

Załącznik do zarządzenia nr ¹⁵15/2018
Starosty Lęborskiego
z dnia 25.05.2018 r.

Polityka ochrony danych osobowych w Starostwie Powiatowym w Lęborku

Lębork, 25.05.2018

Spis treści

1. Zakres i podstawa stosowania	3
2. Zawartość	3
3. Odpowiedzialność	3
4. Skróty i definicje	4
5. Ochrona danych osobowych w Urzędzie – zasady ogólne	5
6. Inwentaryzacja	7
7. Rejestr czynności przetwarzania danych osobowych	8
8. Podstawy przetwarzania	9
9. Sposób obsługi praw jednostki i obowiązków informacyjnych	10
10. Obowiązki informacyjne	11
11. Żądania osób	12
12. Minimalizacja	16
13. Bezpieczeństwo	17
14. Przetwarzający	19
15. Eksport danych	20
16. Projektowanie prywatności	20
17. Załączniki	20

1. Zakres i podstawa stosowania

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych w Starostwie Powiatowym w Lęborku” (dalej: **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Starostwie Powiatowym w Lęborku (dalej: Urząd).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s.1).

2. Zawartość

Polityka zawiera:

- a) opis zasad ochrony danych obowiązujących w Urzędzie,
- b) odwołania do załączników uszczegóławiających.

3. Odpowiedzialność

3.1 Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator, tj. kierownik Urzędu.

3.2 Odpowiedzialnymi za nadzór i monitorowanie przestrzegania Polityki są Inspektor Ochrony Danych (dalej: IOD), Sekretarz Powiatu Lęborskiego (dalej: Sekretarz) oraz Administrator Systemów Informatycznych (ASI).

3.3 Odpowiedzialnymi za stosowanie niniejszej Polityki są wszyscy pracownicy Urzędu w zakresie powierzonych im obowiązków, uprawnień, odpowiedzialności, upoważnień i pełnomocnictw.

3.4 Urząd zapewnia zgodność postępowania kontrahentów Urzędu z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Urząd. Zasady powierzenia procesu przetwarzania danych osobowych opisuje Rozdział 14 niniejszej Polityki.

4. Skróty i definicje

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s.1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16 roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Administrator oznacza osobę kierownika Urzędu, który samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający oznacza organizację lub osobę, której Urząd powierzył przetwarzanie danych osobowych (np. zewnętrzna obsługa BHP, usługodawca IT).

Profilowanie oznacza 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.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Danych Osobowych.

RDCP lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Urząd oznacza Starostwo Powiatowe w Lęborku

5. Ochrona danych osobowych w Urzędzie – zasady ogólne

5.1 Filary ochrony danych w Urzędzie:

- (1) **Legalność** – Urząd dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
- (2) **Bezpieczeństwo** – Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
- (3) **Prawa jednostki** – Urząd umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- (4) **Rozliczalność** – Urząd dokumentuje to, w jaki sposób spełnia obowiązek, aby w każdej chwili móc wykazać zgodność.

5.2 Zasady ochrony danych

Urząd przetwarza dane osobowe z poszanowaniem następujących zasad:

- (1) W oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- (2) Rzetelnie i uczciwie (rzetelność);
- (3) W sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- (4) W konkretnych celach i nie „na zapas” (minimalizacja);
- (5) Nie więcej niż potrzeba (adekwatność);
- (6) Z dbałością o prawidłowość danych (prawidłowość);
- (7) Nie dłużej niż potrzeba (czasowość);
- (8) Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3 System ochrony danych

System ochrony danych osobowych w Urzędzie składa się z następujących elementów:

- (1) **Inwentaryzacja danych.** Urząd dokonuje identyfikacji zasobów danych osobowych w Urzędzie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:
 - a) przypadków przetwarzania danych szczególnych i danych karnych;

- b) przypadków przetwarzania danych osób, których Urząd nie identyfikuje (dane niezidentyfikowane);
 - c) przypadków przetwarzania danych dzieci;
 - d) profilowania;
 - e) współadministrowania danymi.
- (2) **Rejestr.** Urząd opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Urzędzie (Rejestr). Rejestr jest narzędziem rozliczania zgodności ochrony danych w Urzędzie.
- (3) **Podstawy prawne.** Urząd zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
- a) Utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
 - b) Inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Urząd przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora lub osoby, której dane osobowe dotyczą.
- (4) **Obsługa praw jednostki.** Urząd spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
- a) **obowiązki informacyjne.** Urząd przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
 - b) **możliwość wykonania żądań.** Urząd weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
 - c) **obsługa żądań.** Urząd zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane;
 - d) **zawiadamianie o naruszeniach.** Urząd stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych oraz Prezesa Urzędu Ochrony Danych Osobowych.
- (5) **Minimalizacja.** Urząd posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
- a) zasady zarządzania **adekwatnością** danych;
 - b) zasady reglamentacji i zarządzania **dostępem** do danych;
 - c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności.

- (6) **Bezpieczeństwo.** Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
- a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
 - c) dostosowuje środki ochrony danych do ustalonego ryzyka;
 - d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych w ramach zarządzania incydentami.
- (7) **Przetwarzający.** Urząd posiada zasady doboru przetwarzających dane na rzecz Urzędu, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
- (8) **Eksport danych.** Urząd posiada zasady weryfikacji, czy Urząd nie przekazuje danych do państw trzecich (czyli poza Unię Europejską, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
- (9) **Privacy by design.** Urząd zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Urzędzie uwzględniają konieczność oceny wpływu zmian na ochronę danych osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji, czy na początku nowego projektu.
- (10) **Przetwarzanie transgraniczne.** Urząd posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. Inwentaryzacja

6.1 Dane szczególne i dane karne

Urząd identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególne lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W chwili zidentyfikowania przypadku przetwarzania danych szczególnych lub danych karnych Urząd postępuje zgodnie z przyjętymi przepisami prawa zasadami w tym zakresie lub w szczególnych

przypadkach w oparciu o zgodę osoby na przetwarzanie takich danych. Całość procesu przetwarzania opiera się o przesłanki określone w art. 9 ust. 2 i art. 10 RODO.

6.2 Dane niezidentyfikowane

Urząd identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane. Do głównych procesów przetwarzania danych niezidentyfikowanych dochodzi w ramach stosowanego monitoringu w miejscach oznaczonych tabliczką informującą o objęciu terenu czy pomieszczeń monitorowaniem.

6.3 Profilowanie.

Urząd identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Urząd postępuje zgodnie z przyjętymi zasadami w tym zakresie. Profilowanie odbywa się wyłącznie po wyczerpaniu przynajmniej jednej z przesłanek art. 22 ust. 2 RODO.

6.4 Współadministrowanie

Urząd identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami. Administrator przy wsparciu IOD w porozumieniu z współadministratorem ustala podział obowiązków ze szczególnym uwzględnieniem realizacji praw przysługujących osobie, której dane dotyczą w tym obowiązku informacyjnego wg założeń art. 13 RODO oraz wskazuje się punkt kontaktowy dla osób, których dane dotyczą. Ustalenia powyższe każdorazowo mają postać zindywidualizowanej umowy w formie porozumienia pisemnego.

7. Rejestr czynności przetwarzania danych osobowych

7.1 RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2 Urząd prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane.

7.3 Rejestr jest jednym z podstawowych narzędzi umożliwiających Urzędowi rozliczanie większości obowiązków ochrony danych.

7.4 W Rejestrze dla każdej czynności przetwarzania danych, którą Urząd uzna za odrębną dla potrzeb Rejestru, Urząd odnotowuje co najmniej:

- (1) nazwę czynności;
- (2) cel przetwarzania;
- (3) opis kategorii osób;
- (4) opis kategorii danych;
- (5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Urzędu, jeśli podstawą jest uzasadniony interes,
- (6) sposób zbierania danych;
- (7) informację o przekazaniu poza EU/EOG;
- (8) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.5 Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”**. Rejestr ma formę pisemną, w tym formę elektroniczną. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Urząd rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Prowadzenie Rejestru powierza się wyznaczonemu pracownikowi w Urzędzie, która w porozumieniu z IDO dokonuje wpisów aktualizacyjnych na wniosek ze strony pracownika Urzędu, który zamierza podjąć przetwarzanie danych w ramach nowego procesu czy nowej kategorii danych. Pracownik Urzędu jest zobligowany do niezwłocznego złożenia takiego wniosku do Sekretarza po uzyskaniu informacji o zmianach na swoim stanowisku pracy w związku z przetwarzaniem danych. Zmiany takie mogą być wymuszone w szczególności nowymi aktami prawa pociągającymi za sobą konieczność realizacji nowych zadań w tym związanych z przetwarzaniem danych. **Załącznik nr 4 do Polityki – „Wzór wniosku o wpis aktualizacyjny do RCPD”** określa zakres minimalny informacji zamieszczanych we wniosku. Wnioski oraz Rejestr przechowuje się wraz z całością dokumentacji wymienionej w Polityce na wyznaczonym stanowisku pracy do wglądu dla pracowników Urzędu, kontrolujących Urząd Ochrony danych Osobowych oraz w uzasadnionych przypadkach do wiedzy osób wnioskujących o taki wgląd.

8. Podstawy przetwarzania

8.1 Urząd dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2 Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, uzasadniony cel Urzędu), Urząd dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.

8.3 Urząd wdraża metody zarządzania zgodami umożliwiając rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS, itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.4 Zgody stanowią część akt spraw i jako takie podlegają nadzorowi. **Załącznik nr 5 do Polityki – „Wzór zgody na przetwarzanie danych”** określa treść zgody na przetwarzanie, co pozwala na uzyskanie zgody od osoby, której dane dotyczą z zachowaniem jej obowiązkowych wg RODO cech, tj. dobrowolności, konkretności, świadomego i jednoznacznego określenia woli osoby.

8.5 Każdy pracownik Urzędu przetwarzając dane osobowe ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Urzędu, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Urzędu.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1 Urząd dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2 Urząd ułatwia osobom korzystanie z praw poprzez różne działania, w tym: zamieszczenie na stroni internetowej urzędu informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z niech w Urzędzie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Urzędem w tym celu, itp.

9.3 Urząd dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4 Urząd wprowadza adekwatne metody identyfikacji i uwierzytelnienia osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. Podstawowym narzędziem identyfikacji i uwierzytelnienia jest wgląd do dokumentu tożsamości osoby, której dane dotyczą, a na rzecz której to osoby ma nastąpić realizacja jej praw i obowiązków informacyjnych.

9.5 W celu realizacji praw jednostki Urząd zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Urząd, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany. Mechanizmy te w szczególności określa dokumentacja techniczna czy podręcznik użytkownika każdego z systemów elektronicznego przetwarzania danych.

9.6 Urząd dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. Obowiązki informacyjne

10.1 Urząd określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

10.2 Urząd informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3 Urząd informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. Udostępnia się osobie treść klauzuli informacyjnej m.in. bezpośrednio w Urzędzie w miejscu uzyskania danych od osoby, drogą komunikacji na odległość (e-mail, telefon) i na stronie internetowej Urzędu. **Załącznik nr 6 do Polityki – „Wzór klauzuli informacyjnej”** określa zawartość merytoryczną dostępną dla osoby, do której bezpośrednio zbiera się dane osobowe.

10.4 Urząd nie informuje osoby o przetwarzaniu jej danych, przy pozyskaniu danych o tej osobie niebezpośrednio od niej, jeśli pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą lub dane

osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.

- 10.5 Urząd określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka informująca o objęciu obszaru monitoringiem wizyjnym).
- 10.6 Urząd informuje osobę o planowanej zmianie celu przetwarzania danych.
- 10.7 Urząd informuje osobę przed uchyleniem ograniczenia przetwarzania danych.
- 10.8 Urząd informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- 10.9 Urząd bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko praw lub wolności tej osoby.

11. Żądania osób

- 11.1 **Prawa osób trzecich.** Realizując prawa osób, której dane dotyczą, Urząd wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnica handlową, dobra osobiste), Urząd może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
- 11.2 **Nieprzetwarzanie.** Urząd informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
- 11.3 **Odmowa.** Urząd informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia i o prawach osoby z tym związanych.
- 11.4 **Dostęp do danych.** Na żądanie osoby dotyczące dostępu do jej danych Urząd informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu

przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

11.5 Kopie danych. Na żądanie Urząd wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

11.6 Sprostowanie danych. Urząd dokonuje sprostowania danych na żądanie osoby. Urząd ma prawo odmówić sprostowania, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Urząd informuje osobę o odbiorcach danych, na żądanie osoby biorąc pod uwagę, że organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są uznawane za odbiorców.

11.7 Uzupełnienie danych. Urząd uzupełnia i aktualizuje dane na żądanie osoby. Urząd ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Urząd nie musi przetwarzać danych, które są Urzędowi zbędne). Urząd może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Urząd procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8 Usunięcie danych. Na żądanie osoby Urząd usuwa dane, gdy:

- (1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
- (2) zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania,
- (3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- (4) dane były przetwarzane niezgodnie z prawem,
- (5) konieczność usunięcia wynika z obowiązku prawnego,
- (6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej).

Urząd określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą poniższe wyjątki:

- a) jeżeli przetwarzanie danych jest konieczne do korzystania z prawa do wolności wypowiedzi i informacji;

- b) jeżeli przetwarzanie danych jest konieczne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa;
- c) jeżeli przetwarzanie danych jest konieczne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- d) jeżeli przetwarzanie danych jest istotne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- e) jeżeli przetwarzanie danych jest konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie;
- f) jeżeli przetwarzanie danych jest konieczne do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Urząd, Urząd podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Urząd informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9 Ograniczenie przetwarzania. Urząd dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
- b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich stosowania,
- c) Urząd nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
- d) Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Urzędu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Urząd przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że 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.

Urząd informuje osobę przed uchycieniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Urząd informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10 Przenoszenie danych. Na żądanie osoby Urząd wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Urzędowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Urzędu.

11.11 Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane przez Urząd w oparciu o uzasadniony interes Urzędu lub o powierzone Urzędowi zadanie w interesie publicznym, Urząd uwzględni sprzeciw, o ile nie zachodzą po stronie Urzędu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

11.12 Sprzeciw przy celach statystycznych. Jeżeli Urząd przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Urząd uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

11.13 Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Urząd na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Urząd uwzględni taki sprzeciw i zaprzestanie takiego przetwarzania.

11.14 Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli urząd przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Urząd zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Urzędu, chyba że taka automatyczna decyzja:

- (1) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Urzędem,
- (2) jest wprost dozwolona przepisami prawa,

(3) opiera się na wyraźnej zgodzie osoby odwołującej się.

12. Minimalizacja

Urząd dba o minimalizację przetwarzania danych pod kątem:

- (1) adekwatności danych do celów (ilość danych i zakresu przetwarzania),
- (2) dostępu do danych,
- (3) czasu przechowywania danych.

12.1 Minimalizacja zakresu

Urząd zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach RODO.

Urząd dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Urząd przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2 Minimalizacja dostępu

Urząd stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresu upoważnień), fizyczne (strefy dostęp, zamykanie pomieszczeń i szaf) i logiczne ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe.

Urząd stosuje kontrolę dostępu fizycznego, m.in. poprzez ograniczenie dostępu do pomieszczeń serwerowni czy archiwum zakładowego.

Urząd dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających w oparciu o wydane upoważnienia do przetwarzania danych oraz ewidencję osób upoważnionych do przetwarzania danych.

Urząd dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż na raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w **Załącznik nr 7 do Polityki – „Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji”**.

12.3 Minimalizacja czasu

Urząd wdraża mechanizmy kontroli cyklu życia danych osobowych w Urzędzie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Urzędu, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się w kopiach zapasowych systemów i informacji przetwarzanych przez Urząd. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. Bezpieczeństwo

Urząd zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Urząd.

13.1 Analiza ryzyka i adekwatność środków bezpieczeństwa.

Urząd przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

- (1) Urząd zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
- (2) Urząd kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają. Kategoryzacja
- (3) Urząd przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Urząd analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Analiza ryzyka jest wykonywana przy udziale Administratora, Sekretarza, IOD, ASI, osoby wyznaczonej w Urzędzie oraz osoby dokonującej czynności przetwarzania danych. Analiza ryzyka dla czynności przetwarzania danych lub ich kategorii jest dokumentowana w **Załączniku nr 13 do Polityki – „Wzór protokołu**

analizy ryzyka". W zakresie oceny wagi zagrożenia ustala się skalę, gdzie 1 oznacza brak przetwarzania danych osobowych, 2 przetwarzanie danych zwykłych, 3 oznacza przetwarzanie danych szczególnych i/lub karnych. W zakresie prawdopodobieństwa wystąpienia zagrożenia ustala się skalę, gdzie 1 oznacza sporadyczne przetwarzanie (do 100 rekordów miesięcznie), 2 oznacza częste przetwarzanie (do 500 rekordów miesięcznie), 3 oznacza bardzo częste przetwarzanie (powyżej 500 rekordów miesięcznie). Mnożnik wagi ryzyka i prawdopodobieństwa jego wystąpienia daje przedziały ryzyka, gdzie wynik od 1 do 2 zwalnia z konieczności prowadzenia oceny skutków przetwarzania danych (DPIA). Wynik od 3 do 4 z udziałem danych szczególnych i/lub karnych skłania do prowadzenia DPIA. Wynik od 6 do 9 bezwzględnie nakazuje przeprowadzenie DPIA. Wynik analizy widnieje w Rejestrze Czynności Przetwarzania Danych w części DPIA, gdzie stwierdza się konieczność przeprowadzenia oceny skutków przetwarzania danych lub brak takiej konieczności.

- (4) Urząd ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym celu Urząd ustala przydatność i stosuje takie środki i podejście, jak:
- (i) pseudonimizacja,
 - (ii) szyfrowanie danych osobowych,
 - (iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 - (iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

13.2 Oceny skutków dla ochrony danych

Urząd dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

Urząd stosuje metodykę oceny skutków przyjętą w Urzędzie w Załączniku nr 14 do Polityki – „Ocena skutków przetwarzania danych”.

13.3 Środki bezpieczeństwa

Urząd stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz oceny skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Urzędzie i są bliżej opisane w procedurach przyjętych przez Urząd dla tych obszarów.

13.4 Zgłaszanie naruszeń

Urząd stosuje zapisy art. 33 i 34 RODO w identyfikacji, ocenie i zgłoszeniu zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia oraz powiadomienia osób, których dotyczyło naruszenie ochrony danych. W celu udokumentowania nadzoru nad zgłaszaniem naruszeń ochrony danych w Urzędzie stosuje się **Załącznik nr 15 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa”**.

14. Przetwarzający

Urząd posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Urzędu opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw Jednostki i innych obowiązków ochrony danych spoczywających na Urzędzie.

Urząd przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**, a każda umowa jest odnotowana w **Załączniku nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych”**. Proces do realizacji i nadzoru powierzono pracownikowi wyznaczonemu w Urzędzie, a każdy pracownik Urzędu, który zamierza zawrzeć z podmiotem zewnętrznym umowę skutkującą powierzeniem danych powinien powiadomić o tym fakcie Sekretarza, który konsultując się z IOD i wspólnie z Inspektorem i osobą wyznaczoną w Urzędzie przygotowuje treść umowy powierzenia przetwarzania danych, a po jej podpisaniu osoba wyznaczona w Urzędzie odnotowuje ją w ewidencji umów powierzenia. Administrator może zlecić IOD przeprowadzenie weryfikacji wykonywania umowy powierzenia przez podmiot przetwarzający.

Urząd rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad umowy powierzenia danych osobowych.

15. Eksport danych

Urząd rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Urząd okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

16. Projektowanie prywatności

Urząd zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i inwestycji przez Urząd odwołują się do zasady bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

17. Załączniki

Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”

Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”

Załącznik nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych”

Załącznik nr 4 do Polityki – „Wzór wniosku o wpisanie czynności do RCPD”

Załącznik nr 5 do Polityki – „Wzór zgody na przetwarzanie danych”

Załącznik nr 6 do Polityki – „Wzór klauzuli informacyjnej”

Załącznik nr 7 do Polityki – „Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji”

Załącznik nr 8 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie upoważnienia do przetwarzania danych osobowych”

Załącznik nr 9 do Polityki – „Ewidencja osób upoważnionych do przetwarzania danych osobowych”

Załącznik nr 10 do Polityki – „Wzór upoważnienia do przetwarzania danych osobowych”

Załącznik nr 11 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym”

Załącznik nr 12 do Polityki – „Wzór klauzuli poufności”

Załącznik nr 13 do Polityki – „Wzór protokołu analizy ryzyka”

Załącznik nr 14 do Polityki – „Ocena skutków przetwarzania danych”

Załącznik nr 15 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa”.