BURMISTRZ
MIASTA I GMINY
OSTROROG
ul. Wrzesińska 14, 64-560 Ostroróg

Zarządzenie Nr 70/2017
Burmistrza Miasta i Gminy Ostroróg
z dnia 6 października 2017 r.

w sprawie zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2016r. poz. 446 ze zm.) w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r., poz. 922) oraz § 3 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 (Dz. U. z 2004 r., Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Wprowadzam do stosowania „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg, stanowiącą załącznik nr 1 do zarządzenia.

§ 2. Wprowadzam do stosowania „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg", stanowiącą załącznik nr 2 do zarządzenia.

§ 3. Zobowiązuję Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych do zapoznania pracowników Urzędu Miasta i Gminy Ostroróg z niniejszym zarządzeniem.

§ 4. Zobowiązuję pracowników Urzędu Miasta i Gminy Ostroróg do przestrzegania niniejszego zarządzenia.

§ 5. Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemów Informatycznych.

§ 6. Traci moc Zarządzenie Nr 52/2011 Burmistrza Miasta i Gminy Ostroróg z dnia 29 grudnia 2011 r., w sprawie zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Ostroróg

BURMISTRZ MIASTA I GMINY OSTRORÓG

BURMISTRZ
dr Sławomir Szałata

RADCA PRAWNY
dr Krzysztof Drozdowicz

Załącznik nr 1 do
Zarządzenia Nr 70/2017
Burmistrza Miasta i Gminy Ostroróg
z dnia 6 października 2017 r.

POLITYKA BEZPIECZEŃSTWA

przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg

Rozdział I

Postanowienia ogólne

§. 1.1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg, zwana dalej „Polityką", została opracowana w związku z § 3 ust. 1 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 (Dz. U. z 2004r. Nr 100, poz. 1024).

2. Celem Polityki jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora Danych Osobowych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.

3. Polityka określa zasady przetwarzania danych osobowych, oraz ich zabezpieczenia, jako zbiór reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i przetwarzania w Urzędzie Miasta i Gminy Ostroróg.

4. Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.

5. Opracowaną Politykę stosuje się do danych osobowych przetwarzanych systemach informatycznych, na nośnikach elektronicznych oraz w sposób tradycyjny.

6. Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem w stosownym oświadczeniu.

§ 2.1. Definicje i pojęcia zawarte w Polityce.

Wszystkie pojęcia i definicje zawarte w Polityce znajdują wspólne powiązania zawarte w niniejszym dokumencie, a także z innymi dokumentami, które obowiązują w Urzędzie Miasta i Gminy Ostroróg w zakresie ochrony danych osobowych.

2. Administrator Danych Osobowych (ADO) - w Urzędzie Miasta i Gminy Ostroróg jest nim Burmistrz Miasta i Gminy Ostroróg. ADO decyduje o środkach i celach przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg.

3. Administrator Bezpieczeństwa Informacji (ABI) - jest to osoba wyznaczona przez ADO. ABI podlega bezpośrednio ADO. Powołany ABI musi spełniać wymogi,

0 których mowa w art. 36a ust. 5 ustawy o ochronie danych osobowych. ABI podlega zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

4. Administrator Systemów Informatycznych (ASI) - jest to osoba wyznaczona przez ADO. ASI jest odpowiedzialna za funkcjonowanie infrastruktury informatycznej, na którą składa się wyposażenie, systemy i aplikacje informatyczne. Odpowiada za ich przeglądy i konserwację, oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.

5. Bezpieczeństwo Przetwarzania Danych - oznacza zachowanie integralności, poufności i rozliczalności danych osobowych, a ponadto dostępności niezawodności.

6. Dane Osobowe - definicja określona jest w art. 6 ustawy o ochronie danych osobowych.

7. GIODO - oznacza Generalny Inspektor Ochrony Danych Osobowych.

8. Integralność danych - oznacza właściwość zapewniająca pewność, iż nie dokonano zmiany lub zniszczenia danych w sposób nieautoryzowany.

9. Naruszenie ochrony danych osobowych - jest to zamierzone lub niezamierzone naruszenie obowiązujących środków technicznych organizacyjnych, zastosowanych w celu ochrony danych osobowych, w szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, zasady funkcjonowania oprogramowania i komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych.

10. Poufność - jest to właściwość dająca pewność, że do danych osobowych ma dostęp wyłącznie osoba upoważniona.

11. Rozliczalność - jest to właściwość zapewniająca, że działania pracownika/użytkownika zewnętrznego mogą być przypisane w sposób jednoznaczny tylko temu pracownikowi/użytkownikowi zewnętrznemu.

12. Przetwarzanie danych osobowych - są to jakiekolwiek działania wykonywane na danych osobowych, w szczególności takie jak: pozyskiwanie, gromadzenie, wgląd, przenoszenie, utrwalanie, udostępnianie, usuwanie, a również te, które wykonuje się w systemach informatycznych.

13. Ustawa - rozumie się ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz. U. z 2014 r., poz. 1182 z późn. zm.).

14. Rozporządzenie - rozumie się rozporządzenie 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 (Dz.U. z 2004 r., Nr 100, poz. 1024).

15. Urząd - rozumie się Urząd Miasta i Gminy Ostroróg ul. Wroniecka 14, 64-560 Ostroróg.

16. Użytkownik systemu - jest to osoba zatrudniona w Urzędzie, posiadająca upoważnienie, identyfikator, hasło dostępu, upoważniające do przetwarzania danych osobowych w systemie informatycznym.

17. Użytkownik zewnętrzny - jest to osoba niezatrudniona w Urzędzie posiadająca uprawnienia do przetwarzania danych osobowych w związku z wykonywaniem powierzonych obowiązków.

18. Właściciel zasobów danych osobowych - jest to osoba kierująca komórką organizacyjną (Referatem) w Urzędzie, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce lub na samodzielnym stanowisku pracy, zobowiązana zastosować wszelkie środki techniczne i organizacyjne zapewniające właściwą ochronę danych osobowych, stosowną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności: zabezpieczenie danych przed ich udostępnieniem osobie nieupoważnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy, przed nieautoryzowaną zmiana, utrata, uszkodzeniem lub zniszczeniem.

19. System informatyczny - jest to zespół współpracujących urządzeń, programów, procedur związanych z przetwarzaniem danych osobowych, oraz narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

20. Zbiór danych osobowych - jest to każdy, posiadający strukturę zestaw o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

21. Zbiór nieinformatyczny - jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie, prowadzony w formie nieelektronicznej, poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu, a także w każdej innej formie w postaci zbioru.

§ 3 ADO zobowiązany jest do zapewnienie przetwarzania danych osobowych ze szczególną starannością realizując następujące zasady:

1) przetwarzanie danych osobowych na podstawie art. 23 ust. 1 Ustawy,
2) spełnianie obowiązku informacyjnego wobec osób, których dane osobowe dotyczą zgodnie z art. 24 Ustawy,
3) udzielanie informacji na temat przetwarzania danych osobowych, na wniosek osoby, której dane dotyczą.

§ 4. 1. Aktualizacja dokumentacji związanej z ochroną danych osobowych.

Polityka oraz wszystkie dokumenty z nią powiązane, powinny być aktualizowane wraz ze zmianami w przepisach prawa dotyczących ochrony danych osobowych, oraz zmianami wynikającymi z organizacji i funkcjonowania Urzędu.

2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.

3. W każdym przypadku zmiany zapisów niniejszej Polityki wymagają aktualizacji inne dokumenty powiązane z Polityką.

4. Zmiany w dokumentacji wprowadzane są za wiedzą i na polecenie ADO.

§ 5. 1. Zarządzanie ochroną danych osobowych.

Celem właściwej realizacji zamierzeń, a także skutecznej ochrony danych osobowych należy stosować następujące działania:

1) upoważnić pracowników i użytkowników zewnętrznych do przetwarzania danych osobowych,
2) przeszkolić pracowników uprawnionych do przetwarzania danych osobowych w zakresie bezpieczeństwa,

3) przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych, dających możliwość dostępu do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,

4) kontrolować sposób postępowania przy przetwarzaniu danych osobowych,

5) podejmować stosowne działania, celem wyeliminowania stwierdzonych nieprawidłowości,

6) na bieżąco wdrażać nowe rozwiązania techniczne i organizacyjne, które wzmocnią bezpieczeństwo danych osobowych.

2. W procesie nadzoru należy szczególnie uwzględnić zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

3. W procesie zarządzania należy stosować działania, które spowodują, że użytkownicy systemu i użytkownicy zewnętrzni będą:

1) odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych,

2) zapoznani z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w Urzędzie,

3) informowani na bieżąco o wszelkich zmianach w procedurach.

§ 6. Dokumentacja powiązana z Polityką.

Na dokumentację powiązaną z procesem bezpieczeństwa przetwarzanych danych osobowych w Urzędzie składają

się:

Lp.	Nazwa dokumentu	Odpowiedzialny
1.	Rejestr zbiorów danych prowadzony przez ABI wraz z wnioskami.	ABI
2.	Wnioski związane ze zgłoszeniem i aktualizacją zbioru w GIODO.	ADO
3.	Upoważnienie do przetwarzania danych osobowych.	ADO
4.	Ewidencja osób upoważnionych do przetwarzania danych osobowych. Ewidencja prowadzona jest odrębnie dla pracowników i użytkowników zewnętrznych.	ABI
5.	Ewidencja zbiorów danych osobowych podlegających	ABI

	rejestracji.	
6.	Ewidencja zbiorów danych osobowych niepodlegających rejestracji.	ABI
7.	Ewidencja programów komputerowych stosowanych do przetwarzania danych oraz opis sposobu przepływu danych pomiędzy systemami informatycznymi. Ewidencja zawiera także programy komputerowe objęte siecią wewnętrzną, które nie są wykorzystywane do przetwarzania danych osobowych, a są stosowane w Urzędzie.	ASI
8.	Oświadczenie o zapoznaniu się z przepisami i procedurami. Ewidencja szkoleń.	ABI
9.	Rejestry i raporty z naruszenia danych osobowych.	ABI/ASI
10.	Zarządzenia ADO dotyczące powołania AB I, ASI.	ADO/ABI
11.	Dokumentacja ze sprawdzeń planowych i doraźnych, w tym plany, notatki, wyjaśnienia, sprawozdania, zawiadomienia o nieprawidłowościach.	ABI
12.	Protokoły z kontroli zewnętrznych.	ADO/ABI
13.	Ewidencja przenośnych nośników informacji używanych przez pracowników.	ASI
14.	Ewidencja podmiotów, którym powierzono przetwarzanie danych, umowy w tym zakresie.	ABI
15.	Obowiązujące przepisy prawa w zakresie ochrony danych osobowych.	ABI

§ 7. Zadania i obowiązki ADO.

Do głównych zadań i obowiązków ADO należy:

1) zapewnienie, aby dane osobowe były przetwarzane zgodnie z prawem,

2) zbieranie danych dla określonych celów i nie poddawanie dalszemu przetwarzaniu niezgodnie z tymi celami,

3) zapewnienie merytorycznej poprawności i adekwatności danych w stosunku do celów, w jakich są przetwarzane,

4) przechowywanie w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania,

5) zabezpieczenie środkami technicznymi i organizacyjnymi, na poziomie wysokim w rozumieniu zapisów § 6 ust. 4 Rozporządzenia, przetwarzania danych osobowych, poprzez realizację zadań określonych w Ustawie,

6) prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz podjęte środki techniczne i organizacyjne zapewniające ochronę danych,

7) nadanie uprawnień osobom mającym dostęp do danych osobowych,

8) zgłoszenie do rejestracji Głównemu Inspektorowi Ochrony Danych Osobowych, zbiorów danych o których mowa w art. 43 ust. 1a Ustawy.

§ 8. 1. Zadania i obowiązki ABI. Do głównych zadań i obowiązków ABI należy:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

2) opracowywanie sprawozdań dla ADO, oraz Generalnego Inspektora Ochrony Danych Osobowych w przypadku, o którym mowa w art. 19 b ust. 1 Ustawy,

3) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę danych osobowych, oraz przestrzeganie zasad w niej określonych,

4) przeprowadzanie szkoleń oraz zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z obowiązującymi przepisami w tym zakresie,

5) prowadzi rejestr zbiorów danych przetwarzanych przez ADO.

2. ABI w zakresie realizacji swoich obowiązków, ma prawo żądać od pracowników i użytkowników zewnętrznych składania wyjaśnień oraz wzywać i przesłuchiwać w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych.

§ 9. 1. Zadania i obowiązki ASI. ASI nadzoruje przestrzeganie zasad ochrony danych osobowych w systemach informatycznych Urzędu.

2. Do zakresu obowiązków ASI należy:

1) realizowanie decyzji ADO odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku Technologii Informacyjnej - zwanej dalej IT - Urzędu tj.:

a) tworzenie kont użytkowników w systemach informatycznych;

b) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont;

c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany;

d) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych,

e) resetowanie utraconych haseł;

f) usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie;

g) dostarczanie ABI, danych potrzebnych do oceny prawidłowości funkcjonowania systemu informatycznego/ programów.

2) planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie,

3) prowadzenie rejestru stosowanych programów oraz sprzętu komputerowego obejmującego rodzaj i konfigurację sprzętu,

4)zapewnienie i kompletowanie dokumentacji dotyczącej legalności oprogramowania wykorzystywanego na stacjach roboczych / serwerach,

5) zabezpieczenie systemów przetwarzania danych osobowych, w zależności od kategorii przetwarzanych w tym systemie danych,

6) planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych,

7) automatyzacja zadań konserwacyjnych w systemie,

8) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,

9) w przypadku powstania zagrożenia ochrony danych osobowych, bezzwłoczne podjęcie stosownych działań, przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,

10) analiza raportów wszelkich zdarzeń, w tym incydentów związanych z bezpieczeństwem systemów przetwarzających dane,

11) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,

12) zapewnienie eksploatowanym systemom opieki serwisowej producenta - zawieranie umów regulujących formy tej opieki,

13) rozwiązywanie problemów towarzyszących eksploatacji systemów

14) przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji,

15) prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.

§ 10. Odpowiedzialność Właścicieli zasobów danych osobowych.

Do obowiązków Właścicieli zasobów danych osobowych należy:

1) zapewnienie pracownikom niezbędnych uprawnień do przetwarzania danych osobowych, poprzez wnioskowanie do ADO o nadanie upoważnień dla pracowników podległej komórki organizacyjnej,

2) zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych i informacji na temat zabezpieczenia tych danych,

3) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,

4) realizacja obowiązku informacyjnego o przetwarzaniu danych osobowych wobec osób, których dane są pozyskiwane,

5) zapewnienie na żądanie uprawnionych osób, udostępnienia informacji o przetwarzanych danych osobowych, oraz podmiotach, którym zostały one udostępnione,

6) współpraca i informowanie ABI oraz ASI o konieczności utworzenia nowego zbioru danych osobowych, jego zakresie, celu przetwarzania i udostępnianiu,

7) złożenie wniosków o rejestrację i aktualizację zbioru danych do ABI.

§ 11. 1. Odpowiedzialność pracowników i użytkowników systemów.

W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych, konieczne jest szczególne zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2. Pracownicy, oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach i słabościach systemu przetwarzającego dane osobowe do ABI.

3. Pracownicy i użytkownicy zewnętrzni są zobowiązani do:

1) postępowania zgodnie z zasadami określonymi w Polityce,

2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczania,

3) ochrony danych osobowych, oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

4) wykonywania niezbędnych działań w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym:

a) przestrzegania procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wchodzeniem do obszarów przetwarzania danych osobowych osób nieupoważnionych,

b) informowania ABI lub kierownictwo Urzędu o podejrzanych osobach poruszających się w obszarze przetwarzania,

c) dokonywania identyfikacji ewentualnych zagrożeń i przedkładanie ABI projektów i propozycji nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa danych.

§ 12. 1 Odpowiedzialność za naruszenie zasad ochrony danych osobowych. Rozdział 8 Ustawy, a także art. 266 Kodeksu karnego, określa odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy - obowiązkiem pracownika jest przestrzegania tajemnic prawnie chronionych określonych w odrębnych przepisach.

3. Ciężkie naruszenie obowiązków pracowniczych, może skutkować rozwiązaniem umowy o pracę z winy pracownika bez wypowiedzenia umowy o pracę.

§ 13. 1. Szkolenia.

Przed dopuszczeniem do przetwarzania danych osobowych, każdy pracownik, użytkownik zewnętrzny, który będzie pracować na danych osobowych powinien zostać zapoznany z obowiązującymi przepisami i przeszkolony przez ABI oraz ASI - jeżeli będzie przetwarzać dane w systemie informatycznym. Szkolenie powinno obejmować następujące zagadnienia:

1) obowiązujące przepisy w zakresie ochrony danych osobowych,

2) procedury oraz zasady przetwarzania danych osobowych,

3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych,

4) zasady użytkowania oprogramowania, urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,

5) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych,

6)zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

7) zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,

8)odpowiedzialność w przypadku naruszenia ochrony danych osobowych.

2. Pracownicy i użytkownicy zewnętrzni powinni odbywać szkolenia okresowe nie rzadziej niż raz na dwa lata. Szkolenia te prowadzi ABI lub firma zewnętrzna.

§ 14. Zasady szczególnej staranności.

Każdy pracownik i użytkownik zewnętrzny dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych, a w szczególności:

1) stosowania wszelkich metod zabezpieczeń wynikających w Polityki,

2) zabezpieczenia wydruków elektronicznych, a także tych, które mogą być tworzone podczas kserowania, kopiowania, skanowania,

3) udzielania informacji zawierających dane osobowe wyłącznie osobom i podmiotom uprawnionym,

4) prowadzenia rozmów telefonicznych w sposób bezpieczny, zapewniający przekazywanie informacji wyłącznie osobom uprawnionym. Zachowanie w tym zakresie zasady ograniczonego zaufania.

§ 15. 1. Miejsca i pomieszczenia przeznaczone do przetwarzania danych osobowych.

Obszar przetwarzania danych osobowych obejmuje pomieszczenia znajdujące się w budynku Urzędu przy ul. Wronieckiej 14:

1) piwnica – pomieszczenie centrali telefonicznej

2) parter – pokój nr 3

3) pierwsze piętro - pokoje numer 11; 12; 13; 14; 15; 16; 17

4) drugie piętro - pokoje numer 22; 23; 24; 25; 26; 27

2. Dane osobowe przetwarzane są wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje ich przetwarzanie.
3. Pomieszczenia bezpieczne to takie, które nie jest pozostawione bez nadzoru odpowiedzialnego pracownika, użytkownika zewnętrznego.
4. Pomieszczenia, w których przetwarzane są dane osobowe, podczas nieobecności osoby upoważnionej, należy zamykać na klucz.
5. Obiekt jak i pomieszczenia są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami:
6. Okna pomieszczeń usytuowanych na parterze budynku od strony Urzędu Stanu Cywilnego zabezpieczone są kratami.
7. Pomieszczenia wyposażone są w sprzęt ppoż.
8. W przypadku wykonywania prac naprawczych, remontowych, montażowych przez firmy zewnętrzne, dane osobowe zostają należycie zabezpieczone przed nieupoważnionym dostępem.
9. Kopie zapasowe nie mogą być przechowywane w pomieszczeniu, w którym znajdują się zbiory podstawowe.
10. Każdy pracownik Urzędu w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia, zobowiązany jest do niezwłocznego poinformowania ABI.

§ 16. 1. Upoważnienia do przetwarzania danych osobowych.

Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika upoważnienia do ich przetwarzania podpisanego przez ADO.

2. Upoważnienie do podpisania przez ADO przygotowuje ABI na pisemny wniosek bezpośredniego przełożonego pracownika bądź Sekretarza.
3. Pracownik, użytkownik zewnętrzny po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami. Upoważnienie oraz oświadczenie przechowywane jest w aktach osobowych, oraz dokumentacji ABI.

4. Po podpisaniu upoważnienia ABI przekazuje kopię upoważnienia ASI w celu nadania odpowiednich uprawnień w systemach informatycznych.

§ 17. 1. Ewidencja osób upoważnionych.

ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja jest prowadzona przez ABI.
3. Ewidencja zawiera:
   1) imię i nazwisko osoby upoważnionej.

2) data nadania upoważnienia,
3) data ustania upoważnienia,
4) zakres i numer upoważnienia,
5) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

§ 18. 1. Zbiory danych osobowych.

Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych i w kartotekach ewidencyjnych.

2. Zbiory danych osobowych są zlokalizowane w pomieszczeniach Urzędu.

3. Wykaz systemów i aplikacji związanych z przetwarzaniem danych osobowych, oraz struktury zbiorów danych osobowych i opis struktur wskazujący zawartość poszczególnych pól, prowadzony jest przez ASI.

4. ASI prowadzi dokumentację związaną ze sposobem i zasadami współpracy i przepływu danych pomiędzy poszczególnymi systemami.

§ 19. 1. Rejestracja zbiorów danych osobowych.

Zbiory danych osobowych podlegają rejestracji w rejestrze prowadzonym przez ABI lub ogólnokrajowym rejestrze prowadzonym przez GIODO z wyjątkiem danych o których mowa w art. 43 ust 1. Ustawy.

2. Kierownicy Referatów, oraz pracownicy zatrudnieni na samodzielnych stanowiskach pracy zgłaszają potrzebę i zamiar przetwarzania nowego zbioru danych osobowych w celu zarejestrowania go, lub dokonania aktualizacji w rejestrze prowadzonym przez ABI, lub GIODO. Kierownicy przedkładają ABI wniosek o planowanym utworzeniu zbioru danych.

3. Projekt zgłoszenia zbioru danych, lub jego aktualizację, który podlega rejestracji w ogólnokrajowym rejestrze zbiorów danych osobowych prowadzonych przez GIODO, przygotowuje ABI i przedkłada go do podpisania ADO. Rejestracji dokonuje ABI wypełniając wniosek na platformie e-giodo, znajdującej się na stronie www.giodo.gov.pl.

4. Zbiór należy zarejestrować przed rozpoczęciem przetwarzania danych.

5. Po zarejestrowaniu zbioru, ABI aktualizuje prowadzoną ewidencję zbiorów danych.

§ 20. 1. Udostępnianie danych osobowych - zasady i procedury.

Udostępnianie danych osobowych odbywa się na zasadzie potrzeby koniecznej.

2. Udostępnianie danych osobowych zewnętrznym uprawnionym podmiotom odbywa się na pisemny wniosek.

3. W przypadku udostępniania danych osobowych na zewnątrz ABI dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia.

4. Dane osobowe przekazywane na zewnątrz są przekazywane listem poleconym za zwrotnym poświadczeniem odbioru, lub innym bezpiecznym sposobem określonym wymogami prawa lub umową.

5. Fakt udostępnienia danych należy udokumentować pisemnie, poprzez wykonanie pisma przewodniego lub notatki urzędowej.

§ 21. Odmowa udostępnienia danych osobowych.

ADO odmawia udostępnienia danych osobowych, jeżeli spowodowałoby to:

1) ujawnienie wiadomości zwierających informacje niejawne,

2)zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa publicznego,

3)zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

§ 22. 1. Powierzenie przetwarzania danych osobowych.

Powierzenie danych osobowych odbywa się na zasadach określonych art. 31 ust. 1 Ustawy.

2. Powierzenie danych występuje wówczas, gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez Urząd.

3. ADO może powierzyć innemu podmiotowi, współpracującemu z Urzędem, przetwarzanie danych, na zasadach wynikających z umowy powierzenia.

4. W Urzędzie przetwarzane mogą być dane osobowe, powierzone Urzędowi do przetwarzania przez inny podmiot, na zasadach określonych w umowie powierzenia.

5. Umowa powierzenia musi mieć formę pisemną i powinna zawierać:

1) cel i zakres przetwarzania danych osobowych,

2) sposoby zabezpieczenia danych i zasady ich przetwarzania,

3) zasady organizacyjne i techniczne jakie powinien spełnić podmiot, któremu powierzono dane osobowe,

4) odpowiedzialność podmiotu, któremu powierzono dane osobowe za nieprawidłowe przetwarzanie danych osobowych,

5) prawo do kontroli prawidłowości przetwarzania danych przez upoważnionego przedstawiciela podmiotu powierzającego dane do przetwarzania.

6. Projekt umowy powierzenia przetwarzania danych innemu podmiotowi przygotowuje ABI.

7. Projekt umowy przygotowany przez podmiot powierzający Urzędowi dane do przetwarzania, przed podpisaniem przez ADO przedkłada się do zaopiniowania ABI.

8. ABI prowadzi ewidencję podmiotów, którym powierzono przetwarzanie danych.

§ 23. 1. Zasady postępowania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych.

Pracownicy, użytkownicy zewnętrzni są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.

2. Pracownicy, użytkownicy zewnętrzni, każdorazowo przed przystąpieniem do pracy, są zobowiązani do dokonania oceny i oględzin stanowiska sprawdzając, czy nie ma zauważalnych śladów nieuprawnionych działań dokonanych przez osobę nie upoważnioną.

3. Sytuacje, na które należy zwrócić szczególną uwagę to:

1) próba nieuprawnionego dostępu do pomieszczenia,

2) naruszenie lub próba naruszenia integralności, poufności bądź rozliczalności,

3) niezamierzona zamiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe,

4) próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu,

5) stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy, itp.),

4. W sytuacji stwierdzenia naruszenia lub próby naruszenia ochrony danych osobowych, pracownicy, użytkownicy zewnętrzni zobowiązani są do niezwłocznego powiadomienia o tym fakcie ABI.

5. ABI podejmując działania powinien w szczególności:

1) powiadomić ADO o zaistniałej sytuacji,

2) wypełnić raport z naruszenia ochrony danych osobowych,

3) rozpocząć sprawdzenie doraźne,

4) wstrzymać pracę na stanowisku, a także zabronić wykonywania jakichkolwiek działań, które mogłyby utrudnić ocenę i analizę stwierdzonych działań związanych z naruszeniem ochrony danych,

5) zabezpieczyć materiały, dokumenty w celu uniemożliwienia dostępu osobom nieupoważnionym i dalszymi stratami,

6) dokonać oceny sytuacji, szczególnie dokonać oględzin stanowiska pracy, pomieszczenia, stanu zabezpieczenia pomieszczenia, potencjalne skutki związane z naruszeniem ochrony danych osobowych,

7) sporządzić sprawozdanie i przekazać ADO,

8) podjąć dalsze działania stosownie do potrzeb i zaistniałej sytuacji.

6. Sytuacja związana z naruszeniem lub próbą naruszenia ochrony danych osobowych powinna być przedmiotem analizy i wniosków celem uniemożliwienia podobnych zdarzeń w przyszłości.

§ 24. 1. Ochrona danych osobowych w zbiorach nieinformatycznych.

Zbiory i dane przetwarzane w tych zbiorach, to takie dane, które są przetwarzane w formie tradycyjnej, bez wykorzystywania systemów informatycznych.

2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie, a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.

3. Dokument, wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z ich treścią.

4. Podczas niszczenia dokumentów należy przestrzegać przepisów ustawy o Narodowym Zasobie Archiwalnym i przepisów wykonawczych do tej ustawy.

§ 25. 1. Sprawdzenia dokonywane przez ABI. ABI dokonuje sprawdzenia w trybie, sprawdzeń planowych i doraźnych.

2. Sprawdzeń ABI dokonuje dla ADO oraz GIODO - w przypadkach określonych w Ustawie.

3. Przed przystąpieniem do sprawdzenia ABI przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany ADO przed rozpoczęciem sprawdzenia. Plan sprawdzeń zawiera co najmniej jedno sprawdzenie.

4. Zbiory danych oraz systemy informatyczne służące do przetwarzania danych lub zabezpieczenia danych sprawdzane są co najmniej raz na 5 lat.

5. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

6. Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie.

7. ABI sprawuje nadzór nad opracowaniem i aktualizowaniem dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a także nad przestrzeganiem zasad określonych w wyżej wskazanej dokumentacji w drodze czynności sprawdzających oraz poza sprawdzeniami.

§ 26.1. Postanowienia końcowe.

W sprawach nieuregulowanych w niniejszej Polityce zastosowanie mają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisy wykonawcze do Ustawy.

2. **Wykaz załączników do polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg.**

1. **Załącznik nr 1** - Upoważnienie do przetwarzania danych osobowych, dla pracowników Urzędu,

2. **Załącznik nr 2** - Upoważnienie do przetwarzania danych osobowych, dla użytkowników zewnętrznych,

3. **Załącznik nr 3** - Ewidencja osób upoważnionych do przetwarzania danych osobowych (pracownicy Urzędu).

4. **Załącznik nr 4** Ewidencja osób upoważnionych do przetwarzania danych osobowych (użytkownicy zewnętrzni).

5. **Załącznik nr 5** -. Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg zarejestrowanych w rejestrze GIODO.

6. **Załącznik nr 6** Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg zarejestrowanych w rejestrze ABI.

7. **Załącznik nr 7** - Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg niepodlegających rejestracji.

8. **Załącznik nr 8** - Oświadczenie.

9. **Załącznik nr 9** - Raport z naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy Ostroróg.

10. **Załącznik nr 10** - Ewidencja szkoleń w zakresie ochrony danych osobowych w Urzędzie Miasta i Gminy Ostroróg.

11. **Załącznik nr 11** - Wniosek o planowanym utworzeniu zbioru danych osobowych/ Wniosek o aktualizację zbioru danych w Urzędzie Miasta i Gminy Ostroróg.

12. **Załącznik nr 12 -** Ewidencja programów komputerowych stosowanych do przetwarzania danych oraz opis sposobu przepływu danych pomiędzy poszczególnymi systemami

13. **Załącznik nr 13** -.Ewidencja podmiotów, którym powierzono przetwarzanie danych osobowych.

Burmistrz Miasta i Gminy Ostroróg

BURMISTRZ

dr Sławomir Szałata

Załącznik Nr 1
do Polityki Bezpieczeństwa

WZÓR

U P O W A Z N I E N I E Nr

Na podstawie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) zgodnie z powierzonym zakresem czynności na zajmowanym stanowisku

u p o w a z n i a m

Pana/Panią

imię i nazwisko

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/nieinformatycznym w Urzędzie Miasta i Gminy Ostroróg w zbiorach:

L.p.	Pełna nazwa zbioru	Zakres upoważnienia

D -wg ąd, **W**-wprowadzanie, **M**-modyfikacja, **U**-usuwanie

Identyfikator użytkownika

(w systemie informatycznym)

Powyższe upoważnienie wydaje się na /okres do ..... / czas zatrudnienia.

Ostroróg, dnia

Administrator Danych Osobowych

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 2
do Polityki Bezpieczeństwa

WZÓR

U P O W A Z N I E N I E Nr

Na podstawie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) zgodnie z przydzielonymi zadaniami

u p o w a z n i a m

Pana/Panią

imię i nazwisko

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/nieinformatycznym w Urzędzie Miasta i Gminy Ostroróg w zbiorach:

L.p.	Pełna nazwa zbioru	Zakres upoważnienia

D -wg ąd, **W**-wprowadzanie, **M**-modyfikacja, **U**-usuwanie

Identyfikator użytkownika
(w systemie informatycznym)

Powyższe upoważnienie wydaje się na /okres do ..... /czas trwania stażu/ praktyki/ umowy.

Ostroróg, dnia

Administrator Danych Osobowych

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 3 do Polityki
Bezpieczeństwa

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg (Pracownicy Urzędu)

L.p.	Imię i nazwisko	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres i numer upoważnienia^
1	2	3	5	6	7

·)

wgląd	**D**
wprowadzanie	**W**
modyfikacja	**M**
usuwanie	**U**

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 4 do Polityki
Bezpieczeństwa

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg (użytkownicy zewnętrzni)

L.p.	Imię i nazwisko	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres i numer upoważnienia^
1	2	3	5	6	7

.)

wgląd	**D**
wprowadzanie	**W**
modyfikacja	**M**
usuwanie	**U**

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 5
do Polityki Bezpieczeństwa

WZÓR

Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg zarejestrowanych w rejestrze GIODO

Lp.	zbiór		NAZWA ZBIORU Nr rejestracyjny GIODO	Zakres przetwarzany ch w zbiorze danych o osobach	System przetwarzania danych T- tradycyjny I-informatyczny	Nazwa aplikacji Formy zabezpieczenia	Lokalizacja	Zabezpiecz enie fizyczne
1	2	3	4	5	6	7	8	9
1	Data rejestracji							
	Data aktualizacji							
	Data aktualizacji							

BURMISTRZ
dr Sławomir Szalata

Załącznik Nr 6
do Polityki Bezpieczeństwa

WZOR

Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg zarejestrowanych w rejestrze ABI

Lp.			NAZWA ZBIORU Nr rejestracyjny ABI	Zakres przetwarzanych w zbiorze danych o osobach	Nazwa aplikacji Formy zabezpieczenia	Lokalizacja	Zabezpieczenie fizyczne
1	2	3	4	5	6	7	8
	Data rejestracji						
	Data aktualizacji						
	Data aktualizacji						

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 7
do Polityki Bezpieczeństwa

WZÓR

Ewidencja zbiorów danych osobowych przetwarzanych
w Urzędzie Miasta i Gminy Ostroróg niepodlegających rejestracji

Lp.			NAZWA ZBIORU podstawa prawna wyłączająca obowiązek rejestracji	Zakres przetwarzany ch w zbiorze danych o osobach	System przetwarzania danych T- tradycyjny I-informatyczny	Nazwa aplikacji Formy zabezpieczenia	Lokalizacja	Zabezpiecz enie fizyczne
1	2	3	4	5	6	7	8	9
1	Data utworzenia zbioru							
	Data aktualizacji							
	Data aktualizacji							

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 8
do Polityki Bezpieczeństwa

O S W I A D C Z E N I E

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am się z Polityką Bezpieczeństwa, oraz Instrukcją zarządzenia systemem informatycznym służącym do przetwarzania osobowych w Urzędzie Miasta i Gminy Ostroróg.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182 z późn. zm.) zobowiązuję się do przetwarzania danych osobowych zgodnie z prawem, do ochrony danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskiwaniem danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Ostroróg , oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia/ stażu/praktyki/obowiązywania umowy*.

Jednocześnie oświadczam, że zostałem/am poinformowany/a o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

(data i podpis składającego oświadczenie)

niepotrzebne skreślić

BURMISTRZ
dr Sławomir Szałata

Załącznik nr 9
do Polityki Bezpieczeństwa

WZÓR

Raport
z naruszenia ochrony danych osobowych
w Urzędzie Miasta i Gminy Ostroróg

1. Data: ....., Godzina: .....
(dzień, miesiąc, rok) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeżeli występuje)

3. Lokalizacja zdarzenia:

(np. numer pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa:

5. Podjęte działania:

6. Przyczyny wystąpienia zdarzenia:

7. Postępowanie wyjaśniające:

8. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnych naruszeń ochrony danych osobowych.

(Data i podpis Administratora Bezpieczeństwa Informacji)

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 10 do Polityki
Bezpieczeństwa

WZÓR

Ewidencja szkoleń
w zakresie ochrony danych osobowych
w Urzędzie Miasta i Gminy Ostroróg

Lp.	Data szkolenia	Nazwisko i imię osoby szkolonej	Podpis osoby szkolonej	Podpis ABI	Podpis ASI
1	2	3	4	5	6

BURMISTRZ

dr Sławomir Szałata

Załącznik Nr 11 do
Polityki Bezpieczeństwa

Wzór

Wniosek o planowanym utworzeniu zbioru danych w Urzędzie Miasta i Gminy Ostroróg*

Wniosek o aktualizację zbioru danych w Urzędzie Miasta i Gminy Ostroróg*

1	Proponowana nazwa zbioru danych (nazwa zbioru danych powinna odpowiadać celowi przetwarzania danych oraz ich zakresowi, a także odpowiadać nazewnictwu stosowanemu w przepisach prawa). Nazwa zbioru danych podlegającego aktualizacji	
2	Podstawa prawna przetwarzania danych osobowych w zbiorze danych (należy wskazać przepis prawa lub określić przesłankę dopuszczalności przetwarzania danych określoną w art. 23 ust. lub w art. 27 ust. 2 ustawy o ochronie danych osobowych)	
3	Komórka organizacyjna/ Referat / prowadząca zbiór danych	
4	Sposób przetwarzania danych w zbiorze (system informatyczny, forma papierowa)	
5	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł	
6	Zakres przetwarzania danych (należy wskazać kategorie danych osobowych przetwarzanych w zbiorze danych)	
7	Cel przetwarzania danych osobowych w zbiorze danych	
8	Opis kategorii osób, których dane będą przetwarzane	
9	Sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa	
10	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane	

	mogą być przekazywane,	
11	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	
12	Uzasadnienie potrzeby utworzenia zbioru danych	

data i podpis właściciela zbioru

* niepotrzebne skreślić

Uwaga - w przypadku wniosku o aktualizację zbioru danych, należy wypełnić pola w których dane podlegają aktualizacji.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 12 do Polityki
Bezpieczeństwa

WZÓR

Ewidencja programów komputerowych stosowanych do przetwarzania danych oraz opis sposobu przepływu danych pomiędzy poszczególnymi systemami

Lp.	Nazwa program u	Podstawa prawna użytkowania programu Umowa/ licencja	Miejsce instalacji programu/ użytkownik	Zakres gromadzonych i przetwarzanych danych	Formy zabezpieczenia	Sposób przesyłania danych osobowych	Kierunek przepływu danych osobowych	Uwagi
1	2	3	4	5	6	7	8	9
1	aktualizacja							
	aktualizacja							

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 13 do Polityki
Bezpieczeństwa

Ewidencja podmiotów, którym powierzono przetwarzanie danych

Lp.	Nazwa podmiotu, któremu powierzono przetwarzanie danych	Podstawa prawna powierzenia przetwarzania/ Nr umowy	Data powierzenia	Zakres powierzenia	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

BURMISTRZ
dr Sławomir Szałata

Załącznik nr 2 do
Zarządzenia Nr 70/2017
Burmistrza Miasta i Gminy Ostroróg
z dnia 6 października 2017 r.

INSTRUKCJA
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg

§ 1. 1. Postanowienia ogólne.

Niniejsza Instrukcja reguluje sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg, z uwzględnieniem wymogów określonych w rozporządzeniu 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 (Dz. U. Nr 100, poz. 1024).

2. Celem Instrukcji jest określenie procedur bezpiecznego przetwarzania danych osobowych w systemach informatycznych Urzędu Miasta i Gminy Ostroróg.

3. Zapisy Instrukcji dotyczą ochrony danych osobowych, przetwarzanych w systemach informatycznych w budynku Urzędu Miasta i Gminy Ostroróg przy ul. Wronieckiej , do których dostęp zapewnia lokalna sieć komputerowa, oraz w urządzeniach przenośnych stanowiących własność Urzędu.

4.Nadzór nad przestrzeganiem zasad ochrony opisanych w niniejszej instrukcji pełnią: Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego.

Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym, zobowiązani są do zapoznania się z treścią niniejszej Instrukcji i jej przestrzegania.

5. Fakt zapoznania się z Instrukcją pracownik potwierdza własnoręcznym podpisem w stosownym oświadczeniu.

§ 2. Definicje.

Przez użyte w niniejszym dokumencie określenia, należy rozumieć:

1) Sieć lokalna - połączenie komputerów pracujących w Urzędzie w celu wymiany danych dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,

2) Sieć rozległa (publiczna) – sieć telekomunikacyjna nie będąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy - Prawo telekomunikacyjne.

3) Wykaz zbiorów danych osobowych - wykaz zarejestrowanych jak i nie podlegających rejestracji zborów danych osobowych, przetwarzanych Urzędzie.

§ 3. 1. Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym.

Administratorem systemów informatycznych, będących własnością Urzędu jest Administrator Systemów Informatycznych.

2. Do obsługi programu komputerowego, oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, dostęp ma wyłącznie użytkownik, posiadający pisemne upoważnienie Administratora Danych Osobowych.

3. Uprawnienia wygasają z chwilą rozwiązania stosunku pracy lub pisemnego cofnięcia uprawnień.

4. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia, również po ustaniu zatrudnienia.

5. Administrator Systemów Informatycznych niezwłocznie rejestruje i wyrejestrowuje użytkowników w systemie informatycznym, którzy uzyskują lub tracą prawo dostępu do danych.

6. Administrator Systemów Informatycznych przydziela użytkownikowi identyfikator, oraz pierwsze hasło. Identyfikator osoby, która utraciła uprawnienia nie może być przydzielony innej osobie.

7. Hasło użytkownika jest składowane w systemie w bezpieczny sposób.

8. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.

9. Dostęp do danych możliwy jest wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia za pomocą hasła lub poprawnej weryfikacji karty SMART.

10. Administrator Systemów Informatycznych w sytuacji awaryjnej może zmienić hasło poprzez usunięcie obecnego, zapomnianego przez użytkownika hasła i nadanie nowego hasła, wymagającego zmiany w trakcie pierwszego logowania.

§ 4.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1.Użytkownikowi upoważnionemu do przetwarzania danych, hasło przekazuje ustnie Administratorowi Systemów informatycznych. Użytkownik nie może udostępniać identyfikatora, hasła i stanowiska roboczego innej osobie.

2. Hasło musi się składać z co najmniej 8 znaków. Należy stosować hasła zawierające kombinacje liter, cyfr i znaków specjalnych. Zakazuje się stosowanie haseł zawierających nazwę użytkownika, własnego imienia i nazwiska, ogólnodostępnych informacji o użytkowniku, oraz przewidywalnych sekwencji znaków z klawiatury.

3. Użytkownik obowiązany jest zmienić hasło niezwłocznie po przekazaniu, a następnie nie rzadziej, niż co 30 dni. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych.

4. Hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik. Zabronione jest przekazywanie hasła innym osobom.

§ 5.

1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

Bezpośredni dostęp do danych, w zależności od stosowanego zabezpieczenia, użytkownik ma po poprawnym zweryfikowaniu karty dostępu lub podaniu identyfikatora i właściwego hasła. Użytkownik nie może udostępniać karty dostępu, identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym.

2. Użytkownik ma obowiązek zamykania systemu, programu po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostawać bez kontroli pracującego na nim użytkownika.

3. Użytkownik zobowiązany jest do takiego usytuowania monitora, aby uniemożliwić przypadkowy wgląd do danych osobom nieuprawnionym.

4. W celu zabezpieczenia danych przed wglądem osób nieuprawnionych w przypadku tymczasowego zaprzestania pracy na stanowiskach, na których przetwarzane są dane osobowe, zainstalowana zostać musi funkcja wygaszania ekranu aktywująca się po kilku minutach bezczynności.

5. Zabrania się:

1) wykorzystywania sieci komputerowej do celów innych niż wyznaczone przez Administratora Danych Osobowych,

2) samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),

3) trwałego lub czasowego kopiowania programów komputerowych w całości lub części, jakimikolwiek środkami i w jakiejkolwiek formie,

4) rozpowszechniania programów komputerowych lub ich kopii wśród osób postronnych,

5) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne,

6) tłumaczenia, przystosowywania, zmiany układu, lub dokonywania jakichkolwiek innych zmian w programie komputerowym,

7)używania nielegalnych oprogramowań,

8) udostępniania osobom postronnym programów komputerowych, przez możliwość dostępu do zasobów sieci,

9) używania nośników danych (FDD, HDD, urządzenia mobilne: Pen Drive - USB, Karty Flash), które można podejrzewać o zainfekowanie wirusem.

6. Użytkownik ma obowiązek niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub upoważnioną przez niego osobę oraz Administratora Systemów Informatycznych o:

1) podejrzeniach naruszenia bezpieczeństwa systemu (brak możliwości zalogowania się użytkownika na jego konto),

2) stwierdzeniu fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe.

§ 6.

Procedury tworzenia kopii zapasowych zbiorów oraz kopii zapasowych systemu informatycznego używanych do ich przetwarzania oraz sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe, i kopii zapasowych.

1. Administrator Systemów Informatycznych wykonuje i nadzoruje regularne wykonywanie kopii zapasowych danych przetwarzanych w systemach dla wszystkich baz SQL'owych i bazy z programów działających pod DOS'em.

2. Kopie wykonywane są przy pomocy aktualnie licencjonowanych oprogramowań, służących do zarchiwizowania danych na nośnikach zewnętrznych, oraz poprzez wykonywanie kopii w urządzeniach obsługujących aktualne standardy zapisu danych.

3. Kopie wykonywane są na nośniki: DVD, taśmy do STREAMERA

4. Nośniki z kopiami zapasowymi przechowywane są w pomieszczeniu zabezpieczonym w bezpiecznej metalowej szafie.

5.Wykonywanie kopii bezpieczeństwa odbywa się każdego dnia w porze zmniejszonego obciążenia serwerów. Następnie raz na tydzień wykonywana jest kopia bezpieczeństwa tygodniowa, archiwizowana na nośnik zewnętrzny. Kopie: codzienna, tygodniowa, miesięczna, kwartalna i roczna, są kopiami całościowymi.

6. Administrator Systemów Informatycznych okresowo sprawdza dalszą przydatności nośników z kopiami zapasowym; nośniki nieprzydatne pozbawia zapisu w sposób uniemożliwiający ich odczytanie lub likwiduje poprzez fizyczne zniszczenie Z czynności tych sporządza notatki służbowe, które przechowywane są w pomieszczeniu z serwerem.

7. Administrator Systemów Informatycznych przeprowadza w okresach półrocznych testy kopi bezpieczeństwa.

8. Na stacjach roboczych zainstalowane jest specjalistyczne oprogramowanie antywirusowe mające na celu wychwycenie i zatrzymanie próby infekcji z urządzeń podłączanych do komputera przez użytkownika.

9. Ochronę przed awariami zasilania, oraz zakłóceniami w sieci energetycznej serwerów i stacji roboczych zapewnia zasilacz centralny UPS.

10. W celu zminimalizowania możliwości zainstalowania się szkodliwego oprogramowania podejmowane są czynności profilaktyczne:

1) okresowe sprawdzanie sprawności i skuteczności sprzętu komputerowego zainstalowanego w tutejszym Urzędzie, mające na celu usunięcie nieprawidłowości lub oprogramowania mogącego przyczynić się do niestabilności systemu na poszczególnych stacjach roboczych,

2) stosowanie narzędzi programowych poprzez instalowanie na każdej stacji roboczej (komputerze) z dostępem do aplikacji i danych osobowych systemu antywirusowego. System antywirusowy konfiguruje się w sposób umożliwiający jego samoczynne uruchomienie się i rozpoczęcie nieprzerwanej ochrony przez cały czas pracy tej stacji począwszy od momentu jej włączenia. Instalacja, konfiguracja, uruchomienie i ochrona antywirusowa odbywa się bez wiedzy użytkownika (w tle jego pracy).

11. Osobą odpowiedzialną za zarządzanie oprogramowaniem jest Administrator Systemów Informatycznych, który dokonuje kontroli zastosowanych zabezpieczeń, oraz analizuje ich adekwatność i wskazuje nowocześniejsze środki zabezpieczeń.

12. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych:

1) prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm - serwisantów, pod nadzorem Administratora Systemów informatycznych bez możliwości dostępu do danych osobowych,

2) urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych w sposób trwały lub naprawia się je pod nadzorem Administratora Systemów Informatycznych lub osoby przez niego upoważnionej.

§ 8. 1. Zasady postępowania z komputerami przenośnymi.

Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.

2. Użytkownikom powierza się komputery przenośne na podstawie protokołu powierzenia. Protokół przygotowuje Administrator Systemów Informatycznych.

3. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu.

4. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne, niż użytkownicy, którym zostały one powierzone.

§ 9. 1. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

Danych osobowych w postaci elektronicznej zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych nie można wynosić poza siedzibę Urzędu.

2. Wymienne elektroniczne nośniki i informacji przechowywać należy wyłącznie w zamykanych szafach biurowych w pomieszczeniach stanowiących obszar przetwarzania danych określony w Polityce Bezpieczeństwa Danych Osobowych Urzędu Miasta i Gminy Ostroróg.

3.Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.

4. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe uszkadza w sposób uniemożliwiający ich odczytanie.

5. Wydruki zawierające dane osobowe przechowuje się w miejscu i w sposób uniemożliwiającym dostęp osobom nieupoważnionym, a po upływie ich przydatności, niszczone są w sposób uniemożliwiający ich odczytanie.

§ 10. 1. Postanowienia końcowe.

W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

2. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez użytkowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia, na podstawie art.52 Kodeksu Pracy.

3. Zapisy niniejszej instrukcji, dotyczące zabezpieczeń, wykonywania kopii zapasowych i ich przechowywania, maja również zastosowanie do systemów teleinformatycznych, objętych siecią wewnętrzną Urzędu, które nie służą do przetwarzaniu danych osobowych.

4. Administrator Systemów Informatycznych raz do roku przeprowadza analizę ryzyka dla systemów teleinformatycznych, a także w przypadku istotnej zmiany warunków funkcjonowania systemu teleinformatycznego.

5. Wzór protokołu powierzenia komputera przenośnego do wyłącznego użytkowania pracownikowi Urzędu stanowi załącznik do Instrukcji.

Burmistrz Miasta i Gminy Ostroróg

BURMISTRZ
dr Sławomir Szałata

Załącznik do Instrukcji

Protokół
powierzenia komputera do wyłącznego użytkowania

Sporządzony w dniu: .....pomiędzy:

Pracodawcą - Urząd Miasta i Gminy Ostroróg, ul. Wroniecka 14, 64-560 Ostroróg - reprezentowany przez .....
a
Pracownikiem .....o *(imię i nazwisko)*

§ 1. Pracownik potwierdza, że otrzymał do wyłącznego korzystania w celach służbowych zestaw komputerowy składający się z następujących elementów:

a)

b)

c)

d)

e)

liczba elementów w zestawie:.....(słownie)

Numer identyfikacyjny zestawu nadany przez Referat Finansowy .....

§ 2 Na powyższym komputerze zainstalowane zostało następujące oprogramowanie (nazwa i numer seryjny lub numer licencji):

a) .....
b) .....
c) .....
d) .....
e) .....

§ 3. Przekazany komputer wykorzystywany będzie jedynie w celach służbowych. Zakazuje się instalowania programów mogących powodować wypływ informacji. Zabrania się również instalowania oraz korzystania z oprogramowania czy witryn internetowych powodujących spadek wydajności pracy, dotyczy to wszelkiego rodzaju gier komputerowych, gier on-line czy portali.

§ 4. Pracownik, któremu został przekazany komputer potwierdza, że został pouczony o bezwzględnym zakazie instalowania lub przechowywania na dysku komputera danych pochodzących z wszelkiego rodzaju nośników informacji,

mogących naruszać prawa autorskie podmiotów trzecich.

§ 5. Pracownik, któremu został przekazany sprzęt komputerowy określony w § 1 niniejszego protokołu, ponosi odpowiedzialność materialną określoną w Kodeksie Pracy za szkodę wyrządzoną pracodawcy ze swej winy w związku z niewykonaniem lub niewłaściwym wykonaniem swoich obowiązków.

§ 6. Pracownik zobowiązany jest chronić powierzony sprzęt komputerowy przed uszkodzeniem, kradzieżą i dostępem osób postronnych, z zachowaniem szczególnej ostrożność podczas transportu.

§ 7. Pracownik zobowiązany jest przestrzegać zasad określonych w Polityce bezpieczeństwa i Instrukcji obowiązujących w Urzędzie Miasta i Gminy Ostroróg.

§ 8. Powierzenie następuje na czas .....

Data i podpis Pracownika

Data i popis Pracodawcy

BURMISTRZ
dr Sławomir Szałata