LUBUSKI
URZĄD WOJEWÓDZKI

Załącznik nr 1
do zarządzenia
Wojewody Lubuskiego
z dnia 25 maja 2018 roku

ZATWIERDZAM

Władysław Dajczak
Wojewoda Lubuski

POLITYKA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W LUBUSKIM URZĘDZIE WOJEWÓDZKIM
W GORZOWIE WIELKOPOLSKIM

---

wersja 1.0

HISTORIA ZMIAN

Nr wersji	Data	Opis	Działanie (*)	Rozdziały(**)	Autorzy
1.0		Utworzenie nowego dokumentu	N	W	P. Pikuła. M. Piaskowski.
			W	W	G. Krzeski, K. Jankowiak A. Szymczak, A. Ladowski.

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja

(**) Rozdziały: numery rozdziałów lub W-Wszystkie

Spis treści

SPIS ZAŁĄCZNIKÓW:

Słownik pojęć i skrótów

Termin / skrót	**Wyjaśnienie/opis**
ADO	administrator danych osobowych – Wojewoda Lubuski
AS	administrator systemu – kierownik oddziału ds. informatyki
Polityka	oznacza niniejszą Politykę ochrony danych osobowych Lubuskiego Urzędu Wojewódzkiego
RODO	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. Urz. UE L 119, s. 1).
IOD	inspektor ochrony danych – osoba powołana przez ADO
Kierownik komórki	kierownik komórki – dyrektor wydziału lub biura, Lubuski Wojewódzki Inspektor Nadzoru Geodezyjnego i Kartograficznego, Audytor Wewnętrzny, Pełnomocnik ds. Ochrony Informacji Niejawnych, kierownik Delegatury Lubuskiego Urzędu Wojewódzkiego
LUW	Lubuski Urząd Wojewódzki w Gorzowie Wielkopolskim
Osoba upoważniona	osoba, która upoważniona została na piśmie do przetwarzania danych osobowych przez administratora danych lub osobę wyznaczoną do wydawania odpowiedniego upoważnienia
SZBI	system zarządzania bezpieczeństwem informacji obowiązujący w LUW w rozumieniu Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113).
EU/EOG	państwa należące do Unii Europejskiej/Europejskiego Obszaru Gospodarczego

Prezes Urzędu	Prezes Urzędu Ochrony Danych Osobowych
Organ nadzorczy	Urząd Ochrony Danych Osobowych
Ustawa	ustawa o ochronie Danych Osobowych z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. 2018 poz. 1000
System informatyczny administratora	rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych.
integralność	właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany
poufność	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom
dostępność	właściwość zapewniająca, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie
zbiór danych	uporządkowany zestaw danych osobowych, o którym mowa w art. 4 RODO pkt. 2, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

I. Wstęp

Polityka Bezpieczeństwa Danych Osobowych w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp. ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Niniejszy dokument jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, s. 1).

II. Postanowienia ogólne

1. Cele Polityki Bezpieczeństwa Danych Osobowych

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, niniejsza Polityka ma na celu zapewnić odpowiednie środki, aby przetwarzanie odbywało się zgodnie z RODO.

2. Zakres stosowania

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. stażystów, praktykantów. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń IOD.

Z systemów informatycznych służących do przetwarzania danych osobowych znajdujących się w posiadaniu ADO mogą korzystać również inne podmioty, na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych

na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźnie zdefiniowanie celu i zakresu oraz wskazanie odpowiedzialności.

3. Ogólne zasady dotyczące przetwarzania danych osobowych

Administrator Danych przetwarza dane osobowe z poszanowaniem zasad wyrażonych w art. 5 RODO. Dane osobowe muszą być:

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 nieprzetwarzane dalej w sposób niezgodny 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.

III. System obsługi praw jednostki

Administrator danych zapewnia obsługę praw osób, których dane dotyczą poprzez:

1) wdrożenie zasad przekazywania prawem wymaganych informacji przy pozyskiwaniu danych;
2) wdrożenie zasad, w zakresie realizacji żądań osób, których dane dotyczą w terminach i w sposób wymagany w RODO oraz zapewnienie dokumentacji realizacji tego obowiązku;
3) wdrożenie procedur pozwalających na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych;

4) poszanowanie oraz ochronę praw i wolności osób trzecich.

IV. Przypisanie ról i organizacja procesów przetwarzania danych osobowych

ADO wyznacza role oraz odpowiedzialność poszczególnych osób realizujących zadania w procesie przetwarzania danych osobowych.

1. Administrator danych osobowych

Administrator danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) wdraża adekwatne, proporcjonalne oraz skuteczne środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO; przez odpowiednie środki rozumie się w szczególności:
   a. zatwierdzone kodeksy postępowania (o ile zostały wdrożone);
   b. certyfikację (o ile została dokonana na podstawie kryteriów certyfikacji, o których mowa w RODO przez Prezesa Urzędu lub podmiot certyfikujący zgodnie z wymogami Ustawy);
   c. wytyczne oraz opinie Europejskiej Rady Ochrony Danych;
   d. wytyczne Prezesa Urzędu;
   e. sugestie inspektora ochrony danych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi powierzonych im obowiązków (wzór upoważnienia - załącznik Nr 2);
3) wyznacza inspektora ochrony danych oraz określa zakres jego zadań i czynności i zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
4) zleca Dyrektorowi Generalnemu LUW, by we współpracy z administratorem systemu oraz inspektorem ochrony danych zapewnił użytkownikom odpowiednie warunki pracy umożliwiające bezpieczne przetwarzanie danych;
5) podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia procedur

bezpiecznego przetwarzania danych osobowych.

2. Inspektor Ochrony Danych

Inspektor ochrony danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) informuje 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;
2) monitoruje przestrzeganie RODO, innych przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków;
3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpracuje z organem nadzorczym;
5) pełni funkcję 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;
6) pełni rolę punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;
7) opiniuje wzory dokumentów dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne administratora danych;
8) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji – załącznik Nr 3) oraz ewidencję oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (wzór oświadczenia – załącznik Nr 4);
9) na podstawie otrzymanych informacji z komórek organizacyjnych Urzędu, aktualizuje rejestr czynności oraz rejestr kategorii czynności;

10) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, występuje z wnioskiem do ADO o nadanie upoważnienia do przetwarzania danych osobowych;

11) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, występuje z wnioskiem do AS o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;

12) prowadzi rejestr zasad, instrukcji oraz procedur zatwierdzonych lub wycofanych przez ADO będących uzupełnieniem niniejszej Polityki;

13) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych.

3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na podstawie otrzymanych zgłoszeń z komórek organizacyjnych Urzędu, przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników;

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego ADO;

6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

7) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

8) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii

zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

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

10) prowadzi ewidencję identyfikatorów do stanowisk roboczych poszczególnych użytkowników;

11) na podstawie otrzymanych informacji z komórek organizacyjnych Urzędu, prowadzi wykaz systemów informatycznych niepodlegających zasadom, bezpieczeństwa ochrony danych, określonym w LUW.

4. Kierownicy komórek

1) zobowiązani są do zapewnienia działań zgodnych z prawem w ramach powierzonej komórki organizacyjnej;

2) zobowiązani są do stałego nadzoru i stosowania środków mających na celu zapewnienie bezpieczeństwa powierzonego im zasobu;

3) zobowiązani są zapewnić, aby przetwarzane w ramach powierzonej im komórki organizacyjnej dane były aktualne, adekwatne, stosowne oraz ograniczone do tego co niezbędne w stosunku do celów, w jakich są przetwarzane, a także przetwarzane nie dłużej niż jest to koniczne do realizacji celu;

4) zobowiązani są do realizacji obowiązku informacyjnego oraz o ile to możliwe dokumentowania tej czynności;

5) zobowiązani są do niezwłocznej konsultacji z IOD wszelkich żądań osób, których dane dotyczą i sposobu ich realizacji;

6) zobowiązani są do prowadzenia ewidencji zgłoszonych żądań wraz ze wskazaniem sposobu ich realizacji w zakresie powierzonej komórki organizacyjnej;

7) zobowiązani są do dokumentowania i przechowywania zgód na przetwarzanie danych osobowych;

8) zobowiązani są do zgłoszenia IOD wszystkich przypadków nienależytego

zabezpieczenia danych osobowych;

9) za pośrednictwem IOD występują z wnioskiem do ADO o wydanie, modyfikację lub uchylenie upoważnień do przetwarzania danych osobowych dla podległych im pracowników;

10) zobowiązani są zapewnić, aby podległe im osoby upoważnione do przetwarzania danych osobowych posiadały dostęp wyłącznie do zasobów niezbędnych do realizacji powierzonych obowiązków;

11) zobowiązani są do niezwłocznego informowania IOD o wszystkich zmianach przepisów, mających wpływ na sposób, cele lub zakres przetwarzania danych osobowych w podległej komórce organizacyjnej;

12) w procesie zarządzania zmianami organizacyjnymi lub technologicznymi mającymi wpływ na sposób, cele lub zakres przetwarzanych danych osobowych zobowiązani są do konsultacji nowych rozwiązań z IOD oraz AS w fazie projektowania;

13) zapewniają funkcjonowanie systemów informatycznych niepodlegających zasadom bezpieczeństwa LUW w ramach powierzonych komórek organizacyjnych zgodnie z dokumentacją opisującą zasady działania w/w systemów;

14) odpowiadają za dopełnienie obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych w przypadku, gdy występują w roli osoby wnioskującej o udzielanie zamówienia publicznego. Zasady realizacji zamówień publicznych regulują odrębne regulacje administratora danych.

5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do przestrzegania następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) ma obowiązek zachowania tajemnicy danych osobowych oraz przestrzegania

procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych *obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji*;

3) bierze udział w szkoleniach i zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych, postanowieniami niniejszej Polityki oraz SZBI;

4) stosuje określone przez ADO procedury i zasady mające na celu zgodne z prawem przetwarzanie danych;

5) korzysta z systemu informatycznego ADO w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

V. Podstawowe standardy

1. Szkolenia w zakresie ochrony danych osobowych

IOD zakłada następujący plan szkoleń:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych;

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku znaczących zmian zasad lub procedur ochrony danych osobowych;

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

2. Projektowanie zmian

ADO uwzględnia konieczność oceny wpływu projektowanych zmian na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany.

3. Środki bezpieczeństwa

1) Środki ochrony danych dostosowuje się do skali ryzyka w oparciu o metodykę przyjętą w dokumentacji SZBI na podstawie:
   a. procesu szacowania ryzyka uwzględniającego czynności przetwarzania danych oraz kategorie czynności,
   b. oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   c. metod postępowania z ryzykiem.
2) ADO stosuje adekwatne standardy w celu zapewnienia bezpieczeństwa fizycznego i środowiskowego pomieszczeń LUW, w których przetwarzane są informacje oraz przechowywane są urządzenia je przetwarzające zgodnie z dokumentacją SZBI, m.in.: wydziela strefy bezpieczeństwa, reguluje zasady kontroli dostępu, zapewnia fizyczną ochronę obiektu, wdraża zasady minimalizacji ryzyka wynikającego z przyczyn środowiskowych, ustala wymagania bezpieczeństwa dla obszarów przetwarzania danych osobowych, wdraża zasady reglamentacji i zarządzania dostępem do danych.
3) ADO zapewnia poufność, integralność, dostępność systemów i usług przetwarzania oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego zgodnie z zasadami i procedurami przyjętymi w dokumentacji SZBI,
4) ADO zapewnia regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania zgodnie z zasadami i procedurami przyjętymi w dokumentacji SZBI,
5) ADO weryfikuje podmioty przetwarzające dane na jego rzecz, w zakresie możliwości zapewnienia adekwatnego poziomu bezpieczeństwa oraz zapewnia odpowiednie mechanizmy kontroli w/w podmiotów.
6) ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu (Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych – załącznik Nr 1).

4. Inwentaryzacja danych i prowadzone rejestry

1) Przetwarzane przez ADO dane osobowe powinny być poddawane przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zwrócić się do ADO o zarządzenie dodatkowej inwentaryzacji:

a. inwentaryzację przetwarzanych danych osobowych przeprowadza się uwzględniając wszystkie zidentyfikowane czynności przetwarzania przynajmniej pod kątem czynności, celów przetwarzania, kategorii osób, kategorii danych, podstaw prawnych przetwarzania, sposobów zbierania danych, kategorii odbiorców danych, przekazywania poza EU/EOG lub do organizacji międzynarodowych, środków technicznych i organizacyjnych ochrony danych, weryfikacji podstaw prawnych przetwarzania;

b. IOD może zarządzić przeprowadzenie dodatkowej inwentaryzacji w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

2) Rejestr czynności przetwarzania oraz rejestr kategorii przetwarzania zawierają informacje, o których mowa w art. 30 RODO i służą monitorowaniu przez ADO czynności, celów przetwarzania, kategorii osób, kategorii danych, podstaw prawnych przetwarzania, sposobów zbierania danych, kategorii odbiorców danych, przekazywania poza EU/EOG, środków technicznych i organizacyjnych ochrony danych.

3) Administrator danych wdraża:
   a. zasady zarządzania adekwatnością (zakresem) danych,
   b. zasady zarządzania okresem przechowywania danych.

5. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia.

VI. Przeglądy Polityki

1) Polityka bezpieczeństwa danych osobowych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD informacji może zwrócić się do ADO o zarządzenie przeglądu

polityki bezpieczeństwa stosownie do potrzeb.

2) IOD analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
    a. zmian w systemach informatycznych administratora danych,
    b. zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
    c. zmian w obowiązującym prawie.
3) IOD po uzgodnieniu z ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z AS. Zakres, przebieg i rezultaty audytu są dokumentowane.

VII. Postanowienia końcowe

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem w zakresie koniecznym do wykonywanych obowiązków oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2) W zakresie nieuregulowanym niniejszą Polityką stosuje się zasady określone w Systemie Zarządzania Bezpieczeństwem Informacji Lubuskiego Urzędu Wojewódzkiego (SZBI).
3) Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem 25 maja 2018 r.