Polityka Ochrony Danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 1 do Zarządzenia nr 22

Starosty Wrzesińskiego z dnia 14 kwietnia 2026 roku

Polityka Ochrony Danych

I. Informacje ogólne

1. Cel i zakres

Niniejsza Polityka Ochrony Danych ma na celu opisanie zasad i procedur stosowanych przez Administratora w celu spełnienia wymagań 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, zwanego w dalszej części polityki RODO.

Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w artykule 5 ust. 1 ppkt a) – e) RODO.

Administrator zaznacza, że niniejsza polityka to jeden ze środków o charakterze organizacyjnym, za pomocą którego wykazuje się zgodność przetwarzania danych osobowych z RODO.

Administrator deklaruje pełną świadomość charakteru, rodzaju i kontekstu przetwarzanych danych osobowych.

2. Podstawy prawne

2.1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

2.2. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.

3. Budowa dokumentu

3.1. **Polityki** – ogólne zapisy dotyczące stosowania zasad ochrony danych;

3.2. **Procedury** – szczegółowe zapisy dotyczące stosowania tych zasad;

3.3. **Instrukcje** – precyzyjne stosowanie zasad, opisane w procedurach.

4. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

4.1. **Administratorze** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

4.2. **Organizacji** – rozumie się przez to Starostwo Powiatowe we Wrześni;

4.3. **Inspektorze Ochrony Danych** – rozumie się przez to osobę wyznaczoną przez Administratora do pełnienia nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych w Organizacji;

4.4. **Administratorze Systemu Informatycznego** – rozumie się przez to osobę wyznaczoną do pełnienia nadzoru nad prawidłowym działaniem infrastruktury informatycznej;

4.5. **Rozporządzeniu (RODO)** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

4.6. **Ustawie** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;

4.7. **Organie nadzorczym (PUODO/UODO)** – rozumie się przez to ustanowiony niezależny organ publiczny odpowiedzialny za monitorowanie Rozporządzenia w celu ochrony podstawowych praw i wolności osób fizycznych;

4.8. **Danych osobowych** – rozumie się przez to 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;

4.9. **Przetwarzaniu** – rozumie się przez to 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;

4.10. **Incydencie** – rozumie się przez to niepożądane działanie, które może prowadzić do naruszenia ochrony danych osobowych.

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

4.12. **Podmiocie przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

4.13. **Odbiorcy** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania, zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;

4.14. **Profilowaniu** – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych

osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

4.15. **Zgodzie osoby, której dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

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

4.17. **Udostępnieniu danych** – rozumie się przez to przetwarzanie polegające na ujawnieniu osobie trzeciej danych osobowych, których jest się Administratorem.

II. Organizacja przetwarzania

1. **Za przetwarzanie danych osobowych w organizacji oraz ich ochronę** zgodnie z postanowieniami RODO, Ustawy oraz wewnętrznymi regulacjami w organizacji, odpowiada Administrator. Administrator wyznacza i upoważnia osoby, które w jego imieniu realizują określone zadania w zakresie ochrony danych osobowych.
2. **Administratorem danych** przetwarzanych w Starostwie Powiatowym we Wrześni jest Starosta Wrzesiński, z siedzibą we Wrześni przy ul. Chopina 10.
3. **Obszar przetwarzania danych u Administratora** tworzą pomieszczenia biurowe, archiwum, serwerownia, zlokalizowane w siedzibie Starostwa Powiatowego pod adresem wskazanym w pkt. 2, Wydziału Dróg Powiatowych pod adresem ul. 3 Maja 3 we Wrześni oraz siedzibie Powiatowego Zespół do Spraw Orzekania o Niepełnosprawności - budynek Szpitala Powiatowego we Wrześni, ul. Słowackiego 2.

4. Administrator

4.1. **Administrator realizuje zadania** w zakresie ochrony danych osobowych, w tym zwłaszcza:

4.1.1. podejmuje decyzje o celach i środkach przetwarzania danych osobowych, z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, własnej strukturze organizacyjnej oraz technik zabezpieczania danych osobowych;

4.1.2. wdraża odpowiednie środki techniczne i organizacyjne zabezpieczania danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób, których dane dotyczą;

4.1.3. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym, indywidualnym zakresie, odpowiadającym zakresowi ich obowiązków;

4.1.4. wyznacza Inspektora Ochrony Danych oraz określa zakres jego zadań i obowiązków;

4.1.5. wyznacza Administratora Systemu Informatycznego oraz określa zakres jego zadań i obowiązków;

4.1.6. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczeństwa przetwarzania danych osobowych;

4.1.7. przed rozpoczęciem przetwarzania, dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;

4.1.8. zapewnia odpowiednie relacje między Administratorem i podmiotem, któremu powierzono przetwarzanie danych.

4.2. **Obowiązki Inspektora Ochrony Danych** pełni osoba wyznaczona w trybie art. 37 RODO przez Administratora.

4.3. **Administrator,** wyznaczając Inspektora Ochrony Danych, ma obowiązek zawiadomić Organ Nadzorczy o jego wyznaczeniu, zgodnie z art. 10 Ustawy oraz udostępnić jego dane zgodnie z art. 11 Ustawy.

4.4. **Administrator może** każdorazowo odwołać IOD lub wyznaczyć do pełnienia funkcji inną osobę.

5. Inspektor Ochrony Danych

5.1. **Status Inspektora Ochrony Danych:**

5.1.1. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

5.1.2. Administrator zapewnia IOD zasoby niezbędne do wykonania zadań oraz dostęp do danych osobowych i operacji przetwarzania;

5.1.3. IOD w ramach wykonywania swoich zadań podlega bezpośrednio Administratorowi.

5.2. **IOD realizuje zadania** w zakresie ochrony danych osobowych, w tym zwłaszcza:

5.2.1. informuje Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów o ochronie danych i doradza im w tej sprawie;

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

5.2.3. udziela, na żądanie, zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie, zgodnie z art. 35 RODO;

5.2.4. współpracuje z Organem Nadzorczym;

5.2.5. pełni funkcję punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz, w stosownych przypadkach, prowadzi konsultacje we wszelkich innych sprawach.

5.2.6. **Przynajmniej raz w roku przeprowadzane są audyty zgodnie z procedurą.**

5.3. **Administrator może wyznaczyć osobę zastępującą IOD** w czasie jego nieobecności. Do zastępcy IOD stosuje się odpowiednio przepisy dotyczące Inspektora Ochrony Danych.

5.4. **Administrator, który wyznaczył osobę zastępującą IOD,** zawiadamia Organ Nadzorczy o jej wyznaczeniu w trybie określonym w art. 10 Ustawy oraz udostępnia jej dane, zgodnie z art. 11 Ustawy.

6. Administrator Systemu Informatycznego

6.1. **Obowiązki Administratora Systemu Informatycznego** i/lub jego zastępców, pełnią osoby wyznaczone przez Administratora.

6.2. **Administrator może** każdorazowo odwołać ASI.

6.3. **ASI realizuje zadania** w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora, w tym zwłaszcza:

6.3.1. zarządza systemem informatycznym, zlokalizowanym u Administratora, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora;

6.3.2. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego,

6.3.3. zakłada konta oraz przydziela uprawnienia upoważnionym użytkownikom, zgodnie z przekazanym mu wnioskiem;

6.3.4. wyrejestrowuje użytkowników z systemu informatycznego, zgodnie z przekazanym mu wnioskiem;

6.3.5. nadzoruje stosowanie mechanizmów uwierzytelniania użytkowników poprzez kontrolę poprawności użytkowania kont;

6.3.6. w sytuacjach stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje Administratora o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

6.3.7. 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;

6.3.8. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

6.3.9. inicjuje i nadzoruje wdrażanie nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;

6.3.10. informuje Administratora o konieczności wprowadzenia zmian w Instrukcji zarządzania systemem informatycznym (np. z powodu zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych);

6.3.11. nadzoruje wykonywanie kopii bezpieczeństwa i kopii archiwalnych baz danych, zgodnie z ustalonym planem;

6.3.12. zabezpiecza niszczenie nośników danych, zgodnie z obowiązującymi procedurami;

6.3.13. w przypadku współpracy z zewnętrzną firmą informatyczną, zgodnie z zapisami w umowie - obsługującą objęte umową czynności, organizuje i nadzoruje pracę przedstawicieli tych firm, dba o przestrzeganie wymaganych zasad bezpieczeństwa;

6.3.14. współpracuje z Inspektorem Ochrony Danych lub osobą wyznaczoną przez Administratora, wykonującą obowiązki w zakresie zadań związanych z ochroną danych osobowych;

6.3.15. prowadzi szkolenia użytkowników z zakresu bezpieczeństwa systemów informatycznych lub występuje z wnioskiem do Administratora o przeprowadzenie szkolenia użytkowników z zakresu obowiązujących zasad bezpieczeństwa informatycznego;

6.3.16. doskonali się z zakresu wiedzy o bezpieczeństwie systemów informatycznych.

7. **Naczelnicy Wydziałów oraz osoby na samodzielnych stanowiskach**

7.1. **Naczelnicy Wydziałów oraz osoby na samodzielnych stanowiskach, odpowiadają za bieżące zarządzanie ochroną danych osobowych i stosowanie procedur bezpieczeństwa w podległych im wydziałach.** Realizują zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych w swoim wydziale/komórce organizacyjnej oraz na samodzielnym stanowisku poprzez:

7.1.1. zapewnienie prawidłowego przetwarzania danych osobowych, w tym, w szczególności, realizacji obowiązku informacyjnego wobec osób, których dane dotyczą, zgodnie z art. 13 i 14 RODO;

7.1.2. zapewnienie prawidłowego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe w podległej komórce organizacyjnej;

7.1.3. zapewnienie prawidłowego zabezpieczenia danych w formie papierowej i elektronicznej;

7.1.4. zapewnienie prawidłowego działania innych zabezpieczeń fizycznych stosowanych u Administratora;

7.1.5. zapewnienie prawidłowego stosowania środków organizacyjnych;

7.1.6. w sytuacji konieczność przetwarzania nowych zbiorów danych ma obowiązek poinformować o tym fakcie Administratora;

7.1.7. udostępnianie IOD wszelkich informacji, niezbędnych do realizacji zasad określonych w dokumentacji bezpieczeństwa przetwarzania danych osobowych, w tym, w szczególności, o podstawach prawnych przetwarzania poszczególnych zbiorów danych;

7.1.8. konsultuje wdrożone zasady i procedury, związane z ochroną danych osobowych z IOD.

8. **Pozostałe osoby upoważnione do przetwarzania danych** realizują zadania w zakresie ochrony danych osobowych zawartych z zbiorach, do których mają dostęp, a w szczególności zobowiązani są do:

8.1. przestrzegania zasad przetwarzania danych osobowych zapisanych w dokumentacji bezpieczeństwa przetwarzania danych osobowych;

8.2. przekazywania IOD oraz bezpośredniemu przełożonemu wszelkich niezgodności związanych z ochroną danych osobowych;

8.3. informowania IOD o zmianach zaistniałych w przetwarzanych zbiorach;

8.4. niezwłocznego powiadomienia bezpośredniego przełożonego i IOD w sytuacji, gdy pracownik uzna, że dane osobowe zostały bądź są bezprawnie przetwarzane;

III. Weryfikacja posiadanych danych osobowych i zasady ich przetwarzania

1. Inwentaryzacja danych

1.1. Dane osobowe są zorganizowane w struktury, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO,

1.2. Dane osobowe opisane są z uwzględnieniem, co najmniej poniższych informacji:

- nazwy przetwarzanych danych osobowych,
- celów przetwarzania,
- zakresu przetwarzania,
- odbiorców danych,
- zakresu czynności przetwarzania,
- zasobów służących do przetwarzania danych osobowych,
- informacji o konieczności przeprowadzenia oceny skutków dla ochrony danych zawartych w zbiorze,
- okresu przechowywania.
- Szczegółowo opis danych osobowych został przedstawiony w Rejestrze czynności przetwarzania danych. Rejestr zawiera niezbędne elementy, wskazane w art. 30 ust. 1 RODO.
- Wzór rejestru określa Załącznik nr 1 do Polityki.

2. Legalność procesu przetwarzania danych osobowych

2.1. Administrator swoimi działaniami i organizacją zapewnia, że:

- dane osobowe przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 oraz art. 9 ust. 2 RODO,
- zakres pozyskiwanych danych wynika z przepisów prawa i jest adekwatny do zdefiniowanych celów przetwarzania,
- określono konkretny czas, przez jaki dane są przetwarzane,

- wobec osób, których dane są przetwarzane, wykonano obowiązek informacyjny, zgodnie z art. 13-14 RODO, ramowy wzór klauzuli informacyjnej wraz z instrukcją do wykorzystania przez pracowników znajduje się w załączniku nr 2,
- obowiązek informacyjny wobec osób może być wykonywany poprzez umieszczenie na tablicy informacyjnej w budynku, umieszczeniu go na formularzach lub na stronie internetowej.
- w szczególnych przypadkach, aby zapewnić większą przejrzystość, można skorzystać z warstwowych sposobów informowania, w pierwszej kolejności przekazuje się tylko podstawowe informacje, wskazując osobie, której dane dotyczą, w jaki sposób może zapoznać się z pełną informacją wymaganą przez art. 13-14 RODO,
- ze wszystkimi współpracującymi podmiotami gospodarczymi, podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty,
- jeżeli dane osobowe nie zostały pozyskane bezpośrednio od osób, których dotyczą, Administrator musi je o tym powiadomić w sposób umożliwiający im niepodważalne powzięcie takiej wiedzy, chyba że:

2.1..1. osoba posiada już te informacje;

2.1..2. przekazanie informacji jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;

2.1..3. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem;

2.1..4. dane osobowe muszą pozostać poufne, zgodnie z obowiązkiem zachowania tajemnicy zawodowej, przewidzianym w prawie.

2.2. Dane osobowe są pozyskiwane bezpośrednio od osób lub od innych podmiotów uczestniczących w procesach.

2.3. W przypadku stosowania zgody jako przesłanki przetwarzania danych, zaleca się pozyskiwanie jej w formie pisemnej. Wzór zgody wymaga konsultacji z IOD.

3. Upoważnienia do przetwarzania danych osobowych:

3.1. Administrator, do przetwarzania danych osobowych, dopuszcza jedynie osoby posiadające stosowne upoważnienia. Wzór upoważnienia stanowi Załącznik nr 3.

3.2. Upoważnienia wydane przed wprowadzeniem niniejszej Polityki zachowują swoją ważność. Wzory upoważnień, o którym mowa w pkt. 3.1., są stosowane dla osób, którym udzielono upoważnienia po dniu wejścia w życie niniejszej Polityki.

3.3. Naczelnik Wydział Informatyki i Bezpieczeństwa przygotowuje upoważnienie do przetwarzania danych osobowych osobie, która wcześniej odbyła szkolenie z ochrony danych osobowych.

3.4. Szkolenie może być przeprowadzone w formie tradycyjnej, w siedzibie Administratora lub poprzez internetową platformę multimedialną. Podczas szkolenia, pracownik zaznajamiany jest z podstawowymi aspektami ochrony danych osobowych (odpowiedzialność prawna, zabezpieczenia danych osobowych w formie papierowej i informatycznej), w szczególności z ustawą i Rozporządzeniem. Kolejno, pracownik zapoznaje się z wewnętrznymi regulacjami związanymi z przetwarzaniem danych osobowych u Administratora:

- Politykę ochrony danych;
- Procedurą postępowania z prawami osób, których dane dotyczą;
- Procedurą postępowania w związku z naruszeniami ochrony danych;
- Instrukcją zarządzania systemami Informatycznymi służącymi do przetwarzania danych osobowych;

3.5. Pracownik podpisuje oświadczenie zawarte w upoważnieniu w zakresie zapoznania i przyjęcia do stosowania przepisów prawa oraz wewnętrznych regulacji Administratora w zakresie ochrony danych osobowych oraz zobowiązuje się do zachowania ich w poufności.

3.6. Administrator, podpisuje upoważnienie.

3.7. Upoważnienia do przetwarzania danych osobowych przygotowywane są w jednym egzemplarzu i przechowywane w teczce, zawierającej wszystkie upoważnienia lub w aktach osobowych pracownika.

3.8. Na prośbę pracownika wydaje się pracownikowi kopię upoważnienia.

3.9. Upoważnienie wydaje się do dostępu do zbiorów danych osobowych w związku z wykonywaniem obowiązków służbowych, wynikających z aktualnego zakresu czynności.

3.10. Zmiana zakresu czynności nie wymaga nadania ponownego upoważnienia.

3.11. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

- Zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań, wynikających z jego indywidualnego zakresu czynności,
- Umyślnego naruszenia zasad ochrony danych osobowych określonych w ustawie, Rozporządzeniu lub Polityce,
- Rozwiązania stosunku pracy,
- Rozwiązania umowy cywilnoprawnej.

3.12. Utratę upoważnienia do przetwarzania danych odnotowuje się w ewidencji osób upoważnionych. Dodatkowo dopuszcza się umieszczenie stosownej adnotacji na samym upoważnieniu.

3.13. Ewidencję osób upoważnionych prowadzi Naczelnik Wydział Informatyki i Bezpieczeństwa. Wzór ewidencji stanowi załącznik nr 4 do Polityki.

4. Poufność procesu przetwarzania danych osobowych.

4.1. Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z Administratorem, jest zobowiązana do:

- przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało jej wydane upoważnienie lub podpisano umowę powierzenia przetwarzania danych osobowych,
- zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,
- niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia lub umowy powierzenia przetwarzania danych osobowych,
- zachowania poufności procesów i metod zabezpieczeń danych osobowych,
- ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacją, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób trzecich.

4.2. Dla osób, które nie otrzymują upoważnienia do przetwarzania danych osobowych, ale mogą mieć styczność z danymi w trakcie wykonywania obowiązków, stosuje się klauzulę poufności, której wzór stanowi załącznik nr 5.

4.3. Osoby dopuszczone do przetwarzania danych osobowych, przed przystąpieniem do pracy, odbywają szkolenie z zasad ochrony danych osobowych.

4.4. Osoby, które zostają dopuszczone do przetwarzania danych osobowych, a które zapoznały się treścią niniejszej Polityki, są zobowiązane do podpisania tzw. oświadczenia o zachowaniu poufności, które jest elementem upoważnienia do przetwarzania danych osobowych.

4.5. Zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.

4.6. Niedopuszczalne jest przekazywanie wszelkich informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.

4.7. W przypadku konieczności wydania dokumentów zawierających dane osobowe, należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w punkcie 4.5, a w przypadku, kiedy odbierającym nie jest adresat dokumentu, należy zażądać upoważnienia.

4.8. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych, np. biurkach, ladach, półkach, parapetach itp.

4.9. Wydruki i inne dokumenty zawierające dane osobowe, są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy. Stosowana jest zasada tzw. czystego biurka.

4.10. Po zakończeniu pracy, wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, zabezpieczonych dodatkowo np. zamkami w drzwiach, kratami w oknach, systemem kontroli dostępu lub innymi zabezpieczeniami fizycznymi.

4.11. Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarek.

4.12. Zaleca się zwrócenie szczególnej uwagi pracownikom na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, przy kopiarkach, przy drukarkach itp.

4.13. Administrator jest zobowiązany do weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, dla których ustały podstawy przetwarzania.

5. Współpraca z podmiotami zewnętrznymi

5.1. W działalności Administratora jest dopuszczalna współpraca z podmiotami zewnętrznymi, którym udostępnia się dane osobowe.

5.2. Powierzenie przetwarzania danych osobowych może odbywać się jedynie na podstawie umowy lub innego instrumentu prawnego, zgodnie z zasadami określonymi w art. 28 RODO.

5.3. Wzór umowy powierzenia stanowi załącznik nr 6.

5.4. Dopuszcza się stosowanie innej formy dokumentów niż wymieniona w pkt. 5.3, jeżeli zawiera wszystkie elementy wymagane przez art. 28 RODO.

5.5. Prowadzony jest rejestr podmiotów, z którymi podpisano umowy powierzenia. Wzór rejestru stanowi załącznik nr 7 do Polityki.

5.6. Przed powierzeniem danych, należy dokonać analizy i oceny podmiotu przetwarzającego na podstawie ankiety, która stanowi załącznik do umowy powierzenia.

5.7. Administrator może dokonywać czynności w imieniu innych Administratorów. Wówczas prowadzi Rejestr kategorii czynności przetwarzania zawierający elementy wskazane w art. 30 ust. 2 RODO. Wzór rejestru stanowi załącznik nr 8 do Polityki.

6. Udostępnianie danych

6.1. Administrator udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.

6.2. W przypadku udostępniania dokumentów za pomocą korespondencji mailowej, Administrator ma obowiązek szyfrować przekazywane pliki.

7. Uprawnienia osób, których dane osobowe są przetwarzane

7.1. Administrator zapewnia osobom, których dane osobowe przetwarza, realizację wszystkich przysługujących im praw.

7.2. Realizacja prawa odbywa się na podstawie stosownej procedury, która stanowi załącznik nr 9 do Polityki.

7.3. Prowadzi się ewidencję osób, których prawa są realizowane, wzór stanowi załącznik nr 10 do Polityki.

7.4. W przypadku zastosowania ograniczenia praw osób, należy taką sytuację pisemnie wyjaśnić osobie, która wniosła sprawę w zakresie realizacji jej praw.

8. Naruszenia ochrony danych osobowych

8.1. Opracowana została Procedura postępowania w związku z naruszeniami ochrony danych, która stanowi załącznik nr 11.

8.2. Integralną częścią Procedury jest Raport z naruszenia bezpieczeństwa ochrony danych osobowych, stanowiący załącznik do Procedury.

8.3. Typowe sytuacje, w których dochodzi do naruszenia ochrony danych osobowych, przedstawia tabela stanowiąca załącznik do Procedury.

8.4. Celem procedury jest zdefiniowanie możliwych naruszeń oraz opisanie instrukcji działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.

8.5. W przypadku stwierdzenia naruszenia ochrony danych osobowych u Administratora, opracowywany jest raport zgodnie z procedurą.

8.6. Wszystkie naruszenia są ewidencjonowane. Wzór ewidencji stanowi załącznik nr 12 do Polityki.

9. Procedura zarządzania systemami informatycznymi

9.1. Opracowana została Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

9.2. Instrukcja stanowi załącznik nr 13 do Polityki.

9.3. Celem Instrukcji jest usystematyzowanie działań związanych z systemami informatycznymi służącymi do przetwarzania danych osobowych.

9.4. Kopie bezpieczeństwa systemów informatycznych wykonywane są zgodnie z harmonogramem, który opracowuje ASI.

9.5. Zakres dostępu do systemu informatycznego poszczególnych użytkowników jest przydzielany na wniosek przełożonego. Wniosek może mieć postać pisemną lub elektroniczną. Formę oraz zakres formalno-rzeczowy wniosku ustala ASI po konsultacji z Administratorem oraz IOD.

IV. Ryzyko

1. Analiza ryzyka

1.1. U Administratora przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.

1.2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.

1.3. Analiza ryzyka jest przeprowadzona i ponawiana okresowo zgodnie z udokumentowaną metodyką stanowiącą odrębną od niniejszej Polityki dokumentację.

2. Ocena skutków dla ochrony danych osobowych

2.1. Dla zbiorów danych osobowych, w których znajdują się dane osobowe, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO.

2.2. Ocena skutków dla ochrony danych osobowych polega na:

2.2.1. opisie planowanych operacji i celów przetwarzania,

2.2.2. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,

2.2.3. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

2.2.4. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,

2.3. Ocena skutków dla ochrony danych może być wykonywana przy pomocy dedykowanego oprogramowania.

V. Szkolenia personelu

1. Każdy pracownik/współpracownik Administratora, przed przystąpieniem do pracy na danych osobowych musi odbyć szkolenie wstępne z zakresu ochrony danych osobowych na zasadach określonych w pkt. 3 niniejszej Polityki.
2. Organizowane są szkolenia okresowe dla pracowników, w celu przekazania najnowszej wiedzy z zakresu ochrony danych oraz przypomnienia obowiązujących zasad.
3. Za przeprowadzenie szkoleń odpowiada IOD.

4. Każde szkolenie musi być udokumentowane listą obecności, na której, poza imionami i nazwiskami jego uczestników z ich podpisami, musi być opisany zakres szkolenia.
5. Inspektor Ochrony Danych przeprowadza szkolenia w miarę potrzeb np. po zmianie przepisów mających znaczenie dla procesów ochrony danych osobowych, wystąpieniu incydentu ochrony danych lub na wniosek Administratora lub samych pracowników.
6. Szkolenie, o którym mowa w pkt 4, może być przeprowadzone w formie kursu multimedialnego lub webinarium.

VI. Postanowienia końcowe

1. **Wykaz dokumentacji składającej się na system ochrony danych w Starostwie, z którą obowiązkowo zapoznają się wszyscy pracownicy upoważnienia do przetwarzania danych zawarto w pkt. 3.4. niniejszej Polityki.**
2. **Kontrolę nad ochroną przetwarzanych danych** osobowych organizuje i nadzoruje Administrator, a w jego imieniu, czynności te może wykonywać upoważniony pracownik lub podmiot zewnętrzny;
3. **Kontrolą mogą zostać objęte** wszystkie komórki organizacyjne i stanowiska pracy przetwarzające dane osobowe;
4. **Polityka Ochrony Danych Osobowych jest dokumentem** wewnętrznym i nie może być udostępnia osobom postronnym w żadnej formie, bez zgody Administratora;
5. **Kierownicy komórek organizacyjnych są zobowiązani zapoznać** z zasadami zawartymi w niniejszej Polityce podległych pracowników oraz inne osoby posiadające upoważnienie do przetwarzania danych, w szczególności stażystów i praktykantów;
6. **Pracownicy zobowiązani są do stosowania** postanowień zawartych w niniejszej Polityce przy przetwarzaniu danych osobowych;
7. **Naruszenie przez pracownika zasad określonych w niniejszej Polityce**, może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym przewidzianym w przepisach prawa;
8. **Pracownik, który celowo lub poprzez zaniedbanie** umożliwia dostęp do danych osobowych osobie, która nie jest do tego upoważniona, w tym także innym pracownikom Administratora, bez uzasadnionej potrzeby, ponosi odpowiedzialność dyscyplinarną i podlega sankcjom karnym przewidzianym w przepisach prawa.
9. **Pracownik, który wykorzystuje informacje o osobach,** do których uzyskał dostęp w związku z pełnioną funkcją, w sposób niezgodny z zakresem wykonywanych obowiązków lub w celach prywatnych, ponosi odpowiedzialność dyscyplinarną i podlega sankcjom karnym przewidzianym w przepisach prawa.
10. **Niedopuszczalne jest uzyskiwanie, ujawnianie lub wykorzystywanie** przez pracownika danych osobowych, w tym także danych innych pracowników, w sposób niezgodny z zakresem własnych obowiązków lub w celach osobistych;

11. **Pracownik naruszający powyższe zasady naraża Administratora** na ryzyko kar finansowych za naruszenie ochrony danych osobowych, w związku z czym orzeczona kara dyscyplinarna, wobec pracownika, nie wyklucza możliwości wniesienia wobec niego sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
12. **W sprawach nieuregulowanych** w niniejszej Polityce, mają zastosowanie przepisy RODO oraz Ustawy.

Starosta Wrzesiński
Anita Kraska

Rejestr czynności przetwarzania danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 1 do Polityki Ochrony Danych

REJESTR CZYNNOŚCI PRZETWARZANIA

Nazwa i dane kontaktowe administratora	
Nazwa	Starosta Wrzesiński
Adres	ul. Chopina 10, 62-300 Września
E-mail	starostwo@wrzesnia.powiat.pl
Telefon	61 640 44 44
Inspektor Ochrony Danych (jeśli powołano)	
Imię i nazwisko	Piotr Kropidłowski
E-mail	iod@comp-net.pl

Data zmiany w RCP	Zakres zmiany

Rejestr czynności przetwarzania danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Nazwa czynności przetwarzania	.....
Cel przetwarzania Art. 30 ust. 1 pkt b	
Kategorie osób Art. 30 ust. 1 pkt c	
Kategorie danych osobowych Art. 30 ust. 1 pkt c	
Podstawa prawna	
Źródło danych	
Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe) Art. 30 ust. 1 pkt f	
Nazwa współadministratora i dane kontaktowe (jeśli dotyczy) Art. 30 ust. 1 pkt d	
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy) Art. 30 ust. 1 pkt d	
Kategorie odbiorców (innych niż podmiot przetwarzający) Art. 30 ust. 1 pkt d	
Nazwa systemu lub oprogramowania	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe) Art. 30 ust. 1 pkt g	
DPIA (jeśli tak, lokalizacja raportu)	
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) Art. 30 ust. 1 pkt e	
Jeśli transfer i art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń Art. 30 ust. 1 pkt e	

Starosta Wrzesiński
Anita Kraska

Obowiązek informacyjny		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 2 do Polityki Ochrony Danych

INSTRUKCJA STOSOWANIA KLAUZULI RODO

1. Wobec osób, których dane są przetwarzane, należy wypełnić obowiązek informacyjny, zgodnie z art. 13-14 RODO;
2. Obowiązek informacyjny wobec osób może być wykonywany poprzez umieszczenie informacji na stanowisku obsługi, dołączenie do druku formularza lub wniosku oraz korespondencji z osobą;
3. Pracownicy upoważnieni do przetwarzania danych są zobowiązani do poinformowania przełożonego o konieczności lub podejrzeniu wystąpienia obowiązku zastosowania klauzuli informacyjnej w związku z realizacją zadania, które jest związane z przetwarzaniem danych osobowych;
4. Pracownik lub przełożony pracownika przygotowuje stosowną klauzulę korzystając ze wzoru wskazanego poniżej;
5. Opracowany wzór zawiera elementy stałe, jak np. oznaczenie Administratora danych, kontakt do Inspektora ochrony danych, opis praw osoby, której dane dotyczą. Pola wymagające uzupełnienia (pkt. 3 klauzuli) w zależności od rodzaju sprawy oraz podstawy przetwarzania danych zostały „wykropkowane", należy podać cel przetwarzania – krótki opis zadania jakie jest realizowane w związku z pozyskaniem danych lub odwołanie do ustawy na podstawie której, dane zadanie jest realizowane, oraz podstawę prawną - czyli konkretny punkt z paragrafu 6 ust. 1 lub 9 ust. 2 RODO;
6. W przypadku wątpliwości lub braku wiedzy co do przygotowania klauzuli pracownik konsultuje się z IOD;
7. Zaleca się, aby każda przygotowana klauzula oraz sposób jej dystrybucji, był zaopiniowany przez IOD;
8. W szczególnych przypadkach, aby zapewnić większą przejrzystość, można skorzystać z warstwowych sposobów informowania (zastosować klauzulę skróconą), w pierwszej kolejności przekazuje się tylko podstawowe informacje, wskazując osobie, której dane dotyczą, w jaki sposób może zapoznać się z pełną informacją wymaganą przez art. 13-14 RODO;
9. Stosowanie klauzul warstwowych powinien zatwierdzić IOD;
10. W przypadku zmian w przepisach prawa należy zweryfikować stosowane klauzule informacyjne w obszarze objętym zmianami, w przypadku wątpliwości zmiany należy konsultować z IOD.

Obowiązek informacyjny		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

WZÓR

Klauzula informacyjna o przetwarzaniu danych osobowych

1. **Administratorem Państwa danych osobowych jest** Starosta Wrzesiński z siedzibą w Starostwie Powiatowym we Wrześni przy ul. Chopina 10, tel. 61 640 44 50, e-mail: starostwo@wrzesnia.powiat.pl
2. **Inspektor ochrony danych.** Możecie się Państwo kontaktować w sprawach dotyczących danych osobowych z wyznaczonym Inspektorem Ochrony Danych pod adresem email: iod@wrzesnia.powiat.pl
3. **Cele i podstawy przetwarzania.** Przetwarzanie danych osobowych jest dokonywane w celu ..... (*opis zadania*), na podstawie ..... (należy wskazać właściwą podstawę z art. 6 ust. 1 lub art. 9 ust. 2 RODO.
4. **Odbiorcy danych osobowych.** W związku z przetwarzaniem danych w celach, o których mowa w pkt 3 Państwa dane mogą zostać udostępnione innym uczestnikom tych postępowań i procedur oraz podmiotom i organom upoważnionym na podstawie przepisów prawa, a także inne podmiotom z którymi administrator posiada umowy o powierzeniu danych.
5. **Okres przechowywania danych.** Państwa dane będą przechowywane przez czas realizacji zadań Administratora wskazanych wyżej, a następnie - zgodnie z obowiązującą u Administratora Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów.
6. **Prawa osób, których dane dotyczą.** Zgodnie z przepisami prawa przysługuje Państwu:
   - prawo dostępu do swoich danych oraz otrzymania ich kopii;
   - prawo do sprostowania (poprawiania) swoich danych;
   - prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
   - prawo do ograniczenia przetwarzania danych;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
7. **Informacja o wymogu zbierania danych.** Podanie przez Państwa danych osobowych jest obowiązkiem wynikającym z przepisów prawa lub warunkiem zawarcia umowy.
8. **Pozyskiwanie danych z innych źródeł.** W przypadku zbierania danych w inny sposób niż od osoby, której dane dotyczą, dane te są pozyskiwane z publicznych rejestrów lub ewidencji albo od innych organów władzy publicznej lub podmiotów wykonujących zadania publiczne lub działających na zlecenie organów władzy publicznej albo od innych uczestników postępowania.
9. **Szczegółowe informacje na temat zasad przetwarzania danych osobowych** przez Administratora w tym opis przysługujących Państwu praw z tego tytułu jest również dostępny w Biuletynie Informacji Publicznej Powiatu Wrzesińskiego.

Starosta Wrzesiński
Anita Kraska

STAROSTA WRZEŚIŃSKI

Załącznik nr 3 do Polityki Ochrony Danych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NR .../.....

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „rozporządzeniem".

Upoważniam Panią/Pana

Zatrudnioną/zatrudnionego/ odbywającą(-ego) staż/praktykę/ wykonującą(-ego) umowę zlecenie* na stanowisku

Do przetwarzania danych osobowych w formie papierowej oraz w ramach nadanych dostępów do systemów informatycznych, służących do przetwarzania danych osobowych u Administratora, w zakresie zgodnym z zakresem obowiązków oraz otrzymanymi poleceniami służbowymi.

Niniejsze upoważnienie traci moc z chwilą ustania stosunku pracy/stażu/praktyki/umowy zlecenia* lub z dniem odwołania upoważnienia.

Zadania i czynności do wykonywania:

- Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu.
- Przestrzeganie przepisów dotyczących ochrony danych osobowych oraz regulacji wewnętrznych, wprowadzonych do stosowania u Administratora.

Września, dnia .....r.

.....
Podpis Administratora

Oświadczam, że zapoznałem(-am) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z rozporządzeniem oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych i zobowiązuję się do ich przestrzegania.
Oświadczam ponadto, że zapoznałem(-am) się z wewnętrzną dokumentacją, wprowadzoną do stosowania u Administratora, w zakresie ochrony danych osobowych.
Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie u Administratora.

.....
Podpis osoby upoważnionej

*) niepotrzebne skreślić

Starosta Wrzesiński
Anita Kraska

STAROSTA WRZESIŃSKI

Ewidencja osób upoważnionych do przetwarzania danych osobowych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 4 do Polityki Ochrony Danych

EWIDENCJA OSÓB

posiadających upoważnienie do przetwarzania danych osobowych w Starostwie Powiatowym we Wrześni

Lp.	*Nazwisko i imię upoważnionego*	*Nr upoważnienia*	*data wystawienia upoważnienia*	*data wygaśnięcia upoważnienia*
1.				
2.				
3.				
...				

Starosta Wrzesiński
Anita Kraska

Klauzula poufności danych osobowych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 5 do Polityki Ochrony Danych

Klauzula poufności danych

Imię i nazwisko
Stanowisko
Seria i numer dowodu osobistego[1]

Oświadczam, że zobowiązuję się do zachowania w tajemnicy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny dostępny sposób, w tym, w szczególności, danych osobowych, do których mogę mieć dostęp, w sposób zamierzony lub przypadkowy, w trakcie wykonywania usługi/ zatrudnienia u Administratora.

Obowiązek ten jest nieograniczony w czasie.

Świadomy praw i obowiązków oświadczam, że znane są mi przepisy:

- dotyczące ochrony danych osobowych - 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 oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych
- art. 266 ustawy z dnia 6 czerwca 1997 r. Kodeks karny „Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."
- art. 267 ustawy z dnia 6 czerwca 1997 r. Kodeks karny „Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."

.....

Data i podpis składającego oświadczenie

[1] Nie dotyczy pracowników etatowych Administratora

Starosta Wrzesiński
Anita Kraska

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____, pomiędzy:

(zwana dalej „**Umową**")

_____

zwany w dalszej części „**Administratorem**",

reprezentowanym przez:

_____

a

_____

zwany w dalszej części „**Podmiotem przetwarzającym**"

(*dane podmiotu, który będzie przetwarzać dane osobowe w imieniu Administratora*),

reprezentowanym przez:

_____

zwane też w dalszej części „**Stronami**"

Niniejsza umowa została zawarta na podstawie przepisów dotyczących 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), zwanego w dalszej części „**Rozporządzeniem**".

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia, dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi RODO określone w § 3 ust. 1 niniejszej Umowy.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie niniejszej Umowy dane. Dane te zostały określone w załączniku nr 1 do umowy.
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu określonym w załączniku nr 1.

§ 3

Obowiązki i prawa Stron

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający określa ogólny opis zabezpieczeń w załączniku nr 1.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych, w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający, po zakończeniu świadczenia usług związanych z przetwarzaniem zobowiązany jest do działania określonego w załączniku nr 1.
6. W miarę możliwości, Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, niezwłocznie zgłasza je Administratorowi, nie później niż w ciągu 48 godzin.
8. Administrator, zgodnie z art. 28 ust. 3 pkt h Rozporządzenia, ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia Umowy.
9. Administrator realizować będzie prawo kontroli, zgodnie z załącznikiem nr 1.
10. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli, w terminie wskazanym przez Administratora.
11. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, określonych w art. 28 Rozporządzenia.

§ 4

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom, jedynie w celu wykonania Umowy, po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający zobowiązuje się do korzystania z usług wyłącznie takich podwykonawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez tych podwykonawców danych osobowych, spełniało wymogi Rozporządzenia.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku, przed rozpoczęciem przetwarzania, Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
6. Podmioty, którym dane Administratora zostały powierzone przez Podmiot przetwarzający, wymienia się w załączniku nr 1.

§ 5

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym

przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, a także:

a) o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego,
b) o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 6

Czas obowiązywania Umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas określony w załączniku nr 1.
2. Każda ze stron może wypowiedzieć niniejszą Umowę, z zachowaniem okresu opisanego w załączniku nr 1.

§ 7

Rozwiązanie umowy

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

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne"). Podjęte zobowiązanie pozostaje w mocy w czasie trwania i po zakończeniu przetwarzania w ramach powierzenia danych osobowych.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora, w innym celu niż wykonania Umowy, chyba że konieczność ujawnienia informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 9

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej, pod rygorem nieważności.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, dla każdej ze Stron.
3. W sprawach nieuregulowanych, zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy, będzie sąd właściwy dla Administratora.

Administrator

Podmiot przetwarzający

Umowa powierzenia przetwarzania danych osobowych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 1

1. Zakres powierzonych danych:

(rodzaje danych osobowych: zwykłe/szczególnej kategorii/dotyczące wyroków skazujących i naruszeń prawa, przykładowe kategorie osób, których dane dotyczą: pracownicy/klienci/kontrahenci Administratora w postaci np. imion i nazwisk/adresów zamieszkania/PESEL)

2. *Cel przetwarzania powierzonych danych*

(np. w celu realizacji umowy z dnia ..... w zakresie świadczenia usług kadrowo-płacowych)

3. *Zastosowane zabezpieczenia – ogólny opis.*

4. *Rodzaj działania z danymi po zakończeniu umowy*

(zwrot/usunięcie, określenie czasu na wykonanie działania)

5. *Kontrola podmiotu przetwarzającego*

(określenie godzin kontroli, określenie czasu na poinformowanie podmiotu przetwarzającego o zamiarze kontroli)

6. *Podmioty podpowierzenia*

(należy wskazać podmioty, pełne nazwy wraz z adresem, którym dane powierzył podmiot przetwarzający)

7. *Okres ważności umowy*

(data obowiązywania umowy)

8. *Okres wypowiedzenia*

(należy określić okres wypowiedzenia)

Umowa powierzenia przetwarzania danych osobowych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 2

Przetwarzający:	
Adres:	
Dane kontaktowe:	

Przygotował	Zatwierdził
data podpis	data podpis

Starosta Wrzesiński jako Administrator danych osobowych, jest zobowiązany na podstawie art. 28 ust. 1 Ogólnego Rozporządzenia o ochronie danych osobowych, do oceny zastosowanych przez podmiot, któremu powierza przetwarzanie danych osobowych, środków techniczno-organizacyjnych dla zapewnienia bezpieczeństwa danym osobowym. Art. 28 ust. 1 RODO - Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.
W związku z powyższym, zwracamy się z prośbą o wypełnienie załączonej ankiety. Ankieta zawiera informację o możliwych do zastosowania środków bezpieczeństwa, prosimy o wskazanie tych środków, które są u Państwa stosowane. Administrator nie warunkuje zawarcia umowy o powierzeniu danych wykazaniem stosowania wszystkich środków łącznie wskazanych w ankiecie. Administrator nie wymaga ujawniania informacji o zabezpieczeniach, które były by dla Państwa poufne lub dotyczyły innych zbiorów niż powierzonych przez Administratora. W przypadku pytań dotyczących ankiety, można skontaktować się z Inspektorem ochrony danych wyznaczonym w Starostwie na adres e-mail: iod@comp-net.pl

Lp.	Pytanie	Odpowiedź *	Uwagi
1	Czy jako podmiot przetwarzający (partner/Serwisant/instalator/firma partnerska) dane osobowe planują Państwo wyznaczyć lub wyznaczyli już Inspektora Ochrony Danych Osobowych (IOD)?	- tak zaplanowano wyznaczenie - tak wyznaczono - nie zaplanowano wyznaczenia (uzasadnienie: np. nie jest wymagane przepisami prawa) - zaplanowano wyznaczenie (kiedy: podać przewidywaną datę)	

Umowa powierzenia przetwarzania danych osobowych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

2	Jeżeli nie planują Państwo wyznaczyć/nie został wyznaczony IOD to proszę o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu....., stanowisko/funkcja...., numer tel.	
3	Czy jako podmiot przetwarzający dane osobowe (partner/Serwisant/instalator/firma partnerska) wprowadzili Państwo środki zabezpieczające (techniczne i organizacyjne), które spełniają wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych? **Prosimy o wskazanie jakie są zastosowane** (np. Polityka Ochrony Danych, szyfrowanie danych, nadanie upoważnień, polityki zarządzania kluczami, system alarmowy, monitoring wizyjny, polityki haseł, inne)	TAK/NIE	Wymienić
6	Czy zobowiązują Państwo podmiot przetwarzający dane/ inne firmy do stosowania odpowiednich zabezpieczeń, środków technicznych i organizacyjnych spełniających wymogi RODO?	TAK/NIE	
7	Jeżeli przekazują Państwo dane poza EOG to na jakiej podstawie prawnej?	TAK/NIE	Wymienić
8	Czy jako podmiot przetwarzający dane osobowe (partner/Serwisant/instalator/firma partnerska) prowadzą Państwo rejestr kategorii czynności dla powierzonych operacji przetwarzania danych osobowych?	TAK/NIE	
9	Czy jako podmiot przetwarzający dane osobowe (partner/Serwisant/instalator/firma partnerska) wdrożyli Państwo procedury dotyczące zarządzania incydentami bezpieczeństwa?	TAK/NIE	
10	Czy jako podmiot przetwarzający (partner/Serwisant/instalator/firma partnerska) wprowadzili Państwo środki zapewniające, że systemy IT używane do przetwarzania danych osobowych są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych?	TAK/NIE	
11	Czy jako podmiot przetwarzający dane realizują Państwo regularne audyty z zakresu bezpieczeństwa danych osobowych? Jeżeli tak to w jakich odstępach czasu odbywają się audyty?	TAK/NIE	Wymienić
12	Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych?	TAK/NIE	

13	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?	TAK/NIE	
14	Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	TAK/NIE	
15	Czy stosuje się szyfrowanie dysków komputerów przenośnych?	TAK/NIE	
16	Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?	TAK/NIE	
17	Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?	TAK/NIE	
18	Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	TAK/NIE	
19	Czy jako podmiot przetwarzający dane osobowe posiadają Państwo aktualny certyfikat ISO 27001?	TAK/NIE	

* Występowanie negatywnych odpowiedzi, nie powodują automatycznie negatywnej oceny przetwarzającego. W rubryce ***Uwagi*** należy wskazać konkretny sposób realizacji lub wyjaśnić powody odstąpienia od stosowania zabezpieczeń/procedur. Po uwzględnieniu charakteru, zakresu oraz sposobu wykonywania umowy powierzenia, dla pozycji ankiety, niemających zastosowania należy wpisać w pole ***Uwagi*** *Nie dotyczy.*

Rejestr umów powierzenia		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 7 do Polityki Ochrony Danych

REJESTR UMÓW
powierzenia przetwarzania danych osobowych

Lp.	*Data zawarcia umowy*	*Oznaczenie podmiotu, z którym zawarta jest umowa powierzenia*	*Zakres powierzenia wynikający z umowy*
1.			
2.			
3.			

Starosta Wrzesiński
Anita Kraska

Rejestr kategorii czynności przetwarzania danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 8 do Polityki Ochrony Danych

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA	
Nazwa i dane kontaktowe podmiotu przetwarzającego	
Nazwa	Starosta Wrzesiński
Adres	ul. Chopina 10, 62-300 Września
E-mail	starostwo@wrzesnia.powiat.pl
Telefon	61 640 44 44
Inspektor Ochrony Danych (jeśli powołano)	
Imię i nazwisko	Kropidłowski Piotr
Dane kontaktowe	iod@comp-net.pl

Rejestr kategorii czynności przetwarzania danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Kategorie przetwarzań	(nazwa kategorii czynności)
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	
Administrator — Nazwa i dane kontaktowe administratora	
Administrator — Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	
Administrator — Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	
Administrator — Inspektor Ochrony Danych administratora (jeśli powołano)	
Czas trwania przetwarzania	
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	
Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	
Podprzetwarzający (podwykonawca) - jeśli dotyczy — Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	
Podprzetwarzający (podwykonawca) - jeśli dotyczy — Kategorie podpowierzonych przetwarzań	

Starosta Wrzesiński
Anita Kraska

Załącznik nr 9 do Polityki Ochrony Danych

Procedura postępowania z prawami osób, których dane dotyczą

1. **Cel procedury**

Procedura przygotowana została w celu ujednolicenia i usystematyzowania realizacji prawa osób

2. **Realizacja praw osób**

2.1. Żadna z osób, których dane dotyczą nie może być w jakikolwiek sposób ograniczana w możliwości skorzystania ze swoich praw i w celu ich realizacji może zgłosić stosowny wniosek do Administratora.

2.2. Osoba musi złożyć pisemny wniosek (lub przesłać informację mailem) o dostęp do informacji. Każdy wniosek (żądanie, zapytanie, skarga, itp.), o którym mowa w pkt. 2.1 może być złożony w każdej formie, a sprawa z nim związana jest dokumentowana i załatwiana zgodnie z obowiązującym w Organizacji systemem kancelaryjno-archiwizacyjnym, chyba że Administrator wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą.

2.3. Po wpłynięciu wniosku należy go zweryfikować pod kątem właściwości merytorycznej - uprawnienia danej osoby do jego złożenia. W przypadku złożenia wniosku przez przedstawiciela osoby, której dane dotyczą należy najpierw zweryfikować prawidłowość reprezentacji.

2.4. Wnioski rozpatruje się wyłącznie, gdy zostały złożone przez uprawnioną osobę, tj. osobę, której dane dotyczą lub osobę właściwie umocowaną.

2.5. Nie udziela się odpowiedzi na zapytania ustne, w tym kierowane telefonicznie, o ile Administrator nie ma możliwości potwierdzenia tożsamości rozmówcy.

2.6. Wnioski rozpatruje się biorąc pod uwagę ich treść, a nie tytuł.

2.7. Każdy wpływający wniosek należy niezwłocznie skonsultować z Inspektorem Ochrony Danych.

2.8. Każdy projekt odpowiedzi na wniosek wymaga przed jego wysłaniem konsultacji z Inspektorem Ochrony Danych.

2.9. Odpowiedzi na wnioski udziela się bez zbędnej zwłoki, najpóźniej w terminie miesiąca od daty otrzymania wniosku. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

2.10. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

2.11. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach

niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

2.12. Działania podejmowane w zakresie obsługi wniosków są wolne od opłat.

2.13. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator może odmówić podjęcia działań w związku z żądaniem.

2.14. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Administratorze.

2.15. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

3. Prawo dostępu:

3.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich.

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

3.3. Administrator nie przekazuje informacji, o której mowa w pkt. 3.1. w przypadku wykonywania zadania publicznego, a szczegóły z tym związane reguluje art. 5 Ustawy z dnia 10 maja 2018 o ochronie danych osobowych.

3.4. Jeżeli przetwarzanie danych nie ma miejsca, Administrator informuje osobę występującą z wnioskiem o nie występowaniu przetwarzania danych jej dotyczących. W tym celu Administrator weryfikuje wszystkie miejsca, w którym może następować przetwarzanie danych (dokumenty papierowe, systemy IT, poczta elektroniczna, itp.).

4. Prawo do sprostowania

4.1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania (poprawienia) dotyczących jej danych osobowych, które są nieprawidłowe.

4.2. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia (np. dla celów uprzedniej weryfikacji prawidłowości i aktualności podawanych danych).

5. Prawo do usunięcia danych

5.1. Osoba, której dane dotyczą, ma prawo żądania od Administratora danych niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z okoliczności, o których mowa w art. 17 ust. 1 RODO:

5.1.1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

5.1.2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania;

5.1.3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

5.1.4. dane osobowe były przetwarzane niezgodnie z prawem;

5.1.5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

5.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego – dane osobowe dziecka (art. 8 ust. 1 RODO).

5.2. Jeżeli upubliczniono dane osobowe, co do których istnieje obowiązek usunięcia, to biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje się rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe w wyniku udostępnienia, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

5.3. Prawo usunięcia danych nie ma zastosowania w przypadkach, gdy przetwarzanie jest niezbędne:

5.3.1. do korzystania z prawa do wolności wypowiedzi i informacji;

5.3.2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

5.3.3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;

5.3.4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;

5.3.5. do ustalenia, dochodzenia lub obrony roszczeń.

6. Prawo do ograniczenia przetwarzania danych

6.1. Osoba, której dane dotyczą, ma prawo zażądać ograniczenia przetwarzania jej danych osobowych w następujących przypadkach:

6.1.1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

6.1.2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

6.1.3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na mocy art. 21 ust. 2 ;

6.1.4. dane osobowe były przetwarzane niezgodnie z prawem;

6.1.5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;

6.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego – zgoda dziecka.

6.2. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

6.3. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

7. Prawo do przenoszenia danych

7.1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez żadnych przeszkód ze strony Administratora, jeżeli:

7.1.1. przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a) RODO) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz

7.1.2. przetwarzanie odbywa się w sposób zautomatyzowany.

7.2. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu Administratorowi, o ile jest to technicznie możliwe.

7.3. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

7.4. Prawo, o którym mowa w pkt. 7.1. nie może niekorzystnie wpływać na prawa i wolności innych.

8. Prawo do sprzeciwu

8.1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych w przypadkach, o których mowa w art. 21 RODO.

9. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych

9.1. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

10. Prawo do wycofania udzielonej zgody na przetwarzanie danych

10.1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. (ust.3 art. 7 RODO).

10.2. W takim przypadku administrator nie ma dłużej prawa przetwarzać danych osobowych w celu objętym oświadczeniem zgody.

10.3. W wyniku odwołania zgody dane przetwarzane w celach objętych zgodą powinny zostać bezpowrotnie usunięte.

Starosta Wrzesiński
Anna Kraska

Załącznik nr 10 do Polityki Ochrony Danych

Ewidencja realizacji praw przez osoby, których danych dotyczą

Lp.	Dane osoby	Rodzaj prawa	Data żądania	Podjęte działania	Uwagi
1					
2					
3					
4					
5					
6					

Starosta Wrzesiński
Anita Kraska

Załącznik nr 11 do Polityki Ochrony Danych

Procedura postępowania w związku z naruszeniami ochrony danych

1. **Naruszenie ochrony danych** - 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. Za naruszenie bezpieczeństwa informacji uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pamięciach flash itp., w formie niezabezpieczonej.
2. **Celem Procedury** jest zdefiniowanie możliwych naruszeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury jest Raport z naruszenia bezpieczeństwa ochrony danych osobowych, stanowiący załącznik do Procedury. Raport opracowuje IOD lub osoba wyznaczona przez Administratora w przypadku stwierdzenia naruszenia ochrony danych osobowych u Administratora. Wszystkie naruszenia są ewidencjonowane, ewidencję prowadzi IOD.
3. **W przypadku stwierdzenia naruszenia**:

3.1. zabezpieczenia systemu informatycznego,

3.2. technicznego stanu urządzeń,

3.3. zawartości zbioru danych osobowych,

3.4. ujawnienia metody pracy lub sposobu działania programu,

3.5. jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

3.6. innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych, należy powiadomić IOD, w razie niemożności zawiadomienia Inspektora, należy powiadomić bezpośredniego przełożonego.

4. **Typowe sytuacje, w których dochodzi do naruszenia ochrony danych osobowych, przedstawia tabela „Wykaz przykładowych naruszeń i sposobu postępowania", stanowiąca załącznik do Procedury.**
5. **Do czasu przybycia na miejsce naruszenia** bezpieczeństwa informacji IOD lub osoby przez niego upoważnionej, należy:

5.1. niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców;

5.2. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej, w celu zabezpieczenia miejsca zdarzenia;

5.3. zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;

5.4. podjąć inne działania, przewidziane i określone w instrukcjach technicznych i technologicznych, stosownie do objawów i komunikatów towarzyszących naruszeniu;

5.5. podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;

5.6. zastosować się do innych instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku;

5.7. udokumentować wstępnie zaistniałe naruszenie;

5.8. nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia, do czasu przybycia osoby upoważnionej.

6. **Po przybyciu na miejsce naruszenia** bezpieczeństwa lub ujawnienia informacji, IOD lub osoba go zastępująca:

6.1. rozpoznaje zaistniałą sytuację i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Administratora;

6.2. może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;

6.3. nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza wewnętrznej struktury Administratora.

7. **Po przywróceniu prawidłowego stanu,** należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia bezpieczeństwa informacji oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

7.1. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.

7.2. Jeżeli przyczyną było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe.

7.3. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje służbowe zgodnie z przepisami.

7.4. Jeżeli przyczyną zdarzenia było włamanie mające na celu pozyskanie bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających, w celu zapewnienia skuteczniejszej ochrony bazy danych.

7.5. Jeżeli przyczyną zdarzenia był zły stan urządzeń lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo – programowe.

8. **Inspektor Ochrony Danych dokumentuje** zaistniały przypadek naruszenia oraz sporządza raport, wg wzoru stanowiącego załącznik do Procedury:

8.1. wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem;

8.2. określenie czasu i miejsca naruszenia i powiadomienia;

8.3. określenie okoliczności towarzyszących i rodzaju naruszenia;

8.4. wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;

8.5. wstępną ocenę przyczyn wystąpienia naruszenia;

8.6. ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego;

8.7. decyzję, co do zgłoszenia naruszenia do Organu Nadzorczego oraz jej uzasadnienie;

8.8. decyzję, co do poinformowania osób, których dane dotyczą, i jej uzasadnienie;

8.9. IOD niezwłocznie przekazuje raport Administratorowi, a w przypadku jego nieobecności - osobie uprawnionej.

9. **Po wyczerpaniu niezbędnych środków doraźnych** po zaistniałym naruszeniu, IOD zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

10. **Zaistniałe naruszenie** może stać się przedmiotem szczegółowej, zespołowej analizy, prowadzonej przez Kierownictwo Administratora, IOD oraz osoby zainteresowane. Analiza ta, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

11. **W ciągu 72 godzin po stwierdzeniu naruszenia**, należy je zgłosić do Organu Nadzorczego. Zawiadomienie to zawiera:

11.1. opis i charakter naruszenia ochrony danych osobowych;

11.2. kategorie i przybliżoną liczbę osób, których dane dotyczą;

11.3. kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

11.4. imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

11.5. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

11.6. opis środków zastosowanych lub proponowanych przez Administratora, celem zaradzenia naruszeniu ochrony danych osobowych, w tym zastosowanych środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

12. **W przypadku, gdy jest mało prawdopodobne**, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, nie zawiadamia się Organu Nadzorczego.

13. **W przypadku, gdy z analizy naruszenia wyniknie**, że naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator, bez zbędnej zwłoki, zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Nie zawiadamia się osób, których dane mogą dotyczyć, jeżeli:

13.1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

13.2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby;

13.3. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik nr 1

Raport nr RRRR/NR z naruszenia ochrony danych osobowych			
Data poinformowania o naruszeniu		*Godzina*	
Data wystąpienia naruszenia		*Godzina wystąpienia naruszenia*	
Osoba powiadamiająca o zaistniałym zdarzeniu (imię i nazwisko, stanowisko służbowe)			
Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia lub nazwa i dane kontaktowe podmiotu przetwarzającego, u którego doszło do naruszenia)			
Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące			
Podjęte działania (korekcja)			
Przyczyny wystąpienia zdarzenia			
Działania korygujące			
Decyzja co do zgłoszenia naruszenia do Organu Nadzorczego oraz jej uzasadnienie			
Data zawiadomienia		*Godzina zawiadomienia*	
Decyzja co do poinformowania osób których dane dotyczą i jej uzasadnienie			
Data zawiadomienia		*Forma zawiadomienia*	
Data i podpis Inspektora Ochrony Danych lub osoby upoważnionej			
Podpis i data zatwierdzenia przez Administratora danych			

Załącznik nr 2

TYPOWE SYTUACJE,
W KTÓRYCH DOCHODZI DO NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Lp.	FORMA NARUSZEŃ	SPOSÓB POSTĘPOWANIA
SPRZĘT I INFRASTRUKTURA IT		
1.	Umożliwienie osobom spoza Organizacji lub podmiotom, z którymi nie ma zawartych umów powierzenia przetwarzania danych osobowych, aby podłączały jakiekolwiek urządzenia do sieci komputerowej, lub dokonywały jakichkolwiek prac na nośnikach pamięci.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI, osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
2.	Umożliwienie osobom spoza Organizacji lub podmiotom, z którymi nie ma zawartych umów powierzenia przetwarzania danych osobowych do przebywania w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI, osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
3.	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych, w ramach pomocy technicznej	Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
4.	Próba nieuzasadnionego przeglądania (modyfikowania), w ramach pomocy technicznej, danych osobowych za pomocą aplikacji w bazie danych, identyfikatorem i hasłem użytkownika.	Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
5.	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Inspektora Ochrony Danych.
DANE OSOBOWE W FORMIE ELEKTRONICZNEJ		
6.	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.

7.	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
8.	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały wykonane przez osoby nieuprawnione. Przerwać działające programy. Niezwłocznie powiadomić ASI, osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
9.	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Inspektora Ochrony Danych. Sporządzić raport.
10.	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać osoby odpowiedzialne za infrastrukturę informatyczną w celu odinstalowania programów. Sporządzić raport.
11.	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać osoby odpowiedzialne za infrastrukturę informatyczną w celu przywrócenia poprzednich parametrów. Sporządzić raport.
12.	Odczytywanie zewnętrznych nośników danych przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać osoby odpowiedzialne za infrastrukturę informatyczną w celu wykonania kontroli antywirusowej. Sporządzić raport.
13.	Próba nieuzasadnionego przeglądania (modyfikowania), w ramach pomocy technicznej, danych osobowych za pomocą zdalnych aplikacji.	Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
14.	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę, odczytującą dane, do zaprzestania czynności, wyłączyć monitor. Sporządzić raport.
15.	Sporządzanie kopii danych na nie służbowych nośnikach danych lub w sytuacjach nieprzewidzianych procedurą.	Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić ASI lub osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.

16.	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić ASI lub osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
DANE OSOBOWE W FORMIE PAPIEROWEJ		
17.	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
18.	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń sporządzić raport.
19.	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport
20.	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych i Inspektora Ochrony Danych. Sporządzić raport.
21.	Udostępnienie danych osobowych osobom nieupoważnionym.	Powiadomić przełożonych i Inspektora Ochrony Danych. Sporządzić raport.
ŚLADY MOGĄCE ŚWIADCZYĆ O MOŻLIWOŚCI NARUSZENIA OCHRONY DANYCH OSOBOWYCH		
22.	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić ASI lub osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
23.	Nieoczekiwane zmiany zawartości bazy danych.	Powiadomić ASI lub osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
24.	Ślady manipulacji przy układach sieci komputerowej lub komputerach. Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić ASI lub osoby odpowiedzialne za infrastrukturę informatyczną oraz Inspektora Ochrony Danych. Sporządzić raport.
25.	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Powiadomić Administratora, Inspektora Ochrony Danych. Sporządzić raport.

Starosta Wrzesiński
Anita Kraska

STAROSTA WRZESIŃSKI

Ewidencja naruszeń ochrony danych		
Wersja: 1.0	Data wprowadzenia:	14 kwietnia 2026 r.

Załącznik nr 12 do Polityki Ochrony Danych

Ewidencja naruszeń ochrony danych

LP.	Data zgłoszenia	Rodzaj naruszenia	Miejsce naruszenia	Data wystąpienia naruszenia	Zawiadomienie UODO	Zawiadomienie osób objętych naruszeniem
1.						
2.						
3.						

Starosta Wrzesiński
Anita Kraska

Instrukcja zarządzania systemami Informatycznymi służącymi do przetwarzania danych osobowych

Niniejsza Instrukcja ma na celu zwiększenie ochrony i bezpieczeństwa danych osobowych w urządzeniach informatycznych w Starostwie Powiatowym we Wrześni.

Urządzeniami informatycznymi nazywamy wszystkie urządzenia elektroniczne służące do przetwarzania danych, ich archiwizacji lub przekazywania, w szczególności: komputer, laptop, tablet, sieć informatyczna, drukarka, telefon komórkowy, pendrive i inne przenośne nośniki danych.

Podstawy prawne:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
3. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.

I. Identyfikacja w systemach informatycznych

1. Każdy z pracowników, który został dopuszczony do przetwarzania danych osobowych w systemach informatycznych, posiada indywidualny login i hasło.
2. Każde hasło należy trzymać w tajemnicy.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie mogą zawierać prywatnych i zawodowych skojarzeń (np. imion, nazwiska, nazw miejscowości, numerów telefonów, dat urodzin itd.)
4. Hasła nie mogą zawierać ustalonej kolejności (np. hasło1, następnie hasło2 itd.).
5. Hasło musi być odpowiedniej długości (co najmniej 12 znaków) oraz zawierać małe i wielkie litery, cyfry lub znaki specjalne. Złożoność hasła oraz częstotliwość zmiany, wynoszącą 90 dni, wymuszają system.
6. Hasła zmieniają użytkownicy samodzielnie, po nadaniu pierwotnego hasła przez administratora.
7. Nie należy używać tego samego hasła, co do celów prywatnych.
8. Przy tworzeniu haseł, można korzystać z następujących zasad:
   a. Łączyć ze sobą dwa słowa, używając jako łącznika dowolnego symbolu, np. CzeRwoNy^GarNek;
   b. Wplatać w hasło znaki specjalne (tj.: !@#$%);
   c. Łączyć i przeplatać znaki dwóch słów, stosując przy tym duże i małe litery, np. czerwony garnek = CeZwRnOyGraEnK12
   d. Tworzyć hasło z błędną pisownią (bądź przy tym konsekwentny), np. mózg = MuSk!
   e. Przeplatać litery dowolnego wyrazu z cyframi, np. flash 9708 = f9L7a0s8H
   f. Stosować duże litery w niekonwencjonalnych miejscach, np. !waRszAwa?
   g. Tworzyć hasło jako zlepek pierwszych liter wyrazów tworzących dłuższą frazę, np. MtRdM! (od: mamy tego roku deszczowy maj).
   h. Zastępować litery cyframi - E=3, A=4, T=7 itd., np. K4$74 (od: kasta).
9. Zabronione jest przeprowadzanie prób łamania haseł, wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

II. Ochrona i bezpieczeństwo danych

1. Podstawowe zasady bezpiecznego przetwarzania danych
   1.1 Dostęp do każdego z profili użytkowników ograniczony jest wyłącznie do jednego pracownika.
   1.2 Dostęp do systemu operacyjnego komputera zabezpieczony jest loginem i hasłem.
   1.3 Zabrania się wynoszenia poza teren Organizacji danych zawartych na nośnikach elektronicznych bez zgody Administratora.
   1.4 Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego, w ramach przydzielonych mu uprawnień systemowych i programowych, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych
2. Ochrona komputera
   2.1 Należy każdorazowo blokować swój komputer odchodząc od stanowiska pracy (np. poprzez ⊞+L);
   2.2 W razie podejrzenia prób włamania do systemu czy pomieszczenia, użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie ASI.
   2.3 Wyłączenie komputera może nastąpić wyłącznie po uprzednim zamknięciu wszystkich aktywnych aplikacji (programów).
   2.4 Na służbowych komputerach może być zainstalowane oprogramowanie pomagające zapewnić bezpieczeństwo, w tym program antywirusowy, programy wykonujące kopie zapasowe danych, programy umożliwiające zdalną aktualizację konfiguracji komputera i zbieranie informacji diagnostycznych. Nie należy wyłączać tych programów, ani ignorować wyświetlanych przez nie ostrzeżeń.
3. Zabezpieczenia danych
   3.1 Nie należy zapisywać żadnych danych Administratora na prywatnych urządzeniach bez jego zgody.
   3.2 Nie należy zapisywać danych prywatnych na urządzeniach informatycznych Administratora. Dotyczy to również danych zawierających nielegalną treść lub naruszających własność intelektualną.
   3.3 Elektroniczne nośniki danych, które zawierają dane osobowe, powinny być przechowywane w zamykanych szafach.
   3.4 Wymagane jest stosowanie szyfrowania na nośnikach służących do zapisu danych osobowych.
4. Poczta e-mail i korzystanie z komunikatorów
   4.1 W przypadku wysyłki wiadomości e-mail, należy sprawdzać czy treść lub załączniki nie zawierają więcej informacji niż jest to konieczne dla odbiorcy.
   4.2 W przypadku wiadomości przesyłanych do kilku odbiorców, należy używać funkcji UDW.
   4.3 Wiadomości, które zawierają dane osobowe lub inne poufne informacje, przekazywane drogą e-mail, powinny być zaszyfrowane. Haseł dostępu, czy kluczy aktywacyjnych do danych, nie można przekazywać tą samą drogą, co danych (np. w kolejnej wiadomości e-mail). Hasło należy przekazywać inny kanałem komunikacji.
   4.4 Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych w zakresie ograniczonym swoimi obowiązkami.

4.5 Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora po uprzednim stosownym zawiadomieniu pracowników zgodnie z przepisami prawa w szczególności Kodeksu Pracy.

4.6 Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

4.7 Niektóre adresy e-mail lub wiadomości przesyłane przez komunikatory mogą być próbą wyłudzenia danych lub nakłonienia do instalacji złośliwego oprogramowania. Nie należy na nie odpowiadać, klikać zawartych w nich linków, ani otwierać załączników, w szczególności gdy: - mamy wątpliwości co do tożsamości nadawcy (na przykład pracownik starostwa lub pracownik innej firmy współpracującej ze starostwem, próbuje kontaktować się z nami z innego konta pocztowego niż zwykle), - wiadomość przysłana została z adresu znanej nam osoby, ale jej treść jest nietypowa i wzbudza podejrzenia, że osoba ta mogła paść ofiarą złośliwego oprogramowania, które wysłało wiadomość w jej imieniu (wiadomości zawierające złośliwe oprogramowanie często przychodzą z adresów osób, które znamy), - wiadomość zawiera pliki wykonywalne lub zaszyfrowane załączniki.

4.8 Korespondencja elektroniczna, prowadzona za pomocą służbowego sprzętu lub kont jest archiwizowana i może być monitorowana, w celu spełnienia wymogów wynikających z przepisów prawa, zapobiegania incydentom bezpieczeństwa i ochrony interesów organizacji.

4.9 Z pracownikami i współpracownikami Starostwa w sprawach służbowych należy kontaktować się tylko za pomocą firmowych środków komunikacji (firmowe konta pocztowe, dopuszczone komunikatory) lub telefonicznie (o ile mamy pewność co do tożsamości rozmówcy). Osoby próbujące wyłudzać dane często zakładają konta pocztowe na nazwisko innego pracownika.

4.10 Należy pamiętać, że socjotechniki (social engineering) są jedną z najczęstszych metod pozyskiwania informacji przez cyberprzestępców. Przykładowo: przestępcy uzyskują dostęp do konta używanego przez jednego z pracowników urzędu (na przykład konta pocztowego lub konta na jednym z portali społecznościowych), a następnie kontaktują się z inną osobą z urzędu w celu wyłudzenia od niej poufnych informacji lub nakłonienia jej do wykonania określonych działań.

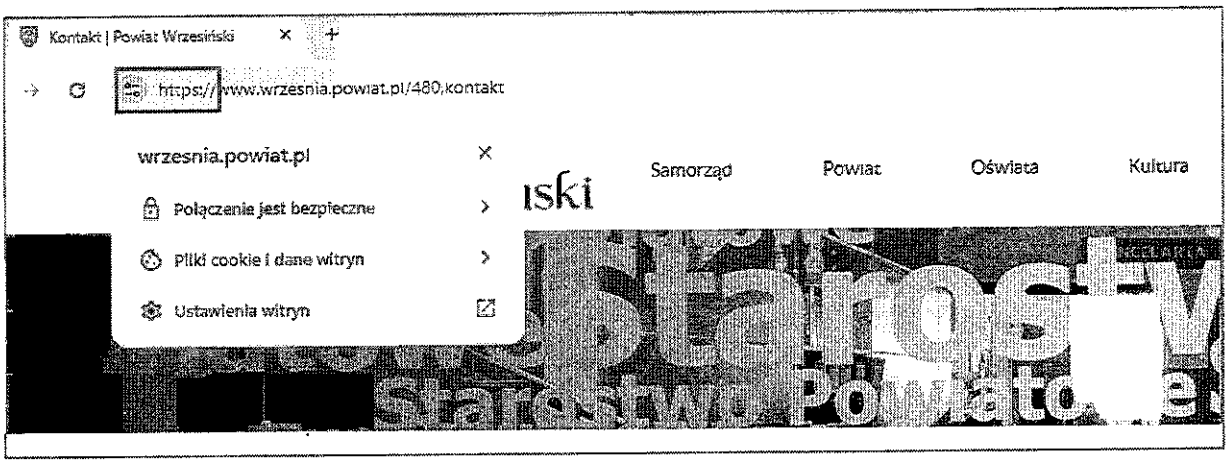
III. Internet

1. Zabrania się korzystania z Internetu w sposób mogący narazić Administratora na jakiekolwiek straty finansowe lub inne.
2. Pracownicy, którzy posiadają dostęp do łączy internetowych, zobowiązani są do ich wykorzystywania wyłącznie w celach służbowych z jednoczesnym zachowaniem dobrych obyczajów i poszanowania praw autorskich i ich dzieł udostępnianych przez sieć Internet.
3. Niedozwolone dla pracownika są samodzielne zmiany konfiguracji stacji roboczych związanych ściśle z przyłączem internetowym oraz ściąganie i instalowanie oprogramowania z Internetu bez zgody ASI nawet w przypadkach, gdy ww. oprogramowanie jest darmowe.

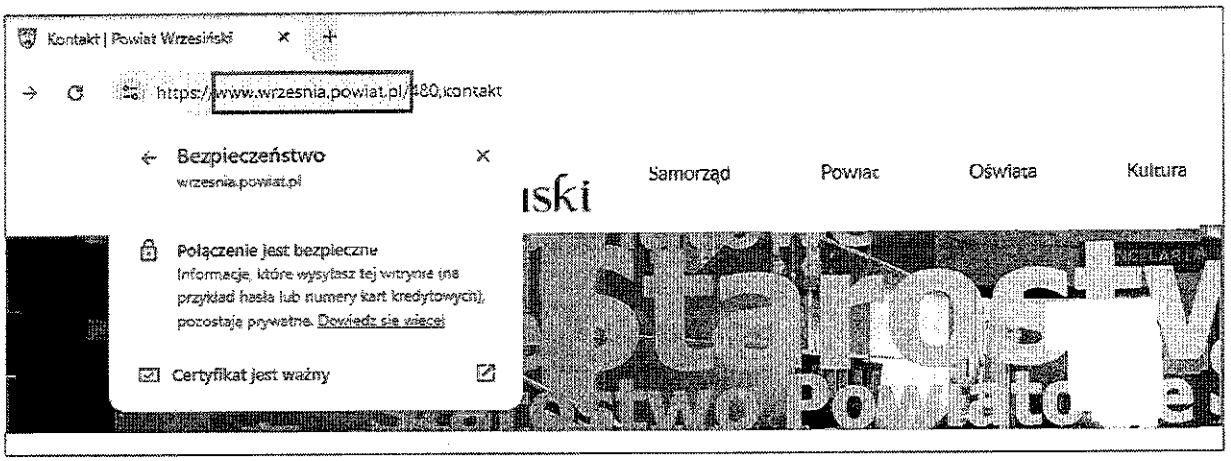
4. Uzyskiwanie dostępu, przeglądanie lub rozprowadzanie niewłaściwych materiałów (np. rozrywkowych, pornografii) poprzez sieć wewnętrzną Administratora lub sieć Internet jest surowo zabronione.

5. Logując się do serwisów internetowych, należy za każdym razem sprawdzać czy:

   - mamy do czynienia z bezpiecznym połączeniem HTTPS, przykład:



   - nazwa domeny wyświetlana w pasku adresu jest prawidłowa, przykład:



6. Nie należy ignorować ostrzeżeń przeglądarki o niepoprawnym certyfikacie SSL lub innych zagrożeniach związanych z odwiedzaną stroną internetową.

IV. Urządzenia mobilne

1. Użytkownik, któremu zostało powierzone urządzenie mobilne, powinien chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu takiego urządzenia.
2. Obowiązkowo należy stosować dostępne metody blokowania dostępu do urządzeń poprzez stosowanie haseł lub innej metody np. rysunku w przypadku smartphone.
3. Obowiązuje zakaz używania urządzenia mobilnego przez osoby inne niż użytkownicy, którym zostały one powierzone.
4. Przy pracy na urządzeniach mobilnych powinno zwrócić się szczególną uwagę na podłączanie ich do nieznanych sieci bezprzewodowych.

V. Kopie bezpieczeństwa i ochrona przed złośliwym oprogramowaniem

1. Pliki zawierające dane osobowe lub inne informacje poufne powinny być zabezpieczone poprzez sporządzenie kopii bezpieczeństwa. Za sporządzanie i bezpieczeństwo kopii danych odpowiedzialny jest ASI lub podmiot zewnętrzny, z którym Administrator zawarł stosowną umowę w tym zakresie.
2. Na wszystkich komputerach jest aktywny program antywirusowy, który chroni je przed zagrożeniami wynikającymi z działania złośliwego kodu.
3. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI.

VI. Zgłaszanie awarii i incydentów bezpieczeństwa

1. W przypadku wystąpienia awarii lub incydentu mogącego mieć wpływ na bezpieczeństwo, należy niezwłocznie powiadomić o nim ASI.
2. Przykłady zdarzeń, które należy zgłosić:
   - nietypowe komunikaty czy dziwne zachowanie się komputera lub telefonu służbowego,
   - brak możliwości logowania na jednym z używanych kont,
   - karta SIM w używanym telefonie przestała łączyć się z siecią komórkową (ktoś nieuprawniony mógł wyrobić duplikat, na przykład, aby przechwycić przychodzące kody SMS),
   - podejrzenie, że osoba postronna mogła uzyskać dostęp do jednego z używanych kont,
   - przypadkowe udostępnienie danych osobowych lub informacji poufnych nieupoważnionej osobie,
   - podejrzane wiadomości otrzymane z konta innego pracownika lub innej osoby.

VII. Odpowiedzialność użytkownika i postanowienia końcowe

1. Przypadki nieuzasadnionego zaniechania przez pracowników obowiązków wynikających z niniejszego dokumentu może być to potraktowane, jako naruszenie obowiązków pracowniczych.
2. Procedury i zasady zawarte w niniejszym dokumencie obowiązują, także stażystów, praktykantów oraz inne osoby, które mają dostęp do przetwarzania danych osobowych u Administratora.