SPIS TREŚCI:

1 POLITYKA BEZPIECZEŃSTWA POWIATU SOKOŁOWSKIEGO/STAROSTWA POWIATOWEGO W SOKOŁOWIE PODLASKIM

W celu zaspokojenia potrzeb i oczekiwań podmiotów współpracujących z Powiatem Sokołowskim, społeczności lokalnej oraz innych zainteresowanych stron, związanych z zachowaniem gwarancji bezpieczeństwa i poufności przetwarzanych informacji, Starosta Sokołowski przyjął następującą Politykę Bezpieczeństwa przetwarzania danych osobowych:

1. Jesteśmy świadomi ważności informacji przetwarzanej w Starostwie Powiatowym w Sokołowie Podlaskim i będziemy stwarzać warunki, aby zapewnić jej bezpieczeństwo, w tym również poprzez zabezpieczenie na jej ochronę odpowiednich środków finansowych.
2. Zobowiązujemy się do spełnienia wymagań prawnych związanych z bezpieczeństwem informacji, szczególnie w zakresie przepisów prawnych dotyczących ochrony danych osobowych.
3. Zakresem ochrony objęto wszelkie informacje przetwarzane w Starostwie Powiatowym w Sokołowie Podlaskim w każdej formie i w każdym z miejsc działania jednostki, ze szczególnym uwzględnieniem danych osobowych.
4. Za bezpieczeństwo informacji w Starostwie Powiatowym w Sokołowie Podlaskim odpowiada każdy właściciel zasobów na swoim stanowisku pracy.
5. Zapewnienie bezpieczeństwa przetwarzania danych osobowych koordynuje Inspektor Ochrony Danych.
6. Na podstawie niniejszej Polityki zostały sformułowane poszczególne cele w zakresie bezpieczeństwa informacji, które są realizowane poprzez odpowiednie polityki i inne zabezpieczenia organizacyjno-techniczne, obejmujące w szczególności:
   6.1. Zapewnienie wykształcenia i świadomości pracowników w zakresie bezpieczeństwa informacji a w szczególności ochrony danych osobowych.
   6.2. Zapewnienie ciągłości działania Starostwa Powiatowego w Sokołowie Podlaskim.
   6.3. Zakomunikowanie pracownikom konsekwencji, w tym dyscyplinarnych, w przypadku naruszenia bezpieczeństwa informacji.
   6.4. Raportowanie incydentów związanych z bezpieczeństwem informacji.
7. W Starostwie Powiatowym w Sokołowie Podlaskim dokonano szacowania ryzyka zgodnie z przyjętą metodą i kryteriami akceptacji ryzyka, opisanymi w raporcie z analizy ryzyka, a następnie wdrożono w stosunku do zidentyfikowanych ryzyk stosowne zabezpieczenia, zgodnie z rekomendacjami.
8. Obowiązkiem pracowników Starostwa Powiatowego w Sokołowie Podlaskim jest przestrzeganie zasad postępowania zawartych w RODO oraz udokumentowanych w niniejszej Polityce i w opisie technicznych i organizacyjnych środków bezpieczeństwa przetwarzania danych osobowych.
9. Pracownicy Starostwa Powiatowego w Sokołowie Podlaskim w ramach zdobytej wiedzy dotyczącej ochrony danych osobowych realizują zasady dotyczące ochrony oraz analizują i eliminują błędy w tym zakresie.

Niniejsza Polityka oraz pozostała dokumentacja bezpieczeństwa funkcjonująca w Starostwie Powiatowym w Sokołowie Podlaskim została zaakceptowana przez Starostę oraz zakomunikowana wszystkim pracownikom, którzy zostali zobligowani do ich stosowania.

Nad przestrzeganiem Polityki czuwa Starosta, Wicestarosta, Sekretarz oraz Inspektor Ochrony Danych Osobowych.

2 DEKLARACJA STOSOWANIA

Administrator Danych deklaruje, że przetwarzanie danych osobowych w Starostwie Powiatowym w Sokołowie Podlaskim jest zgodne z mającymi zastosowanie wymaganiami prawnymi.

Deklaracja ta opiera się w szczególności na zapewnieniu, że dane osobowe są:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane w sposób zgodny z tymi celami,
3) adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane,
4) prawidłowe i w razie potrzeby uaktualniane,
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane,
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

3 DEFINICJE

Definicje pojęć używanych w dokumencie:

1. **Rozporządzenie RODO/GDPR** – 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 (GDPR– General Data Protection Regulation).
2. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U.2019.1781).
3. **Dane osobowe** – 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. **Przetwarzanie danych** – 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.
5. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
6. **Administrator Danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

   Tu: Administratorem Danych (AD) jest Starosta Sokołowski, który decyduje o celach i środkach przetwarzania danych osobowych.
7. **Pracownik** - każda osoba dopuszczona do przetwarzania danych osobowych niezależnie od formy zatrudnienia (umowa o pracę, umowa cywilnoprawna, staż, praktyka).
8. **Podmiot przetwarzający** − osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na polecenie Administratora Danych.
9. **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
10. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
11. **Zgoda osoby, której dane dotyczą –** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
12. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

13. **Zabezpieczenie danych** w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
14. **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
15. **Autentyczność** – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy: użytkowników, procesów, systemów i informacji.
16. **Poufność informacji** – rozumiana jest jako zapewnienie, że tylko osoby uprawnione mają dostęp do informacji.
17. **Integralność informacji** – rozumiana jest jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.
18. **Dostępność informacji** – rozumiane jest jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne
19. **Rozliczalność** – rozumiana jest jako zapewnienie możliwości przypisania w sposób jednoznaczny zrealizowanej czynności do określonego podmiotu.
20. **Niezaprzeczalność** – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
21. **Organ nadzorczy** – niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO: **Prezes Urzędu Ochrony Danych Osobowych (PUODO)**.
22. **Kontrolujący** – osoba, o której mowa w art. 79 Ustawy
23. **Inspektor Ochrony Danych**, (**IOD**) – osoba powołana przez Administratora, wykonująca zadania określone w art 39 RODO.
24. **Administrator Systemów Informatycznych,** (**ASI**) – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych – administrator sieci lokalnej, systemów operacyjnych, baz danych, oprogramowania dziedzinowego, narzędziowego i innych.
25. **Serwisant Systemu Dziedzinowego** – osoba fizyczna lub organizacja serwisująca systemy dziedzinowe Administratorowi Danych, niezależna od Administratora Danych, sprawująca nadzór we własnym zakresie nad prawidłowością przetwarzania danych osobowych w serwisowanym rozwiązaniu bądź systemie.
26. **Użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora Danych lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym Starostwa Powiatowego w Sokołowie Podlaskim.
27. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
28. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
29. **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt. 35 ustawy – Prawo telekomunikacyjne.
30. **Sieć publiczna** – publiczna sieć telekomunikacyjna w rozumieniu art. 2 pkt. 29 ustawy – Prawo telekomunikacyjne.
31. **Aplikacja** – program komputerowy wykonujący konkretne zadanie.
32. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

33. **Polityka Bezpieczeństwa** – ogólny dokument deklaracji Administratora w zakresie zobowiązań, zakresu i sposobów realizacji ochrony danych osobowych

4 PRZEDMIOT, CEL I ZAKRES DOKUMENTU.

Niniejszy dokument zawiera opis technicznych i organizacyjnych środków bezpieczeństwa przetwarzania danych osobowych i jest załącznikiem do Rejestru Czynności Przetwarzania Danych Osobowych Powiatu Sokołowskiego, zgodnie z art. 30 ust 1 lit g) 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 (GDPR– General Data Protection Regulation).

Celem dokumentu jest wypełnienie wymogów nałożonych przez ww. rozporządzenie (RODO/GDPR) realizacja zasad bezpieczeństwa i dostosowania postępowania niezbędnego do prawidłowego wypełniania obowiązków Administratora Danych – Starostę Sokołowskiego w zakresie zabezpieczenia danych osobowych, przetwarzanych zarówno tradycyjnie, jak i przy pomocy systemów informatycznych.

Dokument obejmuje swoim zakresem wszystkich pracowników Starostwa Powiatowego w Sokołowie Podlaskim, osoby i podmioty współpracujące oraz interesantów i klientów.

5 ZAKRES ODPOWIEDZIALNOŚCI PRZY PRZETWARZANIU DANYCH OSOBOWYCH.

5.1 Administrator Danych

Administrator odpowiedzialny jest za:

1. Wprowadzenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w organizacji danych osobowych.
2. Dostarczenie niezbędnych zasobów i środków do zapewnienia przetwarzania w zgodności z przepisami.
3. Stosowanie się do wymagań prawnych w obszarze ochrony danych osobowych.
4. Wyznaczenie i odwoływanie IOD oraz wspieranie IOD w wypełnianiu przez niego zadań.
5. Włączanie IOD we wszystkie sprawy dotyczące danych osobowych, niezwłoczne informowanie IOD o wszystkich zdarzeniach dotyczących bezpieczeństwa danych osobowych (art. 38 ust 1. RODO).

5.2 Inspektor Ochrony Danych

1. Inspektor Ochrony Danych odpowiedzialny jest za wypełnianie zadań określonych w art. 39 RODO, a w szczególności:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich 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,
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania zgodnie z art. 35 RODO,
   d) współpraca z organem nadzorczym,
   e) 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,
   f) na podstawie art. 38 ust 4. RODO IOD udziela odpowiedzi i wyjaśnień na pytania osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw,
   g) na podstawie art. 38 ust 6. RODO IOD dodatkowo może wykonywać zadania nadzorcze, doradcze, monitorujące wewnętrzne dokumenty dotyczące bezpieczeństwa; monitorowanie i konsultacje przy aktualizacji rejestru czynności przetwarzania danych osobowych oraz inne zadania mogące poprawić bezpieczeństwo danych.
2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
3. Status Inspektora Ochrony Danych.
   a) Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
   b) Administrator wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania,

c) Administrator zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. IOD bezpośrednio podlega najwyższemu kierownictwu jednostki,
d) IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań,
e) IOD może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

4. Odwołanie lub zmiana Inspektora Ochrony Danych.
   a) IOD nie może być odwołany ani karany przez Administratora za należyte wypełnianie swoich zadań, nie może zostać odwołany ani karany za udzielenie określonego zalecenia dotyczącego bezpieczeństwa danych osobowych, z którym nie zgadza się Administrator,
   b) zgodnie z przepisami, jak w przypadku każdego innego pracownika czy zleceniobiorcy, IOD może zostać odwołany lub ukarany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, ciężkie naruszenie obowiązków),
   c) Administrator zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o każdej zmianie danych IOD oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.
5. Zespół Inspektora Ochrony Danych.
   a) IOD wykonując swoje zadania może korzystać z pomocy zespołu IOD,
   b) skład zespołu IOD oraz zakresy obowiązków członków zespołu określa Inspektor w uzgodnieniu z Administratorem danych.

5.3 Administrator Systemu Informatycznego

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. Administrację środowiskami informatycznymi przeznaczonymi do przetwarzania danych osobowych.
2. Administrację uprawnieniami nadawanymi / modyfikowanymi / odbieranymi do systemów informatycznych przetwarzających dane osobowe.
3. Zapewnienie ciągłości działania systemu informatycznego i optymalizację jego wydajności.
4. Instalację i konfigurację sprzętu i oprogramowania oraz jego aktualizację.
5. Konfigurację i administrację oprogramowaniem systemowym i sieciowym.
6. Identyfikowanie i zgłaszanie do IOD oraz ADO incydentów z obszaru ochrony danych osobowych, w zakresie obsługiwanych systemów informatycznych przetwarzających dane osobowe oraz innych zdarzeń mogących mieć wpływ na bezpieczeństwo danych osobowych.
7. Zapewnienie bezpieczeństwa przechowywanych w systemie teleinformatycznym danych osobowych.

5.4 Osoby przetwarzające

Wszystkie osoby przetwarzające dane osobowe w Starostwie Powiatowym w Sokołowie Podlaskim są odpowiedzialne za:

1. Przetwarzanie danych osobowych zgodnie z posiadanym aktualnie upoważnieniem.
2. Przestrzeganie zasad ochrony danych osobowych określonych w przepisach prawa oraz niniejszej Polityce bezpieczeństwa przetwarzania danych osobowych, w tym:
   a) zapoznanie się przed dopuszczeniem do przetwarzania danych z wyżej wymienionymi dokumentami,
   b) złożenie stosownego oświadczenia potwierdzającego znajomość ich treści, zgodnie z załącznikiem nr 1,
   c) spełnianie wymogu wynikającego z obowiązku informacyjnego, w szczególności poinformowania osoby, której dane dotyczą.
3. Uczestniczenie w obowiązkowych szkoleniach z zakresu ochrony danych osobowych.

4. Bezzwłoczne zgłaszanie IOD wszelkich dostrzeżonych nieprawidłowości w przetwarzaniu danych osobowych.
5. Bezzwłoczne zgłaszanie wszelkich incydentów, nieprawidłowości dostrzeżonych zagrożeń związanych z bezpieczeństwem danych osobowych, wnioskowanie do IOD o potrzebie uzupełnienia lub uaktualnienia Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych.
6. Niezwłoczne usunięcie / zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania.
7. Informowanie IOD o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z IOD umowy o powierzeniu przetwarzania danych osobowych.
8. Zgłaszanie wszelkich planowanych nowych czynności przetwarzania danych w celu przeprowadzenia analizy i oceny ryzyk z tym związanych i ewentualnej oceny skutków oddziaływania.
9. Dołożenia szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie, dla którego zostały zebrane.
10. Identyfikowanie i zgłaszanie do IOD incydentów z zakresu ochrony danych osobowych oraz innych zdarzeń mogących mieć wpływ na bezpieczeństwo danych osobowych.