Zarządzenie Nr ..... 17 /2018
Starosty Elbląskiego

z dnia ..... 18 grudnia 2018 roku

w sprawie ochrony danych osobowych oraz dokumentacji ochrony danych osobowych w Starostwie Powiatowym w Elblągu

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (t.j. Dz.U z 2018r. poz. 995, z późn. zm.), art. 24 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j.: Dz. U. z 2016 r., poz. 922), art. 9 pkt. 1 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U z 2018r. poz. 1000) oraz § 3 ust. 1 i 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., nr 100, poz. 1024) zarządza się, co następuje:

§ 1

1. Dla zapewnienia ochrony danych osobowych w dniu 25 maja 2018r. wyznaczono w Starostwie Powiatowym w Elblągu Inspektora Danych Osobowych (IOD).
2. W poszczególnych Wydziałach i komórkach organizacyjnych za bezpieczeństwo przetwarzania danych osobowych odpowiedzialni są Sekretarz Powiatu, Skarbnik Powiatu, Naczelnicy Wydziałów, Kierownicy, samodzielne stanowiska oraz pracownicy przetwarzający dane osobowe.

§ 2

1. W celu ustalenia zasad postępowania w procesach przetwarzania danych osobowych oraz ochrony interesów osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych w starostwie Powiatowym w Elblągu, wprowadza się jako obowiązującą dokumentację bezpieczeństwa informacji.
2. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Urzędzie jest zobowiązana do zapoznania się z dokumentacją bezpieczeństwa informacji.

§ 3

W zakres dokumentacji bezpieczeństwa informacji wchodzą w szczególności:

1) „Polityka ochrony danych" - stanowiąca załącznik nr 1 do niniejszego Zarządzenia;
2) „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" - stanowiąca załącznik nr 2 do niniejszego Zarządzenia;
3) „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych" - stanowiąca załącznik nr 3 do niniejszego Zarządzenia.

§ 4

Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 5

Traci moc:

1) Zarządzenie nr 3/2017 r. Starosty Elbląskiego z dnia 17 maja 2017 roku w sprawie ochrony danych osobowych w Starostwie Powiatowym w Elblągu oraz dokumentacji bezpieczeństwa informacji w Starostwie Powiatowym w Elblągu,

§ 6

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 25 maja 2018r.

STAROSTA ELBLĄSKI

mgr Maciej Romanowski

Załącznik nr 1
do Zarządzenia Nr 17/2018
Starosty Elbląskiego z dnia 18 grudnia 2018 r.

POLITYKA OCHRONY DANYCH

§ 1

Administratorem Danych Osobowych (ADO) w Starostwie Powiatowym w Elblągu jest Starostwo Powiatowe w Elblągu reprezentowane przez Starostę Elbląskiego.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

1) Urzędzie - należy przez to rozumieć Starostwo Powiatowe w Elblągu;
2) Ustawie - należy przez to rozumieć ustawy o ochronie danych osobowych;
3) Rozporządzeniu - należy przez to rozumieć rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
4) RODO – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
5) UODO – Urząd Ochrony Danych Osobowych, ul Stawki 2, 00-193 Warszawa reprezentowany przez Prezesa Urzędu;
6) IOD – Inspektor Ochrony Danych w Starostwie Powiatowym w Elblągu, ul. Saperów 14A, 82-300 Elbląg.

§ 3

1. Osoby, które przetwarzają dane osobowe, winny posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik nr 1 do Polityki ochrony danych.
2. Poza pracownikami, o których mowa w ust. 1 dostęp do danych osobowych podlegających ochronie posiadają: Wicestarosta, Sekretarz Powiatu, Skarbnik Powiatu oraz naczelnicy wydziałów (kierownicy komórek organizacyjnych) w zakresie merytorycznie nadzorowanych zagadnień realizowanych przez wydziały (komórki organizacyjne) zgodnie z Regulaminem Organizacyjnym Starostwa Powiatowego w Elblągu.
3. Każda osoba mająca dostęp do danych osobowych przetwarzanych w Urzędzie zobowiązana jest do podpisania oświadczenia o zachowaniu poufności tych danych. Wzór oświadczenia stanowi załącznik nr 2 do Polityki ochrony danych.

§ 4

Osoby upoważnione do przetwarzania danych mają obowiązek zabezpieczania danych przed ich

udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 5

1. Obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania) stanowią wszystkie pomieszczenia biurowe zajmowane przez komórki organizacyjne Starostwa Powiatowego w budynkach:
   a) przy ul. Saperów 14A, 82 – 300 Elbląg
   b) przy ul. Komeńskiego 40, 82 – 300 Elbląg,
   c) przy ul. Wojska Polskiego 14, 14 – 400 Pasłęk.
2. W przypadku konieczności uzyskania dostępu do obszaru przetwarzania przez osoby, nieupoważnione do przetwarzania danych osobowych, które muszą wykonać prace o charakterze serwisowym lub inne działania doraźne, osoby te muszą zostać powiadomione o zobowiązaniu do zachowania poufności i ochrony danych osobowych pozyskanych w związku z wykonywaną czynnością serwisową, a w szczególnych przypadkach podpisania pisemnego oświadczenia o zachowaniu poufności i ochronie danych osobowych. Osoby nieupoważnione mogą przebywać w obszarach określonych, jako obszar przetwarzania wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. Przebywanie w pomieszczeniach serwerowni Urzędu innych osób niż obsługa informatyczna, ADO i IOD dopuszczalne jest tylko za pisemnym upoważnieniem ADO. Zasada ta dotyczy również osób wykonujących czynności serwisowe niezbędne dla funkcjonowania infrastruktury technicznej lub upoważnionych do prowadzenia kontroli. Wzór wykazu wstępu do serwerowni Urzędu stanowi Zał. Nr. 3 do Polityki ochrony danych. Pracownik obsługi informatycznej zobowiązany jest do umieszczenia wykazu wstępu do pomieszczeń serwerowni na drzwiach do tychże pomieszczeń. Osoby przebywające w serwerowni zobowiązane są do wpisu w ww. wykaz.
4. Klucz do pomieszczeń serwerowni powinien zostać umieszczony w zabezpieczonej skrzynce do której dostęp posiadać będą jedynie osoby upoważnione do przebywania w pomieszczeniach serwerowni.

§ 6

1. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie na podstawie zawartej na piśmie umowy powierzenia przetwarzania danych osobowych. Do zawierania takich umów upoważniony jest jedynie ADO.
2. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie na pisemny wniosek podmiotu i po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia.

§ 7

1. Każda osoba posiadająca dostęp do systemu informatycznego w którym przetwarzane są dane osobowe musi posiadać w tym systemie swój unikalny identyfikator oraz indywidualne hasło.
2. Przetwarzanie zbiorów danych osobowych na komputerach przenośnych poza obszarem przetwarzania, o którym mowa w § 5 ust.1 dozwolone jest jedynie po otrzymaniu zgody ADO.
3. Przenośne nośniki danych mogą służyć do przechowywania zbiorów danych osobowych tylko w wyjątkowych sytuacjach za zgodą IOD i tylko po zastosowaniu środków ochrony kryptograficznej.
4. Wycofane z użycia nośniki danych należy przekazać do pracownika obsługi informatycznej, który w konsultacji z IOD, trwale usunie zamieszczone w nich dane osobowe.

5. Szczegółowe zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Elblągu".

§ 8

1. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.
2. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się wyłącznie poprzez pocięcie w niszczarce.
3. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.
4. Po zakończeniu pracy na biurku powinny pozostać tylko telefon i przybory biurowe.
5. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.
6. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.
7. Ekrany monitorów komputerów powinny być ustawione tak by uniemożliwiały widok osobom postronnym.

§ 9

Inspektor ochrony danych prowadzi:

a) rejestr czynności przetwarzania danych (wg. wzoru stanowiącego załącznik nr 4 do polityki ochrony danych),
b) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych - wg wzoru stanowiącego załącznik nr 5 do Polityki ochrony danych,
c) wykaz podmiotów, którym udostępniono dane - wg wzoru stanowiącego załącznik nr 6 do Polityki ochrony danych,
d) szczegółowy wykaz pomieszczeń, w których przetwarzane są dane osobowe zgodnie ze wzorem stanowiącym załącznik nr 7 do Polityki ochrony danych,
e) rejestr wszystkich kategorii czynności przetwarzania (proponowany wzór - załącznik nr 8 do polityki ochrony danych).

§ 10

W ramach ustalonego w Urzędzie systemu kontroli zarządczej IOD przeprowadza regularnie analizę ryzyk w obszarze przetwarzania danych osobowych w systemach informatycznych Urzędu. Informacje o istotnych zmianach dotyczących bezpieczeństwa przekazuje niezwłocznie ADO..

§11

W sytuacji, kiedy dojdzie do naruszenia ochrony danych osobowych w administrowanym obszarze, ADO za pośrednictwem IOD ma obowiązek zgłoszenia tego faktu do UODO w obowiązkowym terminie do 72 godzin od momentu stwierdzenia zdarzenia. – zgłoszenie następuję za pomocą formularza w wersji elektronicznej udostępnionego przez Prezesa Urzędu Ochrony Danych Osobowych na stronie internetowej urzędu.

§ 12

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą

z art. 102 ust. 1 pkt 1 Ustawy z dnia 10 maja o ochronie danych osobowych oraz RODO.

Załącznik Nr 1
do Polityki ochrony danych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO,** niniejszym upoważniam do przetwarzania danych osobowych:

_____(*imię, nazwisko*)

_____ (*stanowisko, wydział*)

w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.
Okres obowiązywania od _____r.

Upoważniam _____ (*imię i nazwisko)* do przetwarzania danych osobowych zawartych w następujących zbiorach:

- _____
- _____
- _____

Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie (*w tym miejscu należy wskazać kategorie danych oraz operacje na danych osobowych, jakich może dokonywać upoważniony do przetwarzania danych osobowych)*:

- _____
- _____
- _____

Okres ważności upoważnienia: czas pracy na ww. stanowisku w Starostwie Powiatowym w Elblągu, ul. Saperów 14A, 82-300 Elbląg, dotychczasowe: _____

Jednocześnie traci moc upoważnienie do przetwarzania danych osobowych z dnia: .....

Administrator Danych Osobowych

Data: .....

Załącznik Nr 2
do Polityki ochrony danych

....

(imię i nazwisko) (miejscowość, data)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI DANYCH

1. Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Starostwa Powiatowego w Elblągu. Zachowanie tajemnicy obowiązuje mnie także po zaprzestaniu tych czynności.

2. Zobowiązuję się chronić dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych - w szczególności określonych w Polityce Ochrony Danych oraz Instrukcji Zarządzania Systemem Informatycznym.

4. Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z obowiązującym Ogólnym unijnym rozporządzeniem o ochronie danych (RODO), ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Jestem świadomy/-a odpowiedzialności karnej określonej w rozdziałach 10 i 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

(data i podpis osoby składającej oświadczenie)

Załącznik Nr 3
do Polityki ochrony danych

WYKAZ OSÓB PRZEBYWAJACYCH W SERWEROWNI URZĘDU

***Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg**

lub

***ul. Wojska Polskiego 14, 14-400 Pasłęk**

L.p.	Imię i Nazwisko	Stanowisko, Wydział/Firma	Cel

**niepotrzebne skreślić*

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego

Inspektor Ochrony Danych: Grzegorz Dawidziuk

Załącznik Nr 4
do Polityki ochrony danych

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

	1	2	3	4	5	8	9	10	11	13	15	16
LP.	Nazwa czynności przetwarzania	Wydział	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	Transfer do kraju trzeciego lub org. międzynarodowej	
											Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt g	Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego
Inspektor Ochrony Danych: Grzegorz Dawidziuk

Załącznik Nr 5
do Polityki ochrony danych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Komórka organizacyjna	Zakres *(określenie, do jakich czynności przetwarzania ma dostęp dana osoba)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego

Inspektor Ochrony Danych : Grzegorz Dawidziuk

Załącznik Nr 6
do Polityki ochrony danych

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

(wykaz umów powierzenia przetwarzania danych osobowych)

L.p.	**Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Forma udostępnienia** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego
Inspektor Ochrony Danych: Grzegorz Dawidziuk

Załącznik Nr 7
do Polityki ochrony danych

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych

L.p.	Lokalizacja - adres	Precyzyjne określenie pomieszczenia (piętro/pokój)	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1	2	3	4	5
Budynek Starostwa Powiatowego w Elblągu, ul. Saperów 14A, 82 – 300 Elbląg				
1.				
2.				

Budynek Starostwa Powiatowego w Elblągu, ul. Komeńskiego 40, 82 – 300 Elbląg				
L.p.	**Lokalizacja-adres**	**Precyzyjne określenie pomieszczenia**	**Dział/osoba użytkująca pomieszczenie**	**Zabezpieczenie pomieszczenia**
1.				
2.				

Budynek Starostwa Powiatowego w Elblągu, ul. Wojska Polskiego 14, 14 – 400 Pasłęk				
L.p.	**Lokalizacja-adres**	**Precyzyjne określenie pomieszczenia**	**Dział/osoba użytkująca pomieszczenie**	**Zabezpieczenie pomieszczenia**
1.				
2.				

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego
Inspektor Ochrony Danych: Grzegorz Dawidziuk

Załącznik Nr 8
do Polityki ochrony danych

Rejestr kategorii czynności przetwarzania danych osobowych

	1	2	3	4	5	6	9	10
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Starostwo Powiatowe w Elblągu reprezentowane przez Starostę Elbląskiego				Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)		
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a				Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c
1								
2								
3								
4								

Załącznik Nr 2
do Zarządzenia
Nr.....17.2018.....
Starosty Elbląskiego
z dnia...18 grudnia 2018r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w Starostwie Powiatowym w Elblągu

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

1) Urzędzie - należy przez to rozumieć Starostwo Powiatowe w Elblągu;
2) Instrukcji - należy przez to rozumieć niniejszy dokument;
3) Polityce Ochrony Danych - należy przez to rozumieć przyjęty do stosowania w Urzędzie dokument zatytułowany: „Polityka Ochrony Danych";
4) Użytkowniku - należy przez to rozumieć pracownika lub inną osobę działająca na rzecz Urzędu wykorzystującą system informatyczny Urzędu lub wykorzystywany przez Urząd;
5) Systemie informatycznym - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) IOD – Inspektor Ochrony Danych;
7) ADO – Administrator Danych Osobowych.

I. Procedury nadawania i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym

§ 2

1. Osoba, która ma uzyskać dostęp do systemu informatycznego w którym przetwarzane są dane osobowe, musi być upoważniona do przetwarzania danych osobowych (wg załącznika nr 1 do Polityki Ochrony Danych), oraz podpisać oświadczenie (wg załącznika nr 2 do Polityki Ochrony Danych
2. Pracownik obsługi informatycznej dokonuje nadania osobie uprawnień w systemie informatycznym wyłącznie na podstawie pisemnego zgłoszenia użytkownika systemów informatycznych. Wzór zgłoszenia użytkownika stanowi załącznik nr 1 do Instrukcji. Zgłoszenia dokonują Naczelnicy Wydziałów lub w przypadku zgłoszeń dotyczących tychże osób - ich bezpośredni przełożeni wyższego szczebla.
3. Pracownik obsługi informatycznej przydziela danej osobie identyfikator i hasło oraz nadaje zgłoszony zakres uprawnień w systemie informatycznym po konsultacji z IOD.
4. Pracownik obsługi informatycznej przekazuje osobie wskazanej w zgłoszeniu identyfikator i hasło w sposób uniemożliwiający zapoznanie się z nimi osobom trzecim.

§ 3

W przypadku wygaśnięcia upoważnienia do przetwarzania danych osobowych lub odebrania uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych pracownik

obsługi informatycznej po konsultacji z IOD dokonuje czynności, które uniemożliwiają ponowne wykorzystanie identyfikatora użytkownika w tym systemie.

II. Metody i środki uwierzytelniania oraz procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników

§ 4

1. W celu uzyskania dostępu do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło.
2. Komputerowe stanowiska pracy muszą być skonfigurowane w taki sposób aby po okresie 15 minut bezczynności były one automatycznie blokowane. Do wznowienia pracy konieczne jest co najmniej ponowne użycie hasła.

§ 5

1. Hasło użytkownika w systemie informatycznym musi składać się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła.
3. Zmiana hasła następuje co 30 dni. Jeśli system informatyczny nie wymaga dokonania takiej zmiany, każdy użytkownik jest zobowiązany do samodzielnej zmiany hasła. Hasła powinny mieć charakter unikalny, nie powinno się powtarzać poprzednich wersji haseł.
4. Użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed ujawnieniem osobom trzecim.
5. Hasło użytkownika w systemie informatycznym nie może zawierać: imion, nazwisk, daty urodzenia, pseudonimu, nazw miesięcy.

§ 6

1. Do zasilania komputerowych stanowisk pracy i urządzeń peryferyjnych należy stosować tylko gniazda wydzielonej sieci elektrycznej, przeznaczone wyłącznie do zasilania sprzętu komputerowego oraz listwy przepięciowe.
2. Zakazuje się podłączania innych urządzeń (w szczególności grzejników i innego sprzętu AGD) do gniazd wydzielonej sieci elektrycznej zasilającej sprzęt komputerowy.

III. Zasady tworzenia kopii zapasowych oraz ich przechowywania

§ 7

1. Kopie zapasowe wykonuje się codziennie w sposób automatyczny za pomocą przeznaczonego do tego celu oprogramowania, proces wykonywania kopii zapasowych kontroluje na bieżąco osoba pełniąca funkcję informatyka lub w sytuacjach wyjątkowych IOD.
2. Kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, które nie mogą być wykonane w sposób automatyczny wykonywane są przynajmniej raz w miesiącu. Proces wykonywania kopii zapasowych kontroluje na bieżąco pracownik obsługi informatycznej lub w sytuacjach wyjątkowych, osoba go zastępująca (firma zewnętrzna, której powierzono tą funkcję).
3. Nośniki z kopiami zapasowymi mogą być przechowywane jedynie w:
   a) pomieszczeniach o podwyższonym poziomie bezpieczeństwa fizycznego,
   b) pomieszczeniach zamykanych na klucz o ile nośniki znajdują się w szafie pancernej.
4. Dostęp do nośników z kopiami zapasowymi posiada IOD lub osoba pełniąca funkcję informatyka.

§ 8

Nośniki z kopiami zapasowymi zawierającymi dane osobowe są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

IV. Zabezpieczenia przed działalnością szkodliwego oprogramowania

§ 9

1. Serwery i komputerowe stanowiska pracy musza być chronione przed działaniem szkodliwego oprogramowania poprzez zastosowanie zarządzanego centralnie systemu antywirusowego.
2. Sieć komputerowa na styku z Internetem musi być chroniona dedykowanymi do tego urządzeniami klasy firewall/UTM.
3. Do obowiązków obsługi informatycznej należy:
   a) bieżące monitorowanie wdrożonego systemu antywirusowego;
   b) bieżące monitorowanie aktualizowania urządzeń klasy firewall/UTM oraz przepływu informacji pomiędzy systemem informatycznym a Internetem a także kontrola działań inicjowanych z Internetu i systemu informatycznego.
4. IOD oraz informatyk mają prawo inicjowania instalacji mechanizmów uniemożliwiające użytkownikom samodzielnie instalowanie jakiegokolwiek oprogramowania.
5. Użytkownikom nie wolno otwierać plików pochodzących z niewiadomego źródła bez zgody IOD lub osoby pełniącej funkcję informatyka.

V. Wymaganie funkcjonalności systemów informatycznych

§ 10

1. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu (automatycznie)
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie)
   c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą)
   d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia (nie dotyczy systemu używanego do przetwarzania danych zawartych w zbiorach jawnych)
   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych
2. Funkcjonalności określone w ust. 1 nie obowiązują w przypadku systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie. Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust.1.

VI. Zasady dokonywania przeglądów i konserwacji

§ 11

1. Nie rzadziej niż co 3 miesiące osoba pełniąca funkcję informatyka dokonuję przegląd systemu informatycznego, polegającego na ustaleniu poprawności działania tych jego elementów i

funkcjonalności, które nie są na bieżąco monitorowane.

2. Regularnemu przeglądowi – co sześć miesięcy, podlegają także nośniki z kopiami zapasowymi pod względem ich użyteczności oraz konta użytkowników systemu informatycznego w zakresie ich aktualności i prawidłowości wykorzystywania.
3. W przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu informatycznego informatyk po konsultacji z IOD podejmuje niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.
4. Jeżeli do przywrócenia prawidłowego działania systemu lub dokonania jego konserwacji niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności naprawcze, powinny odbywać się w obecności informatyka lub IOD - w sytuacji wyjątkowej - osoby przez niego wyznaczonej
5. W sytuacji, kiedy dojdzie do naruszenia ochrony danych w systemie informatycznym ADO za pośrednictwem IOD zgłasza ten fakt do UODO w obowiązkowym terminie do 72 godzin od momentu wykrycia zdarzenia.

VII. Zasady użytkowania urządzeń przenośnych oraz dostępu z zewnątrz do sieci informatycznej

§ 12

Użytkownik komputera przenośnego zawierającego dane osobowe zobowiązany jest do:

a) zachowania szczególnej ostrożności podczas jego przenoszenia, przechowywania i użytkowania,
b) zabezpieczenia hasłem plików lub folderów zawierających dane osobowe stosując dodatkowo środki ochrony kryptograficznej.

§ 13

Dostęp z zewnątrz do sieci informatycznej Urzędu możliwy jest tylko w określonych przypadkach:

a) dostęp doraźny (jednorazowy) w celu prac serwisowych z wykorzystaniem oprogramowania zaakceptowanego przez informatyka po konsultacji z IOD,
b) w uzasadnionych przypadkach dostęp stały dla wybranych pracowników Urzędu
   - z wykorzystaniem połączenia VPN, do którego zestawienia każdy użytkownik musi posiadać indywidualny login i hasło nadane przez informatyka po konsultacji z IOD,
   - w uzasadnionych przypadkach dostęp sposób stały (na okres świadczenia usług) dla użytkowników nie będących pracownikami Urzędu, świadczących usługi na jego rzecz - z wykorzystaniem połączenia VPN, do którego zestawienia każdy użytkownik musi posiadać indywidualny login i hasło nadane przez informatyka po konsultacji z IOD.

§ 14

1. Elektroniczne nośniki pamięci, zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych i uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Nośniki przekazywane podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odczytanie.
3. Nośniki przeznaczone do naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odczytanie albo naprawia się je w konsultacji z IOD lub osobą przez niego wyznaczoną.
4. Powyższe czynności są dokumentowane przez osobę pełniącą funkcję informatyka, dokumentacja powinna zostać przekazana IOD do wiadomości.

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego
Inspektor Ochrony Danych: Grzegorz Dawidziuk

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym

Zgłoszenie użytkownika systemów informatycznych

Imię i nazwisko: .....

Nazwa komórki / jednostki organizacyjnej:

Stanowisko: .....

Proszę o nadanie/odebranie*
uprawnień w systemie informatycznym lub zmianę realizowanych funkcji - dla w/w osoby w zakresie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Data i podpis dokonującego zgłoszenia (przełożonego):

- Wypełnia Inspektor Ochrony Danych –

Nadany identyfikator w systemie informatycznym:.....

Zmiany dokonane w zakresie funkcji realizowanych przez użytkownika w systemie oraz inne uwagi:

Załącznik nr 3
do Zarządzenia Nr 17/2018
Starosty Elbląskiego
z dnia 18 grudnia 2018 r.

INSTRUKCJA

POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Celem niniejszej regulacji jest określenie zasad postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych oraz tradycyjnych w sytuacji, gdy:

a) stwierdzono naruszenie zabezpieczenia systemu informatycznego w obszarze danych osobowych;
b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych;
c) stwierdzono naruszenie bezpieczeństwa fizycznego pomieszczeń, kartotek lub szaf, w których znajdują się nośniki danych osobowych

d) stwierdzono naruszenie ochrony danych osobowych.

§2

Naruszeniem zabezpieczenia systemu informatycznego oraz ochrony danych osobowych, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub jakiegokolwiek elementu systemu informatycznego/ ochrony danych osobowych, a w szczególności:

a) nieautoryzowany dostęp do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnienie danych nieuprawnionym podmiotom,
d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł,
f) instalowanie nielegalnego oprogramowania.

§3

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Elblągu jest zobowiązany niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego oraz Inspektora Ochrony Danych a następnie postępować stosownie do podjętej przez nich decyzji.
2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a) opisanie symptomów naruszenia ochrony danych osobowych,

b) określenie sytuacji i czasu w jakim stwierdzono naruszenie ochrony danych osobowych,
c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
d) określenie wszelkich kroków podjętych po ujawnieniu zdarzenia.

§4

Inspektor Ochrony danych podejmuje działania w zakresie:
a) zabezpieczenia dowodów umożliwiających ustalenie przyczyn, skutków czy sprawcy naruszenia ochrony danych,
b) minimalizacji negatywnych skutków zdarzenia,
c) wyjaśnienia okoliczności zdarzenia,
d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§ 5

1. Inspektor Ochrony Danych ma prawo do podejmowania działań, a w szczególności:
   a) żądania wyjaśnień od pracowników,
   b) korzystania z pomocy konsultantów,
   c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych,
   d) jeżeli uzna za konieczne - zgłoszenia wystąpienia naruszenia do Urzędu Ochrony Danych Osobowych w ciągu 72 godzin od daty wykrycia nieprawidłowości.
2. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych traktowana będzie jako ciężkie naruszenie obowiązków pracowniczych.

§ 6

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Inspektora Ochrony Danych lub upoważnionej przez niego osoby, należy:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub osoby upoważnionej.

§ 7

Po przybyciu na miejsce naruszenia lub ujawnienia danych osobowych, Inspektor Ochrony Danych i lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych osobowych,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Starostwa,
5) jeżeli uzna za konieczne - zgłasza wystąpienia naruszenia do Urzędu Ochrony Danych Osobowych w ciągu 72 godzin od daty wykrycia nieprawidłowości.

§ 8

Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia ochrony danych osobowych oraz sporządza raport wg wzoru stanowiącego załącznik nr 1 do Postepowania w sytuacji naruszenia ochrony danych osobowych, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

§ 9

1. Raport, o którym mowa w § 8, Inspektor Ochrony Danych niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.
2. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ochrony danych osobowych Inspektor Ochrony Danych wraz z informatykiem zasięgają niezbędnych opinii i proponują postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
3. Zaistniałe naruszenie ochrony danych osobowych może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Inspektora Ochrony Danych, Pełnomocnika ds. Ochrony Informacji Niejawnych.
4. Analiza, o której mowa w ust. 3, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

§ 10

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Inspektora Ochrony Danych.
3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Inspektora Ochrony Danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

4. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, ustawy z dnia 10 maja 2018r. o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Załącznik 1
do instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych

Administrator Danych Osobowych: Starostwo Powiatowe w Elblągu, ul. Saperów 14A, 82-300 Elbląg reprezentowane przez Starostę Elbląskiego
Inspektor Ochrony Danych: Grzegorz Dawidziuk

Raport
z naruszenia bezpieczeństwa systemu informatycznego/naruszenia ochrony danych osobowych
w Starostwie Powiatowym w Elblągu

1. Data:..... Godzina:.....
(termin ustawowy:72 godziny od wykrycia incydentu)
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
(imię, nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia:
(np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa/ochrony danych osobowych oraz okoliczności towarzyszące:
5. Podjęte działania:
6. Przyczyny wystąpienia zdarzenia:
7. Postępowanie wyjaśniające:

Inspektor Ochrony Danych

Administrator Danych Osobowych