobowiązane są do uwzględnienia opinii IOD i wynikających z niej wskazań i zaleceń w opiniowanych przez niego kwestiach.
7. W momencie utworzenia nowego zbioru danych osobowych lub czynności przetwarzania w ramach zbioru informacji na ten temat IOD odnotowuje w Rejestrze Czynności Przetwarzania, który stanowi załącznik numer 2 do Polityki.

ROZDZIAŁ V. PRAWA I WOLNOŚCI OSÓB, KTÓRYCH DANE DOTYCZĄ


1. Osobom fizycznym, których dane przetwarza Administrator, przysługują uprawnienia do:
 - 1.1. uzyskania informacji na temat przetwarzania jej danych osobowych w momencie ich pozyskania (bezpośrednio od osoby jak i z innych źródeł),
 - 1.2. dostępu do danych, które jej dotyczą,
 - 1.3. sprostowania danych, które jej dotyczą,
 - 1.4. usunięcia danych, które jej dotyczą (tzw. prawo do bycia zapomnianym),
 - 1.5. ograniczenia przetwarzania,
 - 1.6. uzyskania informacji o usunięciu danych lub ich sprostowaniu,
 - 1.7. przenoszenia danych,
 - 1.8. sprzeciwu względem dalszego przetwarzania danych,
 - 1.9. nie podlegania decyzji Administratora, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, a która decyzja wywołuje wobec osoby skutki prawne lub w podobny sposób istotnie wpływa na osobę.
2. Przed zrealizowaniem żądania osoby uprawnionej:
 - 2.1. Jeżeli osobą przyjmującą wniosek lub żądanie osoby, której dane dotyczą, jest Administrator, przypisuje on dany wniosek lub żądanie do IOD, który po rozpoznaniu przekazuje informację zwrotną o dalszym sposobie postępowania.
 - 2.2. Jeżeli wniosek lub żądanie osoby, której dane dotyczą trafia bezpośrednio do pracownika, ten niezwłocznie przekazuje informację o wpływie wniosku lub żądania do IOD. Brak przekazania wniosku lub żądania osoby, której dane dotyczą jest podstawą poniesienia przez pracownika odpowiedzialności dyscyplinarnej.
 - 2.3. Pracownicy obsługujący wniosek lub żądanie podejmują działania zmierzające do potwierdzenia tożsamości osoby składającej żądanie. Zadanie to wymaga udokumentowania.
 - 2.4. Uwierzytelnienie osoby, której dane dotyczą polega na uzyskaniu: imienia i nazwiska oraz okoliczności związanej ze sprawą wnioskującego. Środkiem uwierzytelnienia bez względu na kategorię osób może być adres e-mail zwyczajowo wykorzystywany do kontaktów z osobą, której dane dotyczą.
 - 2.5. Jeżeli pracownik w dalszym ciągu ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie w przedmiocie realizacji uprawnień, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
3. Ogólne zasady informowania i komunikacji z osobami, których dane dotyczą:
 - 3.1. Administrator o realizacji uprawnień przysługujących osobie, której dane są przetwarzane każdorazowo informuje na piśmie (w formie tradycyjnej lub elektronicznej);
 - 3.2. Administrator w miarę możliwości ułatwia osobie, której dane dotyczą, wykonywanie przysługujących jej praw;
 - 3.3. Administrator odmawia osobie wykonania praw jej przysługujących jedynie w sytuacji, w której nie jest w stanie zidentyfikować osoby, której dane dotyczą;
 - 3.4. bez zbędnej zwłoki lub w terminie miesiąca od otrzymania żądania Administrator informuje osobę o działaniach podjętych w związku z otrzymanym żądaniem;
 - 3.5. Administrator ma możliwość przedłużenia terminu o kolejne dwa miesiące w przypadku żądania o skomplikowanym charakterze lub dużej liczby żądań – co wymaga poinformowania w ramach odrębnego pisma;

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	11 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 3.6. jeżeli Administrator nie może podjąć działań w związku z otrzymanym żądaniem osoby, najpóźniej w terminie 1 miesiąca od otrzymania żądania, informuje o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz o możliwości skorzystania ze środków ochrony prawnej przed sądem;
- 3.7. realizacja uprawnień przysługujących osobie, której dane dotyczą jest wolna od opłat, chyba że żądania osoby są ewidentnie nieuzasadnione lub nadmierne (ze względu na ustawiczny charakter). W takim wypadku Administrator może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku z żądaniem. Na Administratorze spoczywa obowiązek wykazania, że żądanie osoby miało ewidentnie nieuzasadniony lub nadmierny charakter.
4. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą:
 - 4.1. pracownicy poszczególnych komórek organizacyjnych w momencie w którym dochodzi do pierwszego utrwalenia informacji o osobie, której dane dotyczą, dołączają do treści uzupełnianych przez tę osobę formularzy tzw. klauzule informacyjne;
 - 4.2. w przypadku korespondencyjnej obsługi spraw osoby, której dane dotyczą, udostępnienie klauzul informacyjnych następuje w pierwszym piśmie stanowiącym odpowiedź na złożony wniosek;
 - 4.3. klauzule informacyjne są opracowywane przez pracowników zgodnie z załącznikiem numer 3 do Polityki: „Klauzula informacyjna – zbieranie danych od osoby”;
 - 4.4. informacje potrzebne do zasilenia klauzuli informacyjnej odpowiednimi danymi pracownicy pobierają z Rejestru Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki;
 - 4.5. Administrator dodatkowo realizuje ogólną politykę informacyjną przez swoją stronę internetową oraz Biuletyn Informacji Publicznej zgodnie z załącznikiem numer 6 do Polityki: „Ogólna polityka Informacyjna”.
5. Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą:
 - 5.1. w sytuacji kiedy pracownicy poszczególnych komórek organizacyjnych pozyskują informacje dotyczące osoby z innych źródeł, są zobowiązani do przekazania tej osobie w nieprzekraczalnym terminie do 30 dni tzw. klauzulę informacyjną,
 - 5.2. klauzula informacyjna jest opracowywana przez pracowników zgodnie z załącznikiem numer 4 do Polityki: „Klauzula informacyjna – zbieranie danych z innych źródeł”,
 - 5.3. informacje potrzebne do zasilenia klauzuli informacyjnej odpowiednimi danymi pracownicy pobierają z Rejestru Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki.
6. Prawo dostępu do danych, przysługujące osobie której dane dotyczą:
 - 6.1. Administrator umożliwia osobom, których dane dotyczą uzyskanie dostępu do ich danych,
 - 6.2. Administrator na żądanie osoby udziela potwierdzenia/zaprzecza, czy przetwarzane są dane osoby składającej żądanie,
 - 6.3. Administrator na żądanie osoby udziela informacji o: celu przetwarzania, kategoriach danych osobowych, odbiorcach lub kategoriach odbiorców danych, planowany okres przechowywania danych osobowych (oraz o ile to możliwe: kryteria ustalenia tego okresu), prawie wniesienia skargi do organu nadzorczego, źródle danych, zautomatyzowanym podejmowaniu decyzji/profilowaniu, stosowanych zabezpieczeniach w przypadku przekazywania danych osobowych do państwa trzeciego,
 - 6.4. Administrator na żądanie osoby dostarcza kopię danych osobowych, które podlegały przetwarzaniu. Udostępnienie pierwszej kopii danych jest wolne od opłat, natomiast za każde kolejne Administrator może pobrać opłatę administracyjną,
 - 6.5. Prawo uzyskania kopii danych nie może wpływać niekorzystnie na prawa i wolności innych osób. Wymaga się aby kopia danych przekazana do udostępnienia była wolna od danych osób trzecich (np. poprzez animizację lub zaciemnienie kopii).
7. Prawo do sprostowania danych:
 - 7.1. Administrator na żądanie osoby, której dane dotyczą umożliwia niezwłoczne sprostowanie danych, które nie są prawidłowe,
 - 7.2. Administrator na żądanie osoby, której dane dotyczą umożliwia uzupełnienie niekompletnych danych osobowych,
 - 7.3. IOD informuje każdego odbiorcę danych, któremu uprzednio przekazano dane objęte sprostowaniem lub uzupełnieniem. IOD na żądanie osoby informuje o tych odbiorcach.
8. Prawo do usunięcia danych („prawo do bycia zapomnianym”):

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	12 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 8.1. Administrator umożliwia na żądanie osoby, której dane dotyczą usunięcie jej danych bez zbędnej zwłoki w następujących przypadkach:
 - 8.1.1. ustalił cel dla którego przetwarzanie danych było niezbędne,
 - 8.1.2. osoba wycofała zgodę na której opiera się przetwarzanie danych przez Administratora i brak jest innej podstawy prawnej przetwarzania,
 - 8.1.3. osoba, której dane dotyczą wniosła sprzeciw co do dalszego przetwarzania a Administrator nie wykaze nadrzędnych prawnie uzasadnionych podstaw przetwarzania,
 - 8.1.4. dane osobowe były przetwarzane niezgodnie z prawem,
 - 8.1.5. dane osobowe muszą zostać usunięte ze względu na przewidziany w unijnym lub krajowym porządku prawnym obowiązek,
 - 8.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (tj. świadczenie usług drogą elektroniczną).
- 8.2. Administrator odmówi spełnienia żądania usunięcia danych w zakresie w jakim przetwarzanie jest niezbędne:
 - 8.2.1. do korzystania z prawa do wolności wypowiedzi i informacji,
 - 8.2.2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator,
 - 8.2.3. do ustalenia, dochodzenia lub obrony roszczeń.
- 8.3. IOD informuje każdego odbiorcę danych, któremu uprzednio przekazano dane o wniesionym żądaniu usunięcia danych. IOD na żądanie osoby informuje o tych odbiorcach.
9. Prawo do ograniczenia przetwarzania:
 - 9.1. Administrator umożliwia na żądanie osoby, której dane dotyczą ogranicza przetwarzanie jej danych w następujących przypadkach:
 - 9.1.1. zakwestionowano prawidłowość danych osoby (ograniczenie przetwarzania trwa przez czas pozwalający sprawdzić prawidłowość danych),
 - 9.1.2. przetwarzanie danych jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych żądając w zamian ograniczenia ich wykorzystywania,
 - 9.1.3. Administrator nie potrzebuje już danych osobowych do przyjętych celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,
 - 9.1.4. osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania (ograniczenie przetwarzania trwa do czasu wyjaśnienia czy prawnie uzasadnione podstawy występujące po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby).
 - 9.2. Uznanie przez Administratora żądania osoby, której dane dotyczą w przedmiocie ograniczenia przetwarzania powoduje, że przez czas trwania ograniczenia jedyną dopuszczalną formą przetwarzania danych przez Administratora jest ich przechowywanie. Dane przeznaczone do ograniczonego przetwarzania zostają stosownie oznakowane klauzulą „ograniczone przetwarzanie”.
 - 9.3. Dane osobowe względem, których przetwarzanie zostało ograniczone wyłącznie w przypadku:
 - 9.3.1. zgody osoby, której dane dotyczą;
 - 9.3.2. ustalenia, dochodzenia lub obrony roszczeń;
 - 9.3.3. ochrony praw innej osoby fizycznej lub prawnej (z uwagi na ważne względu interesu publicznego UE lub państwa członkowskiego),
 mogą być przetwarzane w zakresie szerszym niż wyłącznie przechowywanie.
 - 9.4. Zanim Administrator podejmie decyzję o uchyleniu ograniczenia przetwarzania, informuje się o tym osobę, która zażądała ograniczenia.
 - 9.5. Administrator informuje każdego odbiorcę danych, któremu uprzednio przekazano dane o wniesionym żądaniu ograniczenia przetwarzania danych. Administrator na żądanie osoby informuje ją o tych odbiorcach.
10. Prawo do przenoszenia danych:
 - 10.1. IOD przekazuje na żądanie osoby zestaw jej danych osobowych (w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, np. pliki txt, xml, doc), który uprzednio dostarczyła. Administrator nie utrudnia/nie uniemożliwia przesyłania przekazanego zestawu danych osobie, której dane dotyczą innemu administratorowi.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	13 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 10.2. Administrator na żądanie osoby, której dane dotyczą, może przekazać zestaw danych bezpośrednio innemu administratorowi – o ile jest to technicznie możliwe.
- 10.3. Realizacja prawa do przenoszenia danych jest możliwa jeżeli: przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; przetwarzanie odbywa się w sposób zautomatyzowany.
- 10.4. Skorzystanie przez osobę z prawa do przenoszenia danych nie niweluje możliwości skorzystania z prawa do usunięcia danych (prawo do bycia zapomnianym).
- 10.5. Realizacja prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych osób – tym samym jest to przesłanka do odmowy realizacji prawa do przenoszenia danych.
11. Prawo do sprzeciwu:
 - 11.1. Umożliwia się osobom, których dane dotyczą, wniesienie sprzeciwu co do dalszego przetwarzania jej danych oraz respektuje się to uprawnienie w sytuacji kiedy podstawą prawną przetwarzania danych jest prawnie uzasadniony interes realizowany przez ADO.
 - 11.2. W momencie wniesienia zasadnego sprzeciwu nie wolno już przetwarzać danych osobowych objętych sprzeciwem. Wyjątkiem od tej sytuacji jest wykazanie przez ADO ważnych, prawnie uzasadnionych podstaw do przetwarzania – nadrzędnych względem interesów, praw i wolności osoby, której dane dotyczą; lub wykazanie podstaw do ustalenia, dochodzenia lub obrony roszczeń.
12. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach/profilowanie: Administrator nie podejmuje decyzji w indywidualnych przypadkach w sposób zautomatyzowany – dotyczy to również profilowania.

ROZDZIAŁ VI. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH


1. Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Administrator Danych Osobowych musi wykazać, że przetwarzane przez niego dane są:
 - 1.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
 - 1.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - 1.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane
 - 1.4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
 - 1.5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
 - 1.6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

ROZDZIAŁ VII. DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Zasada domyślnej ochrony danych jest realizowana poprzez:
 - 1.1. wdrażanie odpowiednich środków technicznych i organizacyjnych w ten sposób aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania – co zostało zapewnione w ramach Rejestru Czynności Przetwarzania. Niezbędność danych odnosi się do ilości danych, zakresu, okresu przechowywania oraz ich dostępności.
 - 1.2. wdrażanie odpowiednich środków technicznych i organizacyjnych zapewniających aby dane osobowe nie były udostępniane nieokreślonej liczbie osób fizycznych.

ROZDZIAŁ VIII. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Zidentyfikowane zbiory zawierające dane osobowe w wersji papierowej i elektronicznej są przetwarzane i przechowywane w budynkach należących do Administratora, mieszczących się w poniższych lokalizacjach:

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	14 z 46
		Wydanie	1
		Data wydania	2020-09-01

1. Siedziba Administratora: 36-072 Świltza 168.


Szczegółowy wykaz komórek organizacyjnych i pomieszczeń poszczególnych obiektów tworzących obszar dla zbiorów, w których są przetwarzane dane osobowe, zawiera załącznik 5 do niniejszej Polityki Bezpieczeństwa: „Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe”.

ROZDZIAŁ IX. REJESTR CZYNNOŚCI PRZETWARZANIA


1. ADO, spełniając kryterium, o którym mowa w art. 30 ust. 5 Rozporządzenia, prowadzi Rejestr Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki.
2. Za bieżące utrzymanie Rejestru Czynności Przetwarzania odpowiada Inspektor Ochrony Danych.
3. Obowiązek informowania IOD o wszelkich zmianach dotyczących zbiorów lub czynności przetwarzania spoczywa na:
 - 3.1. Informatyku;
 - 3.2. Administratorze;
 - 3.3. Pracownikach Administratora;
 w zakresie właściwych dla nich zbiorów danych lub czynności przetwarzania.
4. Podmioty, o których mowa w pkt. 3 niniejszego rozdziału są zobowiązane raz do roku przeprowadzić badanie aktualności posiadanych informacji z treścią bieżącego Rejestru Czynności Przetwarzania.
5. Zaniechanie lub uchybienie obowiązkowi, o których mowa w pkt. 3 i 4 może stanowić naruszenie obowiązków pracowniczych i być podstawą odpowiedzialności dyscyplinarnej.
6. W rejestrze zamieszcza się wszystkie następujące informacje:
 - 6.1. imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
 - 6.2. cele przetwarzania;
 - 6.3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
 - 6.4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
 - 6.5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, oraz informację o dokumentacji odpowiednich zabezpieczeń;
 - 6.6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
 - 6.7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

ROZDZIAŁ X. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. W systemie ochrony danych osobowych wyróżnia się następujące cechy informacji:
 - 1.1. Poufność – zapewnia, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
 - 1.2. Dostępność – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w złożonym czasie przez kogoś lub coś, kto lub co ma do tego prawo;
 - 1.3. Integralność – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
 - 1.4. Rozliczalność – właściwość zapewniająca, że działanie podmiotu (np. Użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.
2. Zastosowane zabezpieczenia (techniczne i organizacyjne) powinny być adekwatne do stwierdzonych zagrożeń mających wpływ na poziom ryzyka dla poszczególnych systemów, rodzajów zbiorów, kategorii i zakresu przetwarzanych danych osobowych.
3. W celu zapewnienia przetwarzanym danym osobowym atrybutów poufności stosuje się następujące zabezpieczenia:
 - 3.1. Po zakończeniu pracy zamykanie pomieszczeń biurowych na klucz;

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	15 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 3.2. Zbiory danych osobowych w formie papierowej są przechowywane, co najmniej w meblach biurowych zamykanych na klucz;
- 3.3. Obowiązuje polityka zarządzania kluczami;
- 3.4. Obowiązuje zakaz udzielania informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego, za wyjątkiem spraw związanych z wykonywaniem obowiązków służbowych;
- 3.5. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe w sposób uniemożliwiający odczytanie zawartej w nich treści tylko z wykorzystaniem niszczarek do papieru i w uzasadnionych przypadkach płyt CD – klasy, co najmniej P3;
- 3.6. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych. W przypadku pomieszczeń technicznych wchodzących w skład obszaru przetwarzania, w których rozlokowane są elementy systemu informatycznego, przebywanie osób możliwe jest wyłącznie w obecności Informatyka;
- 3.7. Obowiązuje polityka „czystego biurka” i „czystego ekranu”;
- 3.8. W przypadku zawieszenia pracy z systemem informatycznym w związku z tymczasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest do: zablokowania dostępu do użytkowanego systemu komputerowego, w tym również do informacji prezentowanych na jego wyświetlaczu.
- 3.9. Zapewnione jest zdalne monitorowanie sieci z jednej centralnej lokalizacji za pomocą specjalistycznego systemu.
- 3.10. Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem ścian ogniowych;
4. W celu podniesienia poziomu bezpieczeństwa sieci lokalnej poprzez wykrywanie i blokowanie ataków w czasie rzeczywistym zastosowano urządzenie sieciowe – system zapobiegania przed włamaniami (ang. *Intrusion Prevention System – IPS*);
 - 4.1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika;
 - 4.2. Dostęp do systemu oraz wrażliwych funkcji poprzez zdublowane uwierzytelnianie użytkowników do systemu operacyjnego oraz identyfikatora i hasła do wykorzystywanej aplikacji (przy użyciu minimalnie 8 znakowego hasła alfanumerycznego);
 - 4.3. Wyznaczono Inspektora Ochrony Danych;
 - 4.4. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia;
 - 4.5. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez ADO;
 - 4.6. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy;
 - 4.7. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarkach;
 - 4.8. Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych przetwarzanych przez Administratora.
5. W celu zapewnienia przetwarzanym danym osobowym atrybutów **dostępności i integralności** stosuje się następujące zabezpieczenia:
 - 5.1. Wykonywanie kopii zapasowych danych i programów oraz bezpieczny sposób ich przechowywania;
 - 5.2. Systemy służące do przetwarzania danych osobowych posiadają architekturę klient-serwer, wobec czego wszystkie informacje przechowywane są na serwerze, przez co możliwe jest lepsze zabezpieczenie danych. Serwer decyduje, kto ma prawo do odczytywania, kopiowania i zmiany danych;
 - 5.3. Komputery przenośne i elektroniczne nośniki informacji użytkowane przez Administratora zawierające dane osobowe podczas transportu, przechowywania i użytkowania są zabezpieczone w sposób zapewniający poufność i integralność tych danych np. z wykorzystaniem środków ochronnych kryptograficznej. Odpowiedzialność za powierzony elektroniczny nośnik informacji ponosi bezpośrednio jego użytkownik.
 - 5.4. Stosowanie zasad wykonywania okresowych przeglądów systemu informatycznego;

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	16 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 5.5. Opracowano i wdrożono „Politykę bezpieczeństwa danych osobowych”;
- 5.6. Zapewnia się bezpieczeństwo nośników informacji zawierających dane osobowe w przypadku, gdy zachodzi konieczność naprawy sprzętu, w którym te nośniki są zamontowane (wymontowanie w przypadku naprawy poza siedzibą Administratora lub nadzór nad serwisem jego siedzibie ADO);
- 5.7. Zastosowano system ochrony ciągłości zasilania, zmniejszający ryzyko utraty danych znajdujących się aktualnie w pamięci operacyjnej serwerów, a nawet uszkodzenia urządzeń pamięci masowej.
6. W celu zapewnienia przetwarzanym danym osobowym atrybutów **rozliczalności** stosuje się następujące zabezpieczenia:
7. Zakaz używania nośników elektronicznych nie dopuszczonych do użytku przez Informatyka;
8. Stosowanie procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkownika systemu informatycznego;
9. Stosowane są zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych;
10. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do jego zasobów;
11. Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich;
12. Identyfikator użytkownika, który utracił upoważnienie do przetwarzania danych, nie jest przydzielany innej osobie.


ROZDZIAŁ XI. ZARZĄDZANIE DOSTĘPEM DO DANYCH OSOBOWYCH

1. Postanowienia ogólne

Na zasadach określonych w niniejszym rozdziale, polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych mogą wynikać z zakresu czynności, przyjętej polityki zastępstw, pełnomocnictwa (prokury), zarządzenia, zawartej umowy lub wniosku stanowiącego załącznik numer 7 do Polityki.

2. Nadawanie uprawnień do przetwarzania danych osobowych osobom zatrudnionym w Urzędzie Gminy Świlcza

- 2.1. W przypadku pracowników, za polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych poczytuje się zakres czynności. Zakres czynności wydaje się każdemu pracownikowi do zawartej umowy o pracę i przechowuje w aktach osobowych pracowników.
- 2.2. W przypadku pracowników oddelegowanych do zastępowania innego pracownika w czasie jego nieobecności, za polecenie przetwarzania danych osobowych poczytuje się przyjętą politykę zastępstw, zaś za upoważnienie do przetwarzania danych osobowych uznaje się zakres czynności pracownika zastępowanego.
- 2.3. Szczególnymi rodzajami polecenia przetwarzania danych osobowych oraz upoważnienia do przetwarzania danych osobowych są pełnomocnictwo i prokura. Uprawniają one pełnomocników oraz prokurentów do przetwarzania danych osobowych w zakresie niezbędnym do wykonania pełnomocnictwa (prokury).
- 2.4. Polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych mogą wynikać z zarządzenia. Dotyczy to w szczególności zarządzeń w sprawie powołania komisji lub zespołów do wykonywania określonych zadań oraz wyznaczenia poszczególnych osób do wykonywania zadań lub pełnienia funkcji. W takim przypadku, kopię zarządzenia przechowuje się wraz z dokumentacją dotyczącą przedmiotu zarządzenia.
- 2.5. W przypadku osób zatrudnionych na podstawie stosunku prawnego innego rodzaju, niż stosunek pracy, za polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych uznaje się zawartą umowę. Umowa powinna jasno określać zakres prac powierzonych do wykonania.
- 2.6. W pozostałych przypadkach, polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych nadaje Wójt na wniosek Sekretarza, na podstawie wniosku stanowiącego załącznik numer 7 do Polityki. Integralną częścią tych wniosków jest zobowiązanie do zachowania w tajemnicy treści danych osobowych, stanowiące załącznik numer 7a do Polityki.
- 2.7. Operacje przetwarzania, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie wykonywane są zgodnie z obowiązującymi przepisami prawa oraz przyznanym zakresem kompetencji. Zakres kompetencji wynika z upoważnienia do przetwarzania danych osobowych.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltcza	Strona	17 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 2.8. Administrator odbiera od każdej zatrudnionej osoby zobowiązanie do zachowania w tajemnicy treści danych osobowych. Zobowiązanie musi pozostawać w mocy zarówno w trakcie świadczenia stosunku pracy jak i po jego rozwiązaniu lub wygaśnięciu. Zobowiązanie może być elementem umowy lub osobnym dokumentem. Wzór zobowiązania stanowi załącznik numer 7a do Polityki.
- 3. Upoważnienia do przetwarzania danych osobowych wydawane członkom Gminnej Komisji Rozwiązywania Problemów Alkoholowych**
- 3.1. Przewodniczący Gminnej Komisji Rozwiązywania Problemów Alkoholowych odpowiada za dopuszczenie do przetwarzania danych osobowych członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych, poprzez złożenie stosownego wniosku do Administratora. Zatwierdzony przez Administratora wniosek o nadanie uprawnień do przetwarzania danych osobowych uznaje się za wydanie polecenia przetwarzania danych osobowych oraz nadanie upoważnienia do przetwarzania danych osobowych.
- 3.2. Upoważnienia do przetwarzania danych osobowych, przeznaczone dla członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych, wydane są w dwóch egzemplarzach, na podstawie załącznika nr 7 do niniejszej Polityki. Integralną częścią tych upoważnień jest oświadczenie, o którym mowa w art. 25a ust. 4 Ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi. Jedne egzemplarze przechowywane są przez Administratora zbiorczo, w wydzielonych do tego aktach, drugie zaś wydawane są poszczególnym członkom Komisji.
- 3.3. Upoważnienia wydawane dla członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych mają charakter indywidualny i abstrakcyjny. Każdy członek Komisji otrzymuje imienne upoważnienie obejmujące zakresem wszystkie sprawy toczące się w momencie wydania upoważnienia jak i wszelkie przyszłe sprawy objęte pracą Komisji w okresie zasiadania w niej osoby upoważnionej.
- 3.4. Upoważnienie do przetwarzania danych osobowych, wydawane członkom Gminnej Komisji Rozwiązywania Problemów Alkoholowych, obejmuje uprawnienie do przetwarzania danych osobowych w każdy możliwy sposób, w szczególności poprzez: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- 3.5. Upoważnienia do przetwarzania danych osobowych, wydawane członkom Gminnej Komisji Rozwiązywania Problemów Alkoholowych, zarówno aktualne jak i uchylone kolejnym upoważnieniem lub jego odwołaniem, przechowywane są zgodnie z przepisami Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
- 4. Oświadczenia składane przez członków Zespołu Interdyscyplinarnego oraz Grup Roboczych**
- 4.1. Urząd Gminy Świltcza przechowuje oświadczenia członków Zespołu Interdyscyplinarnego oraz Grup Roboczych, o których mowa w art. 9c ust. 3 Ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie.
- 4.2. Oświadczenia, składane przez członków Zespołu Interdyscyplinarnego oraz członków Grup Roboczych, przechowywane są zgodnie z przepisami Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.


5. Szczegółowe wzory wniosków o nadanie uprawnień do przetwarzania danych osobowych

Administrator może określić, w drodze zarządzenia, szczegółowe wzory wniosków stanowiących załącznik numer 7 do Polityki, wydawanych na potrzeby pełnienia określonych funkcji lub wykonania określonych zadań.

ROZDZIAŁ XII. UDOSTĘPNIANIE I POWIERZANIE DANYCH OSOBOWYCH

Udostępnianie danych osobowych poza struktury.

1. Udostępnienie danych osobowych, czyli przekazywanie i ujawnianie ich innym osobom lub podmiotom, jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):
 - 1.1. osoba, której dane dotyczą, wyrazi zgodę na udostępnienie danych osobowych (np. osoba chcąc pozyskać od ADO dane osobowe pracownika posiada udzielone przez niego

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	18 z 46
		Wydanie	1
		Data wydania	2020-09-01


upoważnienie/ppełnomocnictwo do uzyskania dostępu do danych – np. w kontekście weryfikacji zatrudnienia przez Banki),

- 1.2. udostępnienie danych jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (podmiot wnoszący o udostępnienie przedstawia podstawę prawną udostępnienia danych),
- 1.3. udostępnienie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- 1.4. udostępnienie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (konieczność wskazania ogólnej podstawy prawnej),
- 1.5. udostępnienie danych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez ADO albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (np. udostępnienie danych w celu umożliwienia wystąpienia z roszczeniem cywilnoprawnym, udostępnienie danych w ramach zawartej umowy).
2. Pracownik, do którego wpłynie zapytanie o udostępnienie danych osobowych (osobiście od osoby zainteresowanej, telefonicznie lub drogą elektroniczną), nie może samodzielnie podjąć decyzji o udostępnieniu danych osobowych.
3. Pracownik, który otrzyma zapytanie o udostępnienie danych osobowych powiadamia o tym fakcie IOD.
4. W celu zbadania wystąpienia przesłanek wymienionych w pkt. 2 i udokumentowania procesu udostępnienia danych osobowych, zainteresowana osoba lub podmiot zobowiązane są do wypełnienia wniosku o udostępnienie danych osobowych – stanowiącego załącznik 8 do niniejszej Polityki.
 - 4.1. Uzupełniony wniosek zostaje przekazany do IOD. Decyduje on o zgodzie lub braku zgody na udostępnienie danych osobowych.
 - 4.2. Pracownik, do którego wpłynął wniosek udostępnia dane osobowe w przypadku pozytywnej opinii wyrażonej przez IOD.
5. W sytuacji wystąpienia zgody na udostępnienie danych osobowych, IOD odnotowuje ten fakt w Ewidencji udostępnień danych osobowych, której wzór stanowi załącznik 9 do niniejszej Polityki.
6. Odnotowanie to powinno zawierać informację o: dacie udostępnienia, osobie która dokonała faktycznej czynności udostępnienia danych osobowych, osobie której dane zostały udostępnione, zakresie danych które zostały udostępnione, osobie/podmiocie któremu udostępniono dane osobowe oraz określeniu przesłanki udostępnienia danych osobowych.
7. W uzasadnionych przypadkach, zgodę na udostępnienie danych osobowych może udzielić ADO, jeśli osoby rozpatrujące wniosek o udostępnienie nie są w stanie wspólnie ustalić wystąpienia zasadności przesłanki legalizującej udostępnienie danych osobowych odbiorcy danych.

Powierzanie przetwarzania danych osobowych

W Urzędzie Gminy Świltza występują przypadki powierzania przetwarzania danych podmiotom zewnętrznym. W związku z tym zasady opisane w poniższych punktach wymagają stosowania zawartych w nich działań.


1. Powierzenie przetwarzania danych osobowych Podmiotom Przetwarzającym (podmiotom którym powierza się dane do przetwarzania) następuje w drodze umowy zawartej na piśmie. Zalecany wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 10 do niniejszej Polityki.
2. Za przygotowanie właściwej umowy powierzenia przetwarzania danych odpowiedzialny jest Administrator, działając we współpracy z osobą odpowiedzialną za obsługę prawną oraz IOD.
3. Przekazanie zbiorów Podmiotowi Przetwarzającemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO.
4. Podmiot Przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.
5. Podmiot Przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do stosowania się do zapisów umownych, mówiących o zabezpieczeniu danych osobowych, zawartych we wzorze umowy powierzenia przetwarzania danych osobowych, stanowiącej załącznik numer 10 do niniejszej Polityki.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	19 z 46
		Wydanie	1
		Data wydania	2020-09-01

6. Administrator, w momencie doboru podwykonawcy lub podmiotu, który w związku z zawieraną umową uzyska dostęp do danych osobowych przetwarzanych w placówce, przekazuje o tym fakcie informację do IOD, informując o zakresie przewidywanych do powierzenia danych oraz zbiorze/zbiorach z którego/których nastąpi powierzenie.
7. Dokonując wyboru podmiotu, z którym zawarta ma być umowa powierzenia przetwarzania danych osobowych, osoby zaangażowane w proces podpisania umowy zobowiązane są dokonać oceny tego podmiotu, aby gwarantował on wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi powszechnie obowiązującego prawa i chroniło prawa osób, których dane dotyczą.
8. W sytuacji, gdy powierzenie przetwarzania danych osobowych dotyczyć by miało danych przetwarzanych w formie elektronicznej, lub powierzenie związane byłoby z obsługą teleinformatyczną – Administrator konsultuje zasadność zawarcia umowy powierzenia z Informatykiem (w kontekście spełniania przez podmiot przetwarzający odpowiednich zabezpieczeń w zakresie ochrony danych osobowych w sferze teleinformatycznej).
9. Administrator przekazuje informację o fakcie, zawarcia stosownej umowy do IOD.
10. Wzór ewidencji podmiotów którym ADO powierza dane osobowe do przetwarzania, stanowi załącznik 12 do niniejszej Polityki. Za aktualizację powyższej listy odpowiedzialny jest IOD.

ROZDZIAŁ XIII. ZARZĄDZANIE RYZYKIEM DANYCH OSOBOWYCH


1. Zarządzanie ryzykiem danych osobowych realizowane na podstawie art. 24, 25, 28, 32 oraz 35 Rozporządzenia odbywa się cyklicznie w odniesieniu do źródeł ryzyka, tj.:
 - a. Zbiorów danych osobowych przetwarzanych w bieżącej działalności Administratora. Aktualny wykaz zbiorów danych osobowych jest zawarty w treści załącznika numer 2 Rejestr Czynności Przetwarzania do niniejszej Polityki;
 - b. Aktywów informacyjnych wykorzystywanych przy przetwarzaniu informacji, np. serwery fizyczne, serwery wirtualne, klastry, urządzenia sieciowe, stacje robocze, komputery przenośne, urządzenia peryferyjne, oprogramowanie, bazy danych, wzory dokumentów, informacje utrwalone w formie cyfrowej lub innej.
2. Proces zarządzania ryzykiem jest uruchamiany:
 - a) przez Inspektora Ochrony Danych raz do roku w pierwszym kwartale, w zakresie przez niego określonym (wybór niektórych lub grup lub wszystkich źródeł ryzyka);
 - b) przez
 - Informatyka;
 - Administratora;
 we właściwych im zakresach (dla właściwych im źródeł ryzyka) każdorazowo na skutek istotnych zmian stosowanych środków technicznych lub organizacyjnych, które mają na celu zapewnienie bezpieczeństwa informacji (tj. ustanowienie nowego zabezpieczenia lub rezygnacja ze stosowanego zabezpieczenia),
 - c) przez IOD, każdorazowo na skutek zidentyfikowanego naruszenia bezpieczeństwa danych osobowych lub podejrzenia jego wystąpienia, którego wartość wyniesie 2 lub więcej,
 - d) przez Kierownika komórki organizacyjnej, w której podjęto decyzję o przekazaniu danych osobowych/informacji do przetwarzania podmiotowi przetwarzającemu,
 - e) przez Inspektora Ochrony Danych, kiedy podjęto decyzję o utworzeniu nowego zbioru danych osobowych (w celu zagwarantowania realizacji zasady prywatności w fazie projektowania zgodnie z postanowieniami niniejszej Polityki).
3. Wszystkie rozpoczęte procesy zarządzania ryzykiem, o których mowa w pkt. 2 niniejszego rozdziału – poza rocznym procesem, o którym mowa w pkt. 2 lit. a – kończą się najpóźniej po upływie 2 tygodni od rozpoczęcia procesu.
4. Zarządzanie ryzykiem danych osobowych odbywa się w następującym cyklu:
 - a) identyfikacja źródeł ryzyka,
 - b) określenie oczekiwanego wyniku materializacji ryzyka,
 - c) identyfikacja zagrożeń, które doprowadzą do materializacji ryzyka,

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	20 z 46
		Wydanie	1
		Data wydania	2020-09-01

- d) określenie stosowanych obecnie działań zapobiegających,
 - e) ocena ryzyka (wpływ i prawdopodobieństwo),
 - f) szacowanie ryzyka,
 - g) proponowanie sugerowanych działań zaradczych,
 - h) określenie ewentualnych szans wynikających z materializacji ryzyka,
 - i) opracowanie planu postępowania z ryzykiem - dla ryzyk, których wartość przekracza próg akceptowalności,
 - j) ocena planu postępowania z ryzykiem przez Informatyka z uwzględnieniem obecnego stanu wiedzy technicznej,
 - k) ocena planu postępowania z ryzykiem przez Głównego Księgowego na okoliczność możliwości pokrycia planowanych rozwiązań zgodnie z bieżącym planem finansowym,
 - l) decyzja Administratora (akceptacja, modyfikacja lub odrzucenie) w sprawie przedstawionego planu postępowania z ryzykiem,
 - m) realizacja zatwierdzonych planów postępowania z ryzykiem przez wyznaczonych pracowników,
 - n) monitorowanie realizacji planu postępowania z ryzykiem,
 - o) prowadzenie zbiorczego rejestru ryzyk bezpieczeństwa informacji.
5. Narzędziem umożliwiającym dokumentowanie procesu identyfikacji ryzyka, zagrożeń, ich ocenę oraz przedstawienie sugestii zabezpieczeń jest załącznik numer 12: „Ankieta Identyfikacji Ryzyk”.
 6. Plan postępowania z ryzykiem, jego ocena, decyzja Administratora oraz monitorowanie realizacji planu dokumentowane są zgodnie z załącznikiem numer 13: „Plan Postępowania z Ryzykiem”. Informacje o realizacji poszczególnych etapów planów postępowania z ryzykiem są przekazywane do IOD.
 7. IOD prowadzi rejestr ryzyk bezpieczeństwa informacji zgodnie z załącznikiem numer 14: „Rejestr Ryzyk Bezpieczeństwa Informacji”.


ROZDZIAŁ XIV. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrola nad ochroną przetwarzanych danych osobowych organizowana jest przez ADO samodzielnie, a w jego imieniu czynności te przeprowadza IOD lub w uzasadnionych przypadkach, na polecenie ADO – audytor wewnętrzny.
2. Kontrole przetwarzania i stanu bezpieczeństwa przeprowadzane są raz do roku lub doraźnie.
3. Czynności kontrolne przeprowadzane są przez osobę, o której mowa w pkt. 1 niniejszego rozdziału, osobiście lub przez wyznaczonych, podległych jej pracowników.
4. Kontrolą, o której mowa w pkt. 1, mogą zostać objęte komórki organizacyjne Administratora, w których przetwarzane są w zbiorach dane osobowe.
5. W ramach utrzymania wysokiego poziomu bezpieczeństwa przetwarzanych danych osobowych mogą być prowadzone przez osoby funkcyjne (IOD/Informatyk) czynności kontrolne w określonych obszarach systemu bezpieczeństwa danych osobowych.
6. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i czynności przeprowadzonych w jej trakcie. We wnioskach protokołu dokonuje się całościowej oceny stanu ochrony danych przetwarzanych w kontrolowanej komórce organizacyjnej Administratora oraz wskazuje występujące w tym zakresie uchybienia wraz ze sposobami i terminem ich usunięcia.
7. Protokół sporządzany jest w dwóch egzemplarzach i podpisywany jest przez osoby wykonujące czynności kontrolne oraz obowiązkowo przez Kierownika kontrolowanej komórki organizacyjnej. Jeden egzemplarz protokołu pozostaje w kontrolowanej komórce organizacyjnej, drugi przechowywany jest u IOD.
8. Osobom wymienionym w pkt. 1 przysługuje prawo do wykonania czynności sprawdzających w zakresie weryfikacji usunięcia przez komórkę uchybień i wykonania innych zaleceń wskazanych w protokole kontrolnym. Z czynności tych spisywany jest protokół. W przypadku niewykonania zaleceń pokontrolnych informuje się pisemnie o tym fakcie Administratora wnioskując o podjęcie działań dyscyplinujących przewidzianych w Kodeksie Pracy.
9. IOD ma prawo do kontroli podmiotów, którym dokonano powierzenia przetwarzania danych w trybie określonym w niniejszym Rozdziale, o ile w umowie o powierzeniu przetwarzania istnieją stosowne postanowienia w tym zakresie.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	21 z 46
		Wydanie	1
		Data wydania	2020-09-01

ROZDZIAŁ XV. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH


1. Za naruszenie bezpieczeństwa danych osobowych uznaje się każde zdarzenie, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób. Zidentyfikowanie naruszenia, które dotyczy bezpieczeństwa danych osobowych, powoduje konieczność zastosowania przedstawionych niżej zasad.
2. Naruszenie praw i wolności osób fizycznych związane z przetwarzaniem danych osobowych to sytuacja, kiedy osoba, której dane dotyczą może doznać lub doznała uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, które m.in. polegają na:
 - 2.1. dyskryminacji,
 - 2.2. kradzieży tożsamości lub oszustwie dotyczącym tożsamości,
 - 2.3. naruszeniu dobrego imienia,
 - 2.4. naruszeniu poufności danych chronionych tajemnicą zawodową,
 - 2.5. nieuprawnionym odwróceniu pseudonimizacji,
 - 2.6. wszelkiej innej znacznej szkodzie gospodarczej lub społecznej.
3. Każda osoba, która poweźmie wiadomość o zaistnieniu jednej z sytuacji określonych w pkt. 1 niniejszego Rozdziału, jest zobowiązana do niezwłocznego zawiadomienia o powyższym swego bezpośredniego przełożonego, IOD, a także Informatyka.
4. IOD każdorazowo dokonuje oceny czy wykryty lub zgłoszony incydent/podejrzenie wystąpienia incydentu powoduje, że naruszenie praw i wolności osób fizycznych, których incydent dotyczy, jest prawdopodobne. Prawdopodobieństwo ocenia w oparciu o Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 z dnia 3 października 2017 r. (WP 250), w skali od 1 do 3 przy czym:
 - 4.1. dla wartości 1 przyjmuje się, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
 - 4.2. dla wartości 2 przyjmuje się, że jest prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
 - 4.3. dla wartości 3 przyjmuje się, że jest wręcz pewne, że naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
5. W przypadku stwierdzenia naruszenia przetwarzania danych w systemie informatycznym IOD oraz Informatyk mogą zdecydować ponadto o natychmiastowym zablokowaniu lub ograniczeniu dostępu do zbioru danych osobie podejrzanej o dokonanie naruszenia, z jednoczesnym powiadomieniem o tym fakcie bezpośredniego przełożonego tej osoby.
6. W szczególnie uzasadnionych przypadkach IOD w porozumieniu z ADO mogą podjąć decyzję o całkowitym lub czasowym zablokowaniu dostępu do zbioru (np. utrata integralności zbioru danych powodująca możliwość jego całkowitej lub częściowej utraty, włamanie do zbioru z możliwością zniszczenia części lub całości danych).
7. Ocena incydentu dokonywana jest na załączniku numer 15 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia”.
8. Każdy zgłoszony lub wykryty incydent, bez względu na jego ocenę, wymaga opisanie:
 - 8.1. charakteru naruszenia danych osobowych; kategorię i przybliżoną ilość osób, których dane dotyczą; kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - 8.2. imienia i nazwiska oraz danych kontaktowych osoby, od której można uzyskać więcej informacji (osoba odpowiedzialna za obsługę incydentu);
 - 8.3. możliwych konsekwencji zaistniałego naruszenia ochrony danych osobowych;
 - 8.4. zastosowanych lub proponowanych przez Administratora środków w celu zaradzenia naruszeniu ochrony danych osobowych.
9. Okoliczności przytoczone wyżej, dokumentowane są przez IOD w ramach załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia”.
10. Incydenty, którym przypisano wartość 1 uwzględnia się w załączniku numer 16 „Rejestr Naruszeń”.
11. Incydenty, którym przypisano wartość 2:

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	22 z 46
		Wydanie	1
		Data wydania	2020-09-01

- 11.1. stają się przedmiotem zgłoszenia do właściwego organu nadzorczego (obecnie Prezes Urzędu Ochrony Danych Osobowych). Zgłoszenie jest dokonywane w przeciągu 72 godzin od stwierdzenia naruszenia poprzez przesłanie do organu kopii uzupełnionego załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia”;
- 11.2. uwzględnia się w załączniku numer 15 „Rejestr Naruszeń”.
12. Incydenty, którym przypisano wartość 3:
 - 12.1. stają się przedmiotem zgłoszenia do właściwego organu nadzorczego (obecnie Prezes Urzędu Ochrony Danych Osobowych). Zgłoszenie jest dokonywane w przeciągu 72 godzin od stwierdzenia naruszenia poprzez przesłanie do organu uzupełnionego załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia”;
 - 12.2. stają się przedmiotem niezwłocznie przekazywanego zawiadomienia, kierowanego do każdej osoby fizycznej objętej incydem, zgodnie z załącznikiem numer 17 „Zawiadomienie osoby fizycznej o naruszeniu”;
 - 12.3. uwzględnia się w załączniku numer 16 „Rejestr Naruszeń”.
13. Nie zawiadamia się osób fizycznych o naruszeniu jeżeli:
 - 13.1. ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (np. doszło do kradzieży laptopa, jednak dane na nim zgromadzone zostały zaszyfrowane w sposób uniemożliwiający odczyt osobom nieuprawnionym);
 - 13.2. ADO niezwłocznie zastosował odpowiednie środki techniczne i organizacyjne eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą;
 - 13.3. Zawiadomienie wymagałoby niewspółmiernie dużego wysiłku. W takim wypadku wydany zostanie publiczny komunikat (a jeżeli naruszenie dotyczy tylko pracowników Administratora - komunikat wewnętrzny), za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób o okolicznościach zawartych w załączniku numer 17 „Zawiadomienie osoby fizycznej o naruszeniu”.
14. Incydenty zawarte w załączniku numer 16 „Rejestr Naruszeń” uwzględnia się w przeprowadzanym corocznie lub doraźnie procesie zarządzania ryzykiem bezpieczeństwa informacji.
15. W przypadku podjęcia decyzji o złożeniu do organów ścigania karnego zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa stosuje się zasady postępowania określone w tej kwestii w odrębnych wewnętrznych aktach organizacyjnych.
16. Określony w niniejszym Rozdziale tryb postępowania ma zastosowanie także w przypadku zaistnienia sytuacji, której okoliczności będą dawały podstawę do skierowania skargi do organu nadzorczego w związku z działaniem podmiotów zewnętrznych w odniesieniu do danych osobowych, których Administratorem Danych Osobowych jest Urząd Gminy w sposób niezgodny z Ustawą i Rozporządzeniem.
17. Wszelkich informacji prasowych na temat zaistniałego zdarzenia może udzielać wyłącznie Administrator lub działający z jego upoważnienia pracownicy.

ROZDZIAŁ XVI. POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Wójt Gminy Świlcza jest zobowiązany zapoznać z treścią „Polityki Bezpieczeństwa Danych Osobowych” podległych pracowników.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na ich podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce”.
5. Szczegółowe zasady przetwarzania danych osobowych określone w niniejszej Polityce, przez podmioty zewnętrzne, regulują stosowne umowy zawarte z nimi w tym zakresie.
6. Procedura udzielenia upoważnienia do przetwarzania danych osobowych dotyczy także osób, które uzyskują dostęp do danych osobowych w trakcie świadczenia pracy na podstawie innej umowy niż stosunek pracy lub wynikających z umów zawartych z innymi podmiotami, np. praktyki studenckie, staże pracownicze.

	Polityka Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	23 z 46
		Wydanie	1
		Data wydania	2020-09-01

7. W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa Danych Osobowych” mają zastosowanie przepisy Rozporządzenia.


[Handwritten signature]

[Handwritten signature]

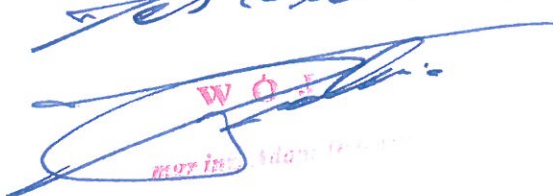
WÓJT

[Handwritten signature]

mgr. Jolanta Dzięcioł


	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	1 z 9
		Wydanie	1
		Data wydania	2020-09-01

*Załącznik Nr 2
do Zarządzenia Nr 140.2020
z dnia 1 września 2020 r.*

[Signature]

 Wójt
 Urząd Gminy Świltza

INSTRUKCJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH URZĄD GMINY ŚWILTZA

WRZESIEŃ 2020

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	2 z 9
		Wydanie	1
		Data wydania	2020-09-01

1. WSTĘP

Niniejszy dokument ma za zadanie stanowić zbiór zasad postępowania w zakresie ochrony danych osobowych. Został stworzony celem przedstawienia pracownikom i współpracownikom uczestniczącym przy przetwarzaniu danych osobowych w celu budowania ich świadomości i prawidłowych nawyków.

Pracownicy w ramach bieżącej pracy przestrzegają następujących zasad:

2. RUCH OSOBOWYCH


- 2.1. W pomieszczeniach gdzie zlokalizowany jest sprzęt komputerowy mogą przebywać wyłącznie osoby upoważnione.
 - 2.1.1. Klienci Jednostki mogą przebywać w pomieszczeniach, gdzie zlokalizowany jest sprzęt komputerowy wyłącznie pod nadzorem pracowników Jednostki.
 - 2.1.2. Pozostałe osoby (inne niż pracownicy, współpracownicy i Klienci Jednostki) mogą przebywać w pomieszczeniach gdzie zlokalizowany jest sprzęt komputerowy oraz dane osobowe wyłącznie w pod nadzorem pracownika Jednostki lub na podstawie zgody udzielonej przez władzę do tego osobę w Jednostce.
- 2.2. Dostęp do pomieszczeń może być możliwy wyłącznie w czasie pracy.
- 2.3. Osoby wykonujące czynności konserwacyjne, naprawcze lub serwisowe, które nie posiadają upoważnienia mogą przebywać w obszarach bezpiecznych pod nadzorem osób upoważnionych.

3. ROZPOCZĘCIE I ZAKOŃCZENIE PRACY W POMIESZCZENIACH, W KTÓRYCH PRZETWARZA SIĘ INFORMACJE

- 3.1. Przed przystąpieniem do pracy w systemie informatycznym należy sprawdzić stację roboczą (komputer) i stanowisko pracy zwracając uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji powodowanych czynnikami zewnętrznymi (np. naruszenie zamków, krat, wybite okna).
- 3.2. Przed wyjściem z pomieszczenia należy upewnić się, że okna oraz miejsca, w których przechowuje się informacje podlegające ochronie zostały zamknięte.
- 3.3. Po zamknięciu pomieszczenia należy odpowiednio zabezpieczyć klucze przed nieuprawnionym użyciem.

4. ZASADY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

- 4.1. Przed uruchomieniem stacji roboczej tam gdzie jest to możliwe, należy upewnić się, że okablowanie jest odpowiednio podłączone i nie zostały uszkodzone gniazda prądowe.
- 4.2. Aby zawiesić pracę (tymczasowa przerwa w pracy w systemie informatycznym) należy zablokować stację kombinacją klawiszy „Microsoft + L”. Dokumenty tradycyjne powinny zostać zabezpieczone zgodnie z polityką czystego biurka.
- 4.3. Kończąc pracę należy wylogować się z systemu informatycznego, zamknąć wszystkie aplikacje i upewnić się, że system operacyjny stacji roboczej zamknął się prawidłowo.

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	3 z 9
		Wydanie	1
		Data wydania	2020-09-01

5. BEZPIECZEŃSTWO WYDRUKÓW

- 5.1. Podczas drukowania należy zachować szczególną ostrożność wybierając drukarkę, na którą mają zostać wydrukowane dokumenty, aby wydruk przez pomyłkę nie dostał się do osób nieupoważnionych.
- 5.2. Wydruki należy niezwłocznie odebrać, aby wydrukowane dokumenty nie pozostały na podajnikach.
- 5.3. W przypadku, gdy wydruki blokują się w kolejkach wydruku, należy o zdarzeniu poinformować osobę odpowiedzialną za działanie drukarek. Nie należy uruchamiać kolejnych wydruków, jeżeli poprzedni wydruk się nie powiódł.
- 5.4. Dokumenty zbędne w bieżącej działalności muszą być niszczone w urządzeniu do tego przeznaczonym – dokumenty takie nie mogą zostać wyrzucone bezpośrednio do kosza na śmieci.

6. ROZMOWY TELEFONICZNE I FAKS


- 6.1. Pracownicy zobowiązani są do przestrzegania zakazu prowadzenia rozmów telefonicznych, podczas których może dochodzić do wymiany informacji chronionych, jeśli rozmowy te odbywają się w miejscach publicznych (np. pociągach, poczekalniach) oraz takich, które nie gwarantują zachowania poufności rozmów.
- 6.2. Pracownikom zabrania się zapisywania w systemach poczty głosowej informacji wrażliwych (tzn. takich, które są istotne i chronione na najwyższym poziomie).
- 6.3. Odczytanie indywidualnych wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła.
- 6.4. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
- 6.5. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje chronione jest zabronione.

7. ZASADY TRANSMISJI PLIKÓW W SIECI TELEINFORMATYCZNEJ


- 7.1. Informacje o wysokiej istotności (np. dane osobowe), wysyłane poza sieć wewnętrzną muszą zostać zaszyfrowane.
- 7.2. Proponuje się wykorzystanie programów 7zip lub WinRar, które dają możliwość zaszyfrowania plików, które chcemy wysłać pocztą elektroniczną.
- 7.3. Hasło do zaszyfrowanego pliku należy przekazać SMS'em lub telefonicznie. Zabronione jest wysyłanie hasła do maila - w mailu do tej osoby.
- 7.4. Jeżeli używany program do edycji tekstu (np. MS Word lub Excel) daje możliwość zaszyfrowania pliku hasłem – można skorzystać z tej funkcjonalności zamiast rozwiązania opisanego w punkcie 6.2.

8. BEZPIECZNA POCZTA ELEKTRONICZNA

- 8.1. W przypadku jednostek publicznych, zaleca się korzystanie wyłącznie z Elektronicznej Platformy Usług Administracji Publicznej (e-PUAP), dopuszczalne jest wykorzystywanie poczty do zastosowań biznesowych.
- 8.2. Nie zaleca się korzystania z darmowych kont pocztowych.

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlecza	Strona	4 z 9
		Wydanie	1
		Data wydania	2020-09-01

- 8.3. Nie zaleca się zapisywania haseł do poczty elektronicznej przez przeglądarkę internetową.
- 8.4. Podczas wysyłania wiadomości należy zweryfikować poprawność adresów e-mail odbiorcy.
- 8.5. Bezpieczne logowanie do poczty elektronicznej:
- 8.5.1. Jeśli logujesz się do swojego konta poprzez interfejs webmail, korzystając z przeglądarki internetowej, sprawdź jaki adres pojawia się w pasku adresu. Powinien rozpoczynać się <https://>.
 - 8.5.2. Sprawdź certyfikat bezpieczeństwa (należy kliknąć kłódkę tuż obok paska adresu – wtedy wyświetla się informacja czy połączenie jest szyfrowane).
 - 8.5.3. Jeżeli zarządzasz swoją pocztą elektroniczną włącz filtr antyspamowy.
 - 8.5.4. Nie otwieraj załącznika, jeśli nie jesteś pewien, kto wysłał do Ciebie wiadomość.
 - 8.5.5. Unikaj otwierania plików, które zawierają końcówkę: .exe, .bat, .com, .lnk, .scr, .vbs.
 - 8.5.6. Nie klikaj w linki od nieznanych nadawców, mogą zawierać przekierowanie do zainfekowanych stron.
 - 8.5.7. Nie odpowiadaj na wiadomości od podejrzanych nadawców.
 - 8.5.8. Korzystaj z dwuetapowego systemu uwierzytelniania, jeśli jest taka możliwość.
 - 8.5.9. Jeśli uznasz wiadomość za niechcianą i podejrzaną, oznacz ją jako SPAM. Możesz to zrobić poprzez wciśnięcie przycisku „zgłoś SPAM”. Umożliwia Ci to filtr antyspamowy. Możesz również dodać nadawcę do tzw. listy zablokowanych nadawców. W ten sposób uczysz swój filtr antyspamowy właściwej oceny swoich maili.
 - 8.5.10. Do każdego konta podawaj zawsze inne hasło.
- 8.6. Korespondencja elektroniczna:
- 8.6.1. Pracownik przysyłając informacje za pośrednictwem poczty elektronicznej ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy.
 - 8.6.2. Zabrania się przysyłania za pośrednictwem poczty elektronicznej treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
 - 8.6.3. Zabrania się przysyłania do innych pracowników, wiadomości o treści niezwiązanej z jej działalnością, a w szczególności wiadomości elektronicznych zawierających m.in.: informacje o charakterze komercyjnym, niechcianych lub niepotrzebnych wiadomości.
 - 8.6.4. Zabrania się rozsyłania za pośrednictwem poczty elektronicznej załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu systemu teleinformatycznego pracodawcy.
 - 8.6.5. Zabrania się wykorzystywania przydzielonego pracownikowi służbowego konta pocztowego do celów prywatnych (np. prowadzenie korespondencji nie związanej z działalnością służbową, rejestrowania się przy użyciu konta służbowego na forach, portalach społecznościowych, newsletterach, itp.).
 - 8.6.6. Zabrania się przekierowywania poczty służbowej na prywatną skrzynkę (np. w celu pracy w domu).
 - 8.6.7. Wiadomości przesyłane pocztą elektroniczną poza sieć służbową, zawierające informacje chronione należy zabezpieczyć.

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	5 z 9
		Wydanie	1
		Data wydania	2020-09-01

8.6.8. W ramach użytkowania poczty elektronicznej zabrania się wysyłania plików multimedialnych (np. .mp3, .wav, .mov, .avi) oraz wykonywalnych (np. .exe, .bat, .com, .cmd), chyba że wynika to wprost z obowiązków służbowych wykonywanych przez pracownika.

9. ZASADA CZYSTEGO EKRANU

9.1. Należy zadbać, aby ustawienia monitorów stacji roboczych nie pozwalały na przeglądanie wyświetlonych informacji osobom postronnym (np. ułożenie monitora komputera „plecami” do wejścia do pomieszczenia lub wydzielonego miejsca na przyjęcie klienta/osoby trzeciej).

10. ZASADY STOSOWANIA HASEŁ


- 10.1. Rekomenduje się zmianę hasła co najmniej raz na sześć miesięcy. Obowiązkiem pracownika jest zmiana hasła raz w roku.
- 10.2. Hasło powinno być złożone z minimum 8 znaków, dużych i małych liter, cyfr lub znaków specjalnych.
- 10.3. Nie dopuszcza się stosowania haseł zawierających: imiona, nazw pracownika, daty, nazwy miast czy państw oraz wyrazów posiadających skojarzenie z osobą.
- 10.4. Udostępnianie własnego hasła jest rażącym naruszeniem obowiązków pracowniczych.
- 10.5. Hasło nie powinno być zapisywane.
- 10.6. W przypadku podejrzenia, iż nasze hasło zostało ujawnione/skompromitowane (zostało zagubione, poznały je niepowołane osoby) należy bezzwłocznie powiadomić o tym fakcie informatyka.
- 10.7. Niedopuszczalne jest stosowanie tych samych haseł prywatnie oraz w pracy.
- 10.8. W przypadku zablokowania hasła należy zwrócić się do informatyka w celu jego odblokowania.

11. ZASADY UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH

- 11.1. Należy przywiązywać szczególną uwagę do weryfikacji poprawności danych przed ich wprowadzeniem do systemu. Wprowadzane dane powinny spełniać wymagania odnośnie jakości.
- 11.2. Wszelkie problemy z jakością oraz błędy w danych zauważone podczas przetwarzania danych należy niezwłocznie zgłaszać przełożonym lub rejestrować w systemie zgłoszeń incydentów, których te problemy dotyczą.
- 11.3. Należy postępować zgodnie z instrukcjami informatyka.

12. OPROGRAMOWANIE


- 12.1. Pracownik może korzystać jedynie z oprogramowania, na które pracodawca posiada aktualne licencje lub posiada prawo do używania.
- 12.2. Pracownik nie może za pomocą komputerów służbowych pobierać z Internetu lub przysyłać nielicencjonowanego oprogramowania oraz innych utworów chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	6 z 9
		Wydanie	1
		Data wydania	2020-09-01

- 12.3. Pracownik nie może instalować na komputerach pracodawcy prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.

13. ZASADY DOTYCZĄCE DOSTĘPU DO SIECI INTERNET

- 13.1. Dostęp do sieci Internet może odbywać się wyłącznie na podstawie nadanych uprawnień w zakresie realizowania zadań służbowych. Korzystając z usług sieciowych należy przestrzegać następujących zasad:
- 13.1.1. użytkować Internet wyłącznie do celów służbowych,
 - 13.1.2. korzystać wyłącznie z witryn internetowych niezbędnych do realizacji zadań służbowych,
 - 13.1.3. zweryfikować certyfikaty udostępniane na witrynie,
 - 13.1.4. pliki zawierające dane chronione należy przed wysłaniem zabezpieczyć (stosując szyfrowanie wiadomości z hasłem do otwarcia pliku).
- 13.2. Korzystaj z antywirusa i konta z ograniczonymi uprawnieniami (nie admina).
- 13.3. W przypadku oznak zainfekowania komputera złośliwym oprogramowaniem należy:
- 13.3.1. Powiadomić osobę odpowiedzialną za nadzór i konserwację systemów informatycznych (zadanie pracownika).
 - 13.3.2. Odłączyć komputer od sieci lokalnej oraz sieci Internet (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
 - 13.3.3. Jeśli nie można uruchomić komputera z dysku twardego (błąd przy starcie), należy spróbować uruchomić system w trybie awaryjnym lub przy użyciu dysku startowego systemu Windows (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
 - 13.3.4. Wykonać pełne skanowanie systemu operacyjnego (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
- 13.4. Korzystanie z sieci Internet.
- 13.4.1. Pracownik ma prawo korzystać z sieci Internet wyłącznie: w celach związanych z realizacją zadań służbowych, zgodnie z obowiązującymi regulaminami i przepisami prawa, w zakresie przyznanych uprawnień.
 - 13.4.2. Pracownikowi zabronione jest korzystanie z sieci Internet w celu: uzyskania nieuprawnionego dostępu do zasobów będących własnością pracodawcy lub zasobów podmiotów zewnętrznych, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów (informacji, danych, tekstów, programów komputerowych, dźwięków, fotografii, grafik, filmów) naruszających prawa własności intelektualnej, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów zakazanych przepisami prawa, w tym m.in. zawierających groźby, treści obraźliwe, zniesławiające, pornograficzne lub naruszających w jakikolwiek inny sposób prawa innych osób.
 - 13.4.3. Zabronione jest podejmowanie przez pracowników działań powodujących istotne ograniczenia w korzystaniu z sieci Internet przez innych pracowników, a w szczególności: pobieranie dużej ilości danych, w sytuacji, gdy nie jest to uzasadnione wykonywanymi obowiązkami służbowymi, podejmowanie działań skutkujących ograniczeniami w funkcjonowaniu jakichkolwiek usług sieciowych.

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	7 z 9
		Wydanie	1
		Data wydania	2020-09-01

13.4.4. Zabronione jest umożliwianie dostępu z Internetu do zasobów zlokalizowanych na urządzeniu komputerowym lub w sieci służbowej (np. przy wykorzystaniu serwerów WWW, ftp, programów tunelujących, P2P).

14. ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH


- 14.1. Pracownik może wnosić sprzęt komputerowy wyłącznie za zgodą przełożonego, po uprzednim upewnieniu się, że urządzenie zostało zaszyfrowane - np. poprzez ustanowienie hasła dostępu.
- 14.2. Komputer nie może być udostępniany osobom nieuprawnionym.
- 14.3. Instalacja oprogramowania może być dokonywana wyłącznie przez informatyka.
- 14.4. W przypadku kradzieży komputera należy o tym fakcie poinformować informatyka.
- 14.5. W razie utracenia urządzenia mobilnego – bez względu na to, czy był on szyfrowany, czy też nie – pracownik jest zobowiązany do poinformowania o tym Informatyka oraz swojego bezpośredniego przełożonego.
- 14.6. Obowiązuje zakaz wykorzystywania prywatnych nośników informacji (płyty CD, DVD, kart SD, kart SSD, dysków zewnętrznych, pendrive, laptopów i im podobnych) do celów służbowych. Odstępstwo od zasady wymaga zgody Wójta wyrażonej na piśmie.
- 14.7. Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo (np. szafy zamykane na klucz).

15. ZASADY DOTYCZĄCE POLITYKI ANTYWIRUSOWEJ

- 15.1. W przypadku, gdy program antywirusowy zgłasza nieaktualną bazę sygnatur wirusów należy o tym fakcie poinformować osobę odpowiedzialną za nadzór i konserwację systemów informatycznych.
- 15.2. W przypadku identyfikacji wirusa na komputerze należy zawiesić pracę i niezwłocznie o tym fakcie poinformować osobę odpowiedzialną za nadzór i konserwację systemów informatycznych.
- 15.3. Wszystkie nośniki zewnętrzne podłączane do stacji roboczej należy przed użyciem sprawdzić programem antywirusowym.

16. ZGŁASZANIE ZDARZEŃ MOGĄCYCH ŚWIADCZYĆ O NARUSZENIU BEZPIECZEŃSTWA

- 16.1. Wszystkie niestandardowe działania systemu informatycznego oraz zdarzenia mogące wskazywać na utratę bezpieczeństwa powinny być niezwłocznie zgłoszone osobie odpowiedzialnej za nadzór i konserwację systemów informatycznych.
- 16.2. Symptomy wskazujące, na możliwość naruszenia bezpieczeństwa teleinformatycznego:
 - obcy identyfikator w oknie logowania,
 - nietypowe obciążenie (spowolnienie pracy) stacji roboczej,
 - nowe oprogramowanie nieznanego typu,
 - wyłączony program antywirusowy,
 - zwiększona ilość niechcianej poczty (spamu),
 - brak możliwości zalogowania się na własny identyfikator i hasło,

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świlcza	Strona	8 z 9
		Wydanie	1
		Data wydania	2020-09-01

- nazwy plików w historii, które nie były otwierane,
- widoczne ślady przebywania osób trzecich w czasie nieobecności.

17. ZASADY NAPRAWY SPRZĘTU KOMPUTEROWEGO


- 17.1. W przypadku, gdy na nośnikach stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje podlegające ochronie, pracownik ma obowiązek zgłosić ten fakt przy przekazywaniu urządzenia do serwisu. Sprzęt taki naprawiany jest pod nadzorem informatyka lub innego właściwego pracownika. Jeżeli zaś taki nadzór nie jest możliwy, to informacje muszą być uprzednio skutecznie usunięte, przy zapewnieniu możliwości ich późniejszego odtworzenia, bądź jeśli istnienie możliwość wymontowania nośnika danych (np. dysku twardego z komputera przenośnego), urządzenie należy przekazać do naprawy po uprzednim wymontowaniu nośnika. Fakt oddania urządzenia do naprawy stwierdza się poprzez spisanie protokołu zdawczo-odbiorczego.
- 17.2. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie przez pracownika.
- 17.3. Pamiętaj, że takie same zagrożenia jakie generuje laptop, w większości przypadków dotyczą również telefonów komórkowych.

18. ZASADY MONITOROWANIA USŁUG I ZASOBÓW

- 18.1. Wszelkie usługi (np.: poczta elektroniczna, serwer plików, Internet), do których pracownik posiada dostęp, nie mogą być wykorzystywane do celów prywatnych ani działań, które stanowią naruszenie obowiązującego w Polsce prawa np. sabotaż, przestępstwa informatyczne, oszustwa, przemoc, rasizm, terroryzm itp.
- 18.2. Pracownik zobowiązany jest przechowywać kopie dokumentów istotnych dla funkcjonowania pracodawcy w folderach sieciowych w celu zapewnienia możliwości objęcia ich procesem tworzenia kopii zapasowych. Dostęp do takich katalogów powinny mieć jedynie osoby uprawnione.
- 18.3. Informacje wrażliwe (np. dane osobowe, tajemnica przedsiębiorstwa) przesyłane pocztą elektroniczną poza siecią służbową winny być przesyłane w postaci zaszyfrowanej lub przesyłane w skompresowanym załączniku z użyciem hasła. Hasło powinno być przekazywane przy wykorzystaniu innego kanału komunikacji np. telefonicznie, przy pomocy wiadomości sms.
- 18.4. Komputery, konta pocztowe, nośniki danych – pamięci flash (pendrive) i inne urządzenia przekazane w ramach obowiązków służbowych, stanowią własność pracodawcy i mogą być wykorzystywane wyłącznie w ramach realizacji powierzonych zadań związanych z wykonywaną pracą.
- 18.5. Wszelkie dane wytworzone przez pracowników na urządzeniach komputerowych należących do pracodawcy są jego własnością.
- 18.6. Przełożeni pracowników, mają prawo i obowiązek kontrolować, czy pracownicy korzystający z urządzeń komputerowych stosują się do regulacji określonych w niniejszym dokumencie.

19. ZASADY ODPOWIEDZIALNOŚCI PRACOWNIKÓW ZA SZKODY ZWIĄZANE Z NIEPRAWIDŁOWYM UŻYTKOWANIEM URZĄDZEŃ SŁUŻBOWYCH

- 19.1. W przypadku uszkodzenia urządzenia komputerowego wynikającego z rażącego zaniedbania pracownika w zakresie sprawowania opieki nad powierzonym urządzeniem, pracownik ten

	Instrukcja Bezpieczeństwa Danych Osobowych Urząd Gminy Świltza	Strona	9 z 9
		Wydanie	1
		Data wydania	2020-09-01

może zostać obciążony kosztami jego naprawy bądź wymiany. Decyzję o obciążeniu kosztami naprawy, bądź odtworzenia sprzętu podejmuje bezpośredni przełożony pracownika.

19.2. Pracownicy naruszający zasady korzystania ze sprzętu komputerowego określone w niniejszym dokumencie, mogą podlegać odpowiedzialności na zasadach określonych w obowiązujących przepisach prawa.

19.3. Pracownicy ponoszą pełną odpowiedzialność za:

- powierzony sprzęt;
- naruszenie prywatności innego pracownika;
- dopuszczenie do infrastruktury teleinformatycznej osób nieuprawnionych;
- udostępnienie swojego komputera lub konta innej osobie oraz wykorzystanie przez nią dostępu do infrastruktury;
- podszywanie się pod innych pracowników;
- wszelkie dane przechowywane w ramach kont pocztowych;
- wszelkie dane przechowywane na komputerze służbowym podłączonym do sieci LAN oraz poczynania dokonywane za pomocą swojego komputera lub z wykorzystaniem swojego konta.