**ZARZĄDZENIE NR 34/2023**
**ZARZĄDU POWIATU NOWOSĄDECKIEGO**

z dnia 27 kwietnia 2023 r.

**w sprawie polityki bezpieczeństwa informacji i ochrony danych osobowych w Starostwie Powiatowym w Nowym Sączu**

Na podstawie § 13 ust. 3 pkt 1 Regulaminu Organizacyjnego Starostwa Powiatowego w Nowym Sączu przyjętego uchwałą Nr 27/IV/2003 Rady Powiatu Nowosądeckiego z dnia 30 stycznia 2003 r. w sprawie zmiany Regulaminu Organizacyjnego Starostwa Powiatowego w Nowym Sączu (z późn. zm.) zarządzam, co następuje:

**§ 1.** Zatwierdzam „Politykę bezpieczeństwa informacji i ochrony danych osobowych" w Starostwie Powiatowym w Nowym Sączu stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

**§ 2.** Zatwierdzam „Księgę systemu zarządzania bezpieczeństwem informacji" w Starostwie Powiatowym w Nowym Sączu stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

**§ 3.** Powołuję „Zespół wdrażający system zarządzania bezpieczeństwem informacji" w Starostwie Powiatowym w Nowym Sączu stanowiący załącznik Nr 3 do niniejszego zarządzenia.

**§ 4.** Upoważniam „Zespół wdrażający system zarzadzania bezpieczeństwem informacji", o jakim mowa w § 3 niniejszego zarządzenia, do aktualizacji „Księgi systemu zarządzania bezpieczeństwem informacji", o której mowa w §2 niniejszego zarządzenia.

**§ 5.** Niniejsze zarządzenia wraz z załącznikami, o których mowa w § 1 i 3 podlegają publikacji w Biuletynie Informacji Publicznej Starostwa Powiatowego w Nowym Sączu. Załącznik Nr 2 nie podlega publikacji w Biuletynie Informacji Publicznej Starostwa Powiatowego w Nowym Sączu, jest dostępny do użytku wewnętrznego w „Intranecie" dla pracowników Starostwa Powiatowego w Nowym Sączu.

**§ 6.** Traci moc zarządzenie Nr 34/2014 Starosty Nowosądeckiego z dnia 11 września 2014 r. w sprawie Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Nowym Sączu.

**§ 7.** Traci moc zarządzenie Nr 25/2018 Starosty Nowosądeckiego z dnia 20 kwietnia 2018 r. w sprawie w sprawie powołania Zespołu do spraw wdrażania obowiązków 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)

**§ 8.** Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Nowosądecki

**Marek Kwiatkowski**

Załącznik Nr 1
do Zarządzenia Nr 34/2023
z dnia 27.04.2023r.
Starosty Nowosądeckiego

# Polityka bezpieczeństwa informacji i danych osobowych

*w Starostwie Powiatowym*
*w Nowym Sączu*

*(Nowy Sącz, kwiecień 2023)*

## §1 Postanowienia ogólne

1. Polityka bezpieczeństwa informacji i danych osobowych (dalej zwana „Polityką Bezpieczeństwa") to zestaw praw, reguł i wewnętrznych praktyk regulujących zarządzanie i ochronę informacji, w tym danych osobowych w Starostwie Powiatowym w Nowym Sączu (dalej zwanym Starostwem).
2. Niniejszy dokument obejmuje zagadnienia związane zabezpieczeniem informacji przetwarzanych zarówno tradycyjnie w postaci papierowych dokumentów, jak i cyfrowo w systemach informatycznych. Polityka Bezpieczeństwa wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych celem zapewnienia właściwej ochrony przetwarzanych informacji.

## §2 Definicje

1. **Administrator lub Administrator Danych Osobowych (ADO)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **Inspektor ochrony danych (IOD)** – osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie prawidłowego przetwarzania danych osobowych i doradzająca w tym zakresie ADO.
3. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. **Bezpieczeństwo informacji** – zachowanie poufności, dostępności, integralności, autentyczności, rozliczalności, niezaprzeczalności, niezawodności informacji.
5. **Poufność danych** – funkcjonalność zapewniająca, że dane są udostępniane wyłącznie upoważnionym podmiotom.
6. **Dostępność –** zapewnienie ciągłego i pewnego dostępu do zasobu wraz z możliwością jego użycia.
7. **Integralność danych** – funkcjonalność zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Niezaprzeczalność** – zapewnienie, zdolność do udowodnienia, że zasób (np. informacje) był jakkolwiek modyfikowany.
9. **Niezawodność** – zapewnienie, iż zasoby (np. systemy obsługujące informacje, procedury etc.), będą spełniały stawiane przed nimi wymagania w zakresie ich działania i funkcjonalności.
10. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
11. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.

12. **Aktywa** – wszystko to, co ma wartość dla organizacji w kontekście informacji, w szczególności zasoby ludzkie, finansowe, organizacyjne, technologiczne i fizyczne, w tym aktywa informacyjne (informacje).
13. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Identyfikator użytkownika** (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
15. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
16. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
17. **Audyt** – niezależna i obiektywna ocena zgodności procesów, procedur, polityk z zadanymi parametrami, normami.
18. **Rozporządzenie (RODO)** – 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).
19. **„Księga systemu zarządzania bezpieczeństwem informacji"** (dalej Księga SZBI) – załącznik Nr 2 do zarządzenia Starosty Nowosądeckiego, które zostało wskazane na pierwszej stronie Polityki Bezpieczeństwa.
20. **„Zespół wdrażający system zarządzania bezpieczeństwem informacji"** (dalej Zespół wdrażający SZBI) – zespół powołany zarządzeniem Starosty Nowosądeckiego, które zostało wskazane na pierwszej stronie Polityki Bezpieczeństwa - w składzie osób wymienionych w załączniku Nr 3 do wskazanego zarządzenia.

## §3 Regulacje prawne

Polityka Bezpieczeństwa uwzględnia w szczególności:

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) (dalej „RODO"),
2. ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych,
3. ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
4. ustawę z dnia 23 kwietnia 1964 r. Kodeks cywilny,
5. ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,

6. przepisy regulujące ochronę danych osobowych, zawarte w aktach wykonawczych do ww. ustaw,
7. kodeksy postepowania, o jakich mowa w art. 40 RODO.

**§4 Deklaracja**

1. Administratorem danych osobowych jest Starosta Nowosądecki.
2. Dane osobowe przetwarzane w Starostwie w ramach realizacji zadań są chronione zgodnie z polskim prawem oraz procedurami dotyczącymi bezpieczeństwa przy ich przetwarzaniu.
3. Administrator mając świadomość, iż przetwarza dane osobowe, dane osobowe szczególnej kategorii, o jakich mowa w art. 6 i 9 RODO, a ponadto dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO, deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
4. Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w motywie 39 RODO oraz art 5 RODO.
5. Każdy pracownik upoważniony do przetwarzania danych, świadomy odpowiedzialności, zobowiązany jest postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich.
6. Wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.
7. Dane osobowe są przetwarzane w Starostwie w sposób legalny, na podstawie art. 6, art. 9 i art. 10 RODO w związku z właściwymi przepisami z zakresu prawa regulującymi zadania i obowiązki samorządu powiatowego bądź w związku z wrażoną zgodą podmiotu danych na przetwarzanie jego danych osobowych.
8. W przypadku konieczności pozyskania zgody na przetwarzanie danych osobowych winna być ona zgodna ze wzorem określnym w Księdze SZBI; zgoda na przetwarzanie danych osobowych o innej treści lub o innym wzorze może zostać pozyskana w dowolny sposób, ale musi ona spełniać przesłanki, o których mowa w art. 7 RODO.
9. Zakres pozyskiwanych danych winien wynikać z przepisów prawa i być adekwatny do zdefiniowanych celów przetwarzania.
10. Okres czasu, przez jaki dane osobowe są przetwarzane, winien być jak najkrótszy, uwzględniać wyrażoną zgodę bądź wynikać z przepisów prawa, w szczególności rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

## §5 Wykaz zbiorów danych (aktyw informacyjnych)

1. Aktywa Starostwa, w tym dane osobowe, są zorganizowane w zbiory, dla których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o której mowa w art. 35 RODO.
2. Zbiory danych osobowych opisane są z uwzględnieniem poniższych informacji:
   a. nazwa zbioru,
   b. rodzaj pomieszczenia, gdzie przetwarzany jest zbiór,
   c. piętro i nr pomieszczenia,
   d. miejsce składowania danych,
   e. opis struktury danych (zbierane dane),
   f. programy, aplikacje służące do przetwarzania danych i sposób przepływu danych między nimi.
3. Szczegółowy wykaz i opis zbiorów danych osobowych zawiera Księga SZBI.

## §6 Wykaz miejsc przetwarzania

1. Obszarem przetwarzania danych są wszystkie budynki, pomieszczenia, korytarze oraz teren przyległy do budynków objęty monitoringiem wizyjnym.
2. Szczegółowy wykaz obszarów, w których przetwarzane są dane osobowe, określny jest w Księdze SZBI, dla pomieszczeń opisano w niej zastosowane środki ochrony.

## §7 Rejestr czynności przetwarzania

1. Dla zbiorów, w których przetwarzane są dane, prowadzony jest rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO.
2. Jedna czynność przetwarzania może obejmować kilka zbiorów, o jakich mowa w §5.
3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, określone w art. 30 ust. 1 RODO tj.:
   a. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
   b. cele przetwarzania;
   c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4. Szczegółowy tryb prowadzenia rejestru czynności przetwarzania określa Księga SZBI.

**§8 Rejestr kategorii czynności przetwarzania**

1. W przypadku powierzenia przez inny podmiot przetwarzania danych, prowadzony jest rejestr wszystkich kategorii czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 2 RODO.
2. Rejestr kategorii czynności przetwarzania winien zawierać co najmniej informacje, określonych w art. 30 ust. 2 RODO tj.:
   a. imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
   b. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
   c. gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
   d. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
3. Szczegółowy tryb prowadzenia rejestru wszystkich kategorii czynności przetwarzania określa Księga SZBI.

**§9 Ewidencja osób upoważnionych do przetwarzania danych osobowych**

1. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
2. Ewidencja zawiera: imię i nazwisko, datę urodzenia osoby upoważnionej, stanowisko, datę nadania, ważności i ustania uprawnień oraz zakres, a w przypadku, kiedy dane są przetwarzane za pomocą aplikacji komputerowej również nazwę tego oprogramowania.
3. Wydanie lub unieważnienie upoważnienia do przetwarzania danych osobowych następuje na piśmie.
4. Sposób prowadzenia ewidencji, wzory rejestru i upoważnień został szczegółowo określony w Księdze SZBI.

## §10 Środki organizacyjne ochrony danych osobowych

1. Przetwarzanie danych osobowych w Starostwie może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień jest ściśle proporcjonalny do tych zadań.
2. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie wydane przez Administratora danych osobowych, o jakim mowa w §9. Wydanie, zmiana lub unieważnienie upoważnienia do przetwarzania danych osobowych następuje na piśmie.
3. Każdy pracownik Starostwa, osoba odbywająca staż lub praktykę w Starostwie, a w szczególności nowoprzyjęty pracownik przechodzi instruktaż przed przystąpieniem do przetwarzania danych. Dąży się do cyklicznych szkoleń zatrudnionych osób z zakresu ochrony danych osobowych, co najmniej raz na dwa lata.
4. Każda osoba upoważniona do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą Polityką bezpieczeństwa, zasadami bezpieczeństwa i świadomości odpowiedzialności za nieprzestrzeganie tych zasad. Wzór oświadczenia w tym zakresie określa Księga SZBI. Podpisany dokument jest dołączany do akt osobowych pracownika lub stanowi załącznik do zawartej umowy.
5. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
6. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
7. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
8. W podmiocie 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 posiadanej dokumentacji lub ewidencji, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.
9. Niedopuszczalne jest przekazywania jakichkolwiek informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.
10. W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. kserokopię akt sprawy, zaświadczenie, postanowienie, decyzję administracyjną, itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w ust. 9, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia.

11. Organizacja rejestracji interesantów i poczekalni dla osób oczekujących na korytarzach i w innych pomieszczeniach winna umożliwiać zachowanie poufności osobom przebywającym bezpośrednio przy rejestracji, w punktach informacyjnych, składającym dokumenty na dzienniku podawczym, bądź załatwiającym sprawę przy stanowisku obsługi.
12. Udzielanie informacji i realizacja usług w Starostwie odbywa się w miejscach specjalnie do tego wyznaczonych. Zabrania się udzielania informacji dotyczących osób i prowadzonych postępowań na korytarzach, w poczekalni lub innych nieprzystosowanych do tego miejscach.
13. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.
14. 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, danego interesanta, stron uczestniczących w postępowaniu administracyjnym, itd. Stosowana jest zasada tzw. czystego biurka.
15. Nie należy gromadzić podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach, o jakich mowa w §5 zgodnie z zasadami określonymi w Księdze SZBI.
16. Dokumenty zawierające dane osobowe należy niszczyć w niszczarkach lub w przypadku dużej ilości dokumentów, korzystać w tym celu z usług profesjonalnych podmiotów, zajmujących się utylizacją dokumentacji.
17. Wobec osób, których dane są przetwarzane wykonuje się obowiązek informacyjny, zgodnie z art. 12-14 RODO, a sposób postępowania w tym zakresie oraz wzór klauzul informacyjnych opisany jest w Księdze SZBI.
18. Obowiązek informacyjny wobec interesantów może być wykonywany poprzez umieszczenie na tablicy informacyjnej w widocznych miejscach w poczekalni, przy stanowiskach obsługi, w punktach informacyjnych i innych tego typu miejscach. Treść klauzul informacyjnych publikuje się na stronie internetowej Starostwa w dedykowanej zakładce lub przy opisach spraw, usług.
19. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
20. Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszary przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
21. Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
22. Komputery, serwery i inne urządzenia, które przetwarzają zbiory osobowe wyszczególnione w Księdze SZBI, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.

23. Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Księdze SZBI.
24. W celu zapewnienia danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego (np. WINDOWS) oraz bezpośrednio do programów przetwarzających dane.
25. Ze wszystkimi współpracującymi podmiotami gospodarczymi, o ile jest to wymagane, należy zawrzeć, zgodnie z art. 28 RODO, umowy powierzenia przetwarzania danych osobowych. W umowach wprowadza się obowiązek zamieszczenia uregulowania odnoszącego się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty. W Starostwie prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia, której wzór określa Księga SZBI.
26. Szczegółowe zasady postępowania w ramach stosowanych środków organizacyjnych przy zabezpieczeniu zbiorów przetwarzanymi elektronicznie określa Księga SZBI.

**§18 Środki techniczne ochrony danych**

1. Starostwo posiada następujący ogólny system zabezpieczeń:
   a. ogólna ochrona budynku – alarm antywłamaniowy, monitoring wizyjny, całodobowy dozór służb ochrony, gaśnice lub systemy ppoż.;
   b. zabezpieczenia okien – pomieszczenia zlokalizowane na parterze lub wyższych kondygnacjach są dodatkowo zabezpieczone poprzez montaż krat, rolet lub szyb antywłamaniowych, zwłaszcza, jeśli istnieje do nich dostęp przez tarasy, dachy niższych budynków, drabiny ppoż. itp.;
   c. zabezpieczenie drzwi – w zależności od kategorii danych i zagrożeń stosowane są drzwi tradycyjne zamykane na klucz lub przeciwpożarowe, zaś w miejscach szczególnie narażonych na zagrożenia (drzwi wejściowe, sekretariaty, księgowość, archiwa, itp.) stosowane są drzwi antywłamaniowe;
   d. zabezpieczenia zbiorów tradycyjnych (papierowych) – w zależności od kategorii danych i zagrożeń do przechowywania danych stosowne są szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych). Dane przeznaczone do zniszczenia niszczy się w specjalistycznych (odpowiedniej kategorii) niszczarkach;
   e. zabezpieczenia zbiorów elektronicznych – dane elektroniczne zabezpiecza poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w systemy antywirusowe i antywłamaniowe (firewall). Kopie danych należy gromadzić w szafach metalowych lub sejfach ognioodpornych.
2. W Księdze SZBI opisuje się dla każdego pomieszczenia indywidualnie, stosowane środki bezpieczeństwa.

4. Środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określono w instrukcjach zarządzania systemami informatycznymi, które są zawarte w Księdze SZBI.

**§11 Udostępnianie danych**

1. Podmiot udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.
2. Dane osobowe, które znajdują się w posiadanej dokumentacji są udostępniane na zasadach, w trybie i w sposób określony w przepisach ustaw i rozporządzeń wykonawczych właściwych dla merytorycznych komórek organizacyjnych Starostwa.
3. Ewidencja udostępnionej dokumentacji prowadzona jest odrębnie w każdej komórce organizacyjnej i zawiera co najmniej: imię (imiona) i nazwisko osoby, której dotyczy udostępniona dokumentacja, sposób udostępnienia dokumentacji, zakres udostępnionej dokumentacji, imię (imiona) i nazwisko lub identyfikator osoby, która udostępniła dokumentację, datę udostępnienia dokumentacji, podpis lub potwierdzeni przyjmującego dokumentację.
4. Wzór ewidencji, o której mowa w ustępie 3 niniejszego paragrafu określa Księga SZBI.
5. Udostępnia się również dane, na innej podstawie niż ta, o której mowa w ustępie 2 niniejszego paragrafu jedynie na uzasadniony, pisemny wniosek i za potwierdzeniem, po uprzedniej konsultacji z IOD.
6. Przesyłając drogą pocztową dokumenty zawierające dane osobowe, przekazuje się je listem poleconym za potwierdzeniem odbioru.
7. W przypadku udostępniania dokumentów za pomocą korespondencji mailowej istnieje obowiązek szyfrowania przekazywanego pliku.
8. Inne zasady i szczegółowy tryb postępowania przy udostępnianiu danych osobowych i przekazywaniu informacji zostały zawarte w Księdze SZBI.

**§12 Administrator systemu informatycznego (ASI)**

1. Dla celów obsługi i zabezpieczenia systemu informatycznego Administrator może powołać Administratora systemu informatycznego i wyznaczyć mu m.in. następujący zakres zadań:
   a. prowadzenie monitoringu przetwarzania danych;
   b. administrowanie systemem informatycznym;
   c. nadawanie uprawnień użytkownikom do systemu informatycznego;
   d. stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej;
   e. kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych;

f. kontrola systemu antywirusowego;
g. kontrola awaryjnego zasilania komputerów;
h. kontrola i wykonywanie kopii awaryjnych;
i. konserwacja oraz uaktualnienia systemów informatycznych;
j. informowanie na bieżąco ADO i IOD o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego;
k. przedstawianie Administratorowi, analizy przetwarzania danych osobowych w systemem informatycznym oraz ewentualne potrzeby w zakresie zabezpieczeń.

2. W przypadku, kiedy ADO nie powołuje ASI wszystkie zapisy w dokumentacji, które odwołują się do ASI są rozumiane jako zapisy dot. ADO.

**§13 Inspektor ochrony danych (IOD)**

1. Z uwagi na zakres przetwarzanych danych oraz obowiązek nałożony na podmioty realizujące zadania publiczne w Starostwie wyznaczony jest inspektor ochrony danych.
2. Za wyznaczenie inspektora ochrony danych odpowiada Administrator.
3. Inspektorem ochrony danych może być osoba, która posiada niezbędną fachową wiedzę na temat prawa i doświadczenie / praktykę w ochronie danych osobowych w sektorze publicznym.
4. Inspektor ochrony danych nie musi być pracownikiem podmiotu.
5. Administrator danych osobowych powiadomi organ nadzorczy – Prezesa Urzędu Ochrony Danych w terminie 14 dni o powołaniu, zmianie bądź odwołaniu inspektora ochrony danych. Dane inspektora ochrony danych są przekazywane organowi nadzorczemu według trybu i za pomocą narzędzi opracowanych i wskazanych przez organ nadzorczy.
6. Administrator jest zobowiązany do udostępnienia danych kontaktowych inspektora ochrony danych w sposób umożliwiający jego identyfikację i kontakt z nim. Poprzez udostępnienie danych inspektora ochrony danych należy rozumieć, co najmniej ich publikację na stronie internetowej Starostwa oraz w widocznym miejscu, w siedzibie urzędu.
7. Administrator ma obowiązek zapewnić inspektorowi ochrony danych możliwość wykonywania jego obowiązków w sposób niezależny i zapewnić mu status, o którym mowa w art. 38 RODO.
8. Zadania inspektora ochrony danych:
   a. informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów regulujących tą materię;
   b. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów;

c. podejmowanie działań zwiększających świadomość personelu Praktyki, inicjowanie i organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania;
d. przeprowadzanie wewnętrznych audytów;
e. udzielanie na żądanie administratora zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
f. współpraca z organem nadzorczym;
g. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

9. Inspektor ochrony danych jest wyznaczony na podstawie odrębnego zarządzenia Starosty Nowosądeckiego.

## §14 Zarządzanie ryzykiem

1. W Starostwie przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.
2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.
4. Analiza ryzyka przeprowadzona jest corocznie dla wszystkich czynności przetwarzania lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych, zgodnie z procedurą przyjętą w Księdze SZBI.
5. Za zarządzania ryzykiem odpowiada Administrator. Zgodnie z trybem ustalonym w Księdze SZBI, Administrator na wniosek Zespołu wdrażającego SZBI wskazuje osoby odpowiedzialne w danym roku za przeprowadzenie analizy ryzyka.
6. Analiza ryzyka winna odbywać się przy udziale inspektora ochrony danych.
7. Wyznaczony zespół, o jakim mowa w ust. 5, ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w Starostwie nie później niż do 31 kwietnia kolejnego roku, za rokiem którego ocena dotyczyła.

## §15 Ocena skutków dla ochrony danych (DPIA)

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 dla ochrony danych osobowych, o której mowa w art. 35 RODO.
2. Ocena skutków dla ochrony danych polega na:
   a. systematycznym opisie planowanych operacji i celów przetwarzania;

b. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów;
c. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu.

3. Ocena skutków dla ochrony danych odbywa się zgodnie z procedurą przyjętą w Księdze SZBI.

### §16 Zasady postępowania w przypadku naruszenia systemu ochrony danych

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z ochroną danych w Starostwie.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest inspektor ochrony danych, a w przypadku jego nieobecności Administrator danych osobowych.
4. Po otrzymaniu takiego powiadomienia inspektor ochrony danych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych IOD podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia Administratora.
6. Po dokonaniu czynności zabezpieczających, IOD ma za zadanie:
   a. przeprowadzić postępowanie wyjaśniające, które ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Starostwa, jak i osób, których dane dotyczyły;
   b. podjąć niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w Starostwie;
   c. opracować działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości;
   d. wskazać osoby odpowiedzialne za wystąpienie sytuacji.
7. Powyższe czynności są dokumentowane przez inspektora ochrony danych w sposób i za pomocą formularzy, które określone zostały w Polityce SZBI.
8. Inspektor ochrony danych, na ile jest to możliwe, ma obowiązek przedstawienia raportu Administratorowi w czasie umożliwiającym powiadomienie o incydencie lub naruszeniu systemu ochrony danych osobowych organu nadzorczego nie później niż na 72 godziny od czasu jego wykrycia.

### §17 Kontrole wewnętrzne i audyty bezpieczeństwa

1. Kontrolą zasad przetwarzania danych osobowych zajmuje się inspektor ochrony danych.

2. Inspektor ochrony danych wykonuje kontrole osobiście, a w uzasadnianych przypadkach, może wnioskować do Administratora o wyznaczenie do przeprowadzenia kontroli innej osoby lub o zlecenie kontroli innemu podmiotowi.
3. Kontrole przeprowadzane są regularnie, na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie. W przypadku wystąpienia incydentu IOD przeprowadza kontrolę doraźną obejmującą wszystkie aspekty działalności w obszarze wystąpienia incydentu, nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił. Wynik kontroli musi być udokumentowany i przekazany administratorowi w ciągu 21 dni od jej zakończenia.
4. Audyty wewnętrzne dot. bezpieczeństwa realizują zespoły audytorów w oparciu o harmonogramy ustalone przez Zespół wdrażający SZBI.
5. Administrator może zlecić badanie audytowe niezależnemu podmiotowi, informuje o tym fakcie inspektora ochrony danych.
6. Kontrole i audyty przeprowadzane są przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postępowania, normami i przepisami wewnętrznymi.
7. Proces kontroli i audytu musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu.
8. Jeśli podczas kontroli lub audytu stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych w Starostwie, kontroler lub audytor niezwłocznie powiadomią o tym fakcie Administratora.
9. Szczegółowy tryb i wzory dokumentów, w tym raportu pokontrolnego określa Księga SZBI.

Załącznik Nr 2
do Zarządzenia Nr 34/2023
z dnia 27.04.2023r.
Starosty Nowosądeckiego

**„Księga systemu zarządzania bezpieczeństwem informacji”**

Dokumentacja dostępna jest na stronie intranetu:

http://int/index.asp?go=szbi/main

wyłączenie do użytku służbowego pracowników Starostwa.

Załącznik Nr 3
do Zarządzenia Nr 34/2023
z dnia 27.04.2023r.
Starosty Nowosądeckiego

**„Zespół wdrażający systemem zarządzania bezpieczeństwa informacji”**

## SKŁAD ZESPOŁU

W skład zespołu wchodzą następujące osoby:

1. Justyna Tokarczyk - Sekretarz Powiatu Nowosądeckiego, jako przewodniczący zespołu
2. Tomasz Czerniec – inspektor ochrony danych
3. Łukasz Świerczek – administrator systemu
4. Janusz Bieniek – audytor wewnętrzny
5. Monika Twardowska – kierownik Zespołu ds. Kontroli i Analiz
6. Karolina Koszut – główny specjalista
7. Beata Mikołajczyk – dyrektor Wydziału Administracyjnego

## ZAKRES ZADAŃ ZESPOŁU

Zespół:

a) inicjuje, koordynuje prace związane z rozwojem i doskonaleniem systemu zarządzania bezpieczeństwem informacji;
b) prowadzi okresowe przeglądy „Księgi systemu zarządzania bezpieczeństwem informacji”;
c) aktualizuje „Księgę systemu zarządzania bezpieczeństwem informacji”;
d) analizuje najpoważniejsze incydenty bezpieczeństwa informacji;
e) nadzoruje realizację procesu analizy ryzyka;
f) promowanie zasad bezpieczeństwa.