SO.0050.28.2018

ZARZĄDZENIE NR 28.2018

Wójta Gminy Rogowo

z dnia 23 maja 2018 r.

w sprawie: wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie.

Na podstawie art. 24 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz art. 33 ust.3 ustawy z dnia 8 marca 1990 o samorządzie gminnym (T. j. Dz. U. z 2017 r. poz. 1875 ze zm.) zarządza się, co następuje:

§ 1

Wprowadza się „Politykę Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie", która stanowi załącznik nr1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy w Rogowie do stosowania zasad określonych w „Polityce Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie".

§ 3

Traci moc zarządzenie nr 6.2016 Wójta Gminy Rogowo z dnia 01 lutego 2016 roku w sprawie: wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Rogowie oraz przyjęcia instrukcji zarządzania systemem informatycznym.

§ 4

Zarządzenie wchodzi w życie z dniem 25 maja 2018 roku.

WÓJT

mgr Barbara Nowakowska

Sporządziła:
Anna Ostrowska

Załącznik nr 1
do Zarządzenia
Wójta Gminy Rogowo
nr 28.2018
z dnia 23.05.2018

Polityka Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie

Spis treści

Wstęp

1. Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora a także Podmiot przetwarzający w celu spełnienia wymagań określonych Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.
3. Ilekroć w Polityce jest mowa o:
   a) administratorze – rozumie się przez to Wójta Gminy Rogowo,
   b) jednostce – rozumie się przez to Urząd Gminy w Rogowie,
   c) danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
   d) zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest zcentralizowany, czy rozproszony funkcjonalnie lub graficznie,
   e) przetwarzaniu danych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
   f) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
   g) systemie tradycyjnym - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,
   h) kierowniku referatu – rozumie się kierowników referatów oraz samodzielne stanowiska pracy,
   i) zgodzie – rozumie się przez to zgodę osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
   j) podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,

Dział I

Ewidencja danych.

1. Dane osobowe w Urzędzie Gminy w Rogowie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz innych zestawach i zbiorach ewidencyjnych poszczególnych referatów i samodzielnych stanowisk pracy, na dokumentach papierowych, jak również w systemach informatycznych, w których stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy), a także na elektronicznych nośnikach informacji.
2. Zestawienie danych osobowych wymagających ochrony wykazano w załączniku nr 1a – Rejestr zbiorów danych osobowych.
3. Rejestr obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.
4. Poszczególne zbiory opisane są w sposób umożliwiający przeprowadzenie analizy ryzyka.
5. Kierownik referatu zgłasza każdorazowo do inspektora danych osobowych rejestrację nowego zbioru danych osobowych oraz przygotowuje w tej sprawie wniosek stanowiący załącznik nr 1b – wniosek o rejestrację zbioru.

Dział II

Zgodność z prawem

1. Administrator danych osobowych zapewnia, że:
   a) dane osobowe przetwarzane są zgodnie z prawem,
   b) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach,
   c) dane osobowe są optymalne do celów przetwarzania (minimalizacja danych),
   d) dane osobowe przetwarzane są przez sprecyzowany czas,
   e) wobec osób, których administrator przetwarza dane osobowe wykonano obowiązek informacyjny wraz ze wskazaniem wszelkich przysługujących praw (m.in. sprostowania, usunięcia, przenoszenia danych, prawo ograniczenia przetwarzania, sprzeciwu),
   f) zapewniono gwarancję ochrony danych osobowych w przypadku powierzenia przetwarzania danych w postaci umów powierzenia. Rejestr umów powierzenia wykazano w załączniku 2a.
2. Potwierdzenie zgodności z prawem przetwarzania danych osobowych w zbiorach określono w załączniku nr 1a – Rejestr zbiorów danych osobowych.
3. Klauzule informacyjne znajdują się w załączniku nr 2b -Klauzule informacyjne.

Dział III

Upoważnienia

1. Administrator danych osobowych odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych osobowych.
2. Do informacji przechowywanych, tworzonych w systemach tradycyjnych (papierowych) jak i systemach informatycznych mają dostęp jedynie osoby mające imienne, zarejestrowane upoważnienie, którego wzór stanowi załącznik nr 3a-Upoważnienie do przetwarzania danych osobowych.

3. Upoważniona osoba musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
4. Upoważnienia nadawane są na wniosek kierownika referatu. Wzór wniosku o nadanie upoważnienia stanowi załącznik nr 3b -Wniosek o nadanie upoważnienia do przetwarzania danych osobowych.
5. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych, co zostało wykazane w załączniku nr 3c - Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Dział IV

Analiza oceny ryzyka

1. Analiza oceny ryzyka precyzuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zagrożeń.
2. W przypadku konieczności przeprowadzenia oceny skutków dla ochrony danych, w celu zapewnienia najwyższego poziomu bezpieczeństwa, wymagane jest wykonanie co najmniej:
   1. systematycznego opisu planowanych operacji przetwarzania i celów przetwarzania - zawarty w załączniku nr 1a - Rejestr zbiorów danych osobowych,
   2. ocenę, czy operacje przetwarzane są niezbędne oraz proporcjonalne do celów zostało zawarte w załączniku nr 1a - Rejestr zbiorów danych osobowych,
   3. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą - załącznik nr 4a - Procedura analizy ryzyka,
   4. środki planowane w celu zapewnienia bezpieczeństwa - załącznik nr 4a - Procedura analizy ryzyka.

Dział V

Procedura postępowania z naruszeniami

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do powiadomienia o stwierdzeniu podatności lub wystąpieniu incydentu zagrażającemu bezpieczeństwu danych osobowych inspektorowi ochrony danych osobowych.
2. W przypadku wystąpienia incydentu inspektor ochrony danych prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   d) rekomenduje działania zapobiegawcze zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejsza straty w momencie ich zaistnienia.
3. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze na formularzu stanowiącym załącznik nr 5a - Formularz rejestracji incydentu.
4. Zabrania się świadomego lub nieumyślnego wywoływania incydentu przez osoby upoważnione do przetwarzania danych.

5. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu.
6. W przypadku naruszenia ochrony danych osobowych powodujących wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Dział VI

Instrukcja ochrony danych osobowych

1. Instrukcja ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe w zakresie bezpiecznych zasad przetwarzania danych osobowych. Instrukcję stanowi załącznik nr 6a – Instrukcja ochrony danych osobowych w Urzędzie Gminy w Rogowie.
2. Z zasadami ochrony danych osobowych obowiązani są wszyscy użytkownicy systemów tradycyjnych i informatycznych składając odpowiednie oświadczenie, którego wzór stanowi załącznik nr 6b – Oświadczenie tajności.

Dział VII

Szkolenia

1. Każda osoba przed rozpoczęciem pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznaniu z przepisami z zakresu ochrony danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada inspektor ochrony danych.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia szkolenia, załącznik nr 7a – Plan szkolenia.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, załącznik nr 6b – Oświadczenie tajności.

Dział VIII

Rejestr czynności przetwarzania

1. Inspektor ochrony danych prowadzi rejestr czynności przetwarzania – załącznik nr 8a – Rejestr czynności prowadzonych przez Administratora.

Dział IX

Kontrole

1. Administrator powinien regularnie testować, sprawdzać i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu Administrator stosuje procedurę kontroli – załącznik nr 9a – Procedura kontroli.

Dział X

Instrukcja przywrócenia dostępności danych osobowych i dostępu do nich w razi incydentu (plany awaryjne i zapobiegawcze)

1. Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego czy technicznego. Procedurę określa załącznik nr 10a – Plan ciągłości działania.

Dział XI

Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które zostały zastosowane w celu ochrony danych osobowych – załącznik nr 11a – Wykaz zabezpieczeń.
2. Wykaz jest aktualizowany po każdej analizie ryzyka.

01a Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych (1)	Aktywa 1. Informacje 2. Programy i systemy operacyjne 3. Infrastruktura IT 4. Infrastruktura 5. Pracownicy i współpracownicy 6. Outsorcing	Podstawa przetwarza-nia	Rejestr czynności przetwarzania	Ocena skutków	Cel przetwarzania Rodzaj i zakres danych Odbiorcy	Opis operacji przetwarzania	Czas przecho-wywania

1b – Wniosek o rejestrację / aktualizację / wykreślenie zbioru

1. **Data wpisu, data aktualizacji treści wpisu albo data wykreślenia wpisu**

2. **Nazwa zbioru danych**

3. **Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki, jeżeli został mu nadany**

4. **Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 28 RODO, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;**

   Nazwa podmiotu, któremu powierzono przetwarzanie danych

   Adres podmiotu, któremu powierzono przetwarzanie danych

5. **Podstawa prawna upoważniająca do prowadzenia zbioru danych;**

6. **Cel przetwarzania danych w zbiorze**

7. **Rodzaj i zakres danych przetwarzanych w zbiorze**

8. **Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;**

9. **Czas przechowywania:**

10. **Programy wykorzystywane do przetwarzania danych zawartych w zbiorze**

11. **Sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa**

12. **Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;**

13. **Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego**

14. **Wzmianka o wykreśleniu wpisu**

15. **Uwagi**

Kierownik referatu

.....

2a - Rejestr umów powierzenia

Lp.	Nr umowy i data zawarcia	Nazwa podmiotu, z którym została zawarta umowa	Data nadania uprawnień	Data ustania uprawnień

2b - Klauzula informacyjna dla klientów urzędu

Treść klauzuli	Sposób wprowadzenia
Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż: 1) administratorem Pani/Pana danych osobowych jest Nazwa Administratora) z siedzibą w (Adres Administratora), 2) kontakt z Inspektorem Ochrony Danych - , 3) Pani/Pana dane osobowe przetwarzane będą w celu realizacji ustawowych zadań urzędu - na podstawie Art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz na podstawie Art. 9 ust.1 lit. g ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r 4) odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa 5) Pani/Pana dane osobowe przechowywane będą w czasie określonym przepisami prawa, zgodnie z instrukcją kancelaryjną 6) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania 7) ma Pani/Pan prawo wniesienia skargi do organu nadzorczego 8) podanie danych osobowych w zakresie wymaganym ustawodawstwem (<podać zakres aktów prawnych na podstawie których działa dany urząd>) jest obligatoryjne * tekst jest opcjonalny	• w postaci wywieszki na tablicy ogłoszeń • na stronie BIP urzędu

3a - Upoważnienie do przetwarzania danych osobowych w systemach informatycznych i zbiorach w wersji papierowej

Dnia ..... Administrator Danych nadaje upoważnienie do przetwarzania danych osobowych w systemach informatycznych i zbiorach w wersji papierowej w podmiocie ..... dla:

Imię i nazwisko: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

.....

.....

.....

Upoważniony otrzymuje dostęp do poniższych systemów informatycznych w celu przetwarzania danych osobowych:

.....

.....

.....

Upoważnienie nadaje się do dnia .....

Administrator Danych

.....

Podpis

Użytkownik

.....

Podpis

3b – Wniosek o nadanie upoważnienia

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr ..... do przetwarzania danych osobowych w systemach informatycznych lub w zbiorach w wersji papierowej

Część I

Z dniem ..... wnioskuję o nadanie upoważnienia do przetwarzania danych osobowych w systemach informatycznych i zbiorach w wersji papierowej dla:

Imię i nazwisko: .....

Stanowisko służbowe: .....

Część II

Wnioskuję o nadanie upoważnienia dla w/w osoby do poniższych zasobów danych osobowych w celu ich przetwarzania:

1. .....
2. .....
3. .....

Wnioskuję o nadanie upoważnienia do dnia .....

Część III

Wnioskuje o nadanie upoważnienia w systemach informatycznych przetwarzających dane osobowe:

Dostęp do systemu Informatycznego Urzędu: ☐TAK ☐NIE

SYSTEM INFORMATYCZNY	**[3]IDENTYFIKATOR**	**MODUŁY/ROLE/KATALOGI**	
		Dostęp: TAK ☐ NIE ☐	☐ Administrator,☐ Użytkownik
		Dostęp: TAK ☐ NIE ☐	Pełny dostęp
		Dostęp: TAK ☐ NIE ☐	Pełny dostęp

Część IV

Pozostałe uprawnienia.

Dostęp do poczty internetowej ☐TAK ☐NIE

Nadano adres poczty internetowej.....

Część V

Anulowanie upoważnienia

Wnioskuje o anulowanie upoważnienia nr ..... dla w/w osoby od dnia.....

Przyczyna odebrania niniejszego upoważnienia

.....

.....

.....

.....

Oświadczam, że niniejszy zakres uprawnień jest niezbędny do realizowania obowiązków służbowych (wynikających z umowy) przez osobę, której dotyczy upoważnienie.

....

(miejscowość i data) (pieczęć i podpis kierownika referatu)

3c - Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i imię	Stanowisko	Nazwa referatu	Data przeszko-lenia	Nr upoważn ienia imienneg o	Zakres upoważnienia	Data nadania upoważnie -nia	Data ustania upoważnien ia
1.								

4a - Procedura analizy ryzyka

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent)
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

1 WYZNACZENIE ZBIORÓW DO ANALIZY RYZYKA Z AKTYWAMI

1. Analizie ryzyka poddawane są zbiory danych osobowych lub procesy przetwarzania.
2. Do analizy wymagane jest zidentyfikowanie aktywów.
3. Przykładowe aktywa:

    - dane osobowe,
    - dane dostępowe (loginy, hasła, piny),
    - dane dotyczące zabezpieczeń (certyfikaty, klucze szyfrujące)
    - dokumentacja techniczna,
    - polityki bezpieczeństwa,
    - umowy,
    - programy i systemy operacyjne,
    - sprzęt komputerowy,
    - telekomunikacja,
    - nośniki danych,
    - obszary chronione (serwerownie, rozdzielnie elektryczne),
    - sprzęt wspomagający (klimatyzatory, zasilacze awaryjne, agregaty),
    - pracownicy i współpracownicy (kompetencje, doświadczenia).

2 WYZNACZENIE ZAGROŻEŃ

1. Administrator z ewentualnym współudziałem IOD jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania
2. Zagrożenia powinny być identyfikowane w odniesieniu do aktywów.
3. Przykładowe zagrożenia:

- wyłudzanie informacji,
- nakłanianie do wykonywania czynności,
- podrzucanie nośników danych,
- ataki telefoniczne,
- łamanie haseł,
- ataki na sprzęt,
- ataki na oprogramowanie,
- skanowanie sieci i usług,
- podsłuchiwanie transmisji,
- wirusy,
- kradzież/zniszczenie sprzętu,
- pożar/eksplozja,
- zalanie,
- przegrzanie,
- awaria zasilania,
- awaria sprzętu,
- nieuprawniony dostęp,
- kradzież tożsamości,
- nieuprawniona modyfikacja/usunięcie,
- nieuprawnione kopiowanie danych,
- kradzież danych lub nośników,
- utrata/kradzież danych dostępowych (hasła, klucze),
- błąd/awaria oprogramowania,
- brak/błąd w wykonaniu kopii bezpieczeństwa,
- udostępnianie danych osobowych osobom nieupoważnionym,
- fałszowanie danych,
- nieprzestrzeganie procedur,
- pomyłki,
- brak świadomości/wiedzy,
- brak aktualnej dokumentacji,
- nieprawidłowe/brak umowy o współpracy.

3 WYLICZENIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B

5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie, nie ma realnej szansy wystąpienia zidentyfikowanego zagrożenia, zagrożenie nigdy nie wystąpiło	1
zagrożenie średnie, zagrożenie jest mało realne, zagrożenie nie wystąpiło w okresie ostatnich 24 miesięcy	2
zagrożenie wysokie, zagrożenie jest realne, zagrożenie wystąpiło w okresie ostatnich 24 miesięcy	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (incydent prasowy lokalny, wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa, zagrożenie nie powoduje strat finansowych lub znikome straty do 10000 PLN)	1
średnie (incydent prasowy ogólnopolski, wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa z wyłączeniem przepisów karnych, lub w przypadku podjęcia odpowiednich działań naprawczych naruszenie prawa zostanie uniknione, wystąpienie zagrożenia spowoduje straty finansowe w przedziale 10000-100000 PLN,)	2
duże (bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych, wystąpienie zagrożenia spowoduje straty finansowe powyżej 100000 PLN,)	3

4 PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZYKIEM

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

5 REAKCJA NA WARTOŚĆ RYZYKA

1. Akceptacja ryzyka - zabezpieczenia są właściwe - brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie -przerzucenie ryzyka (ubezpieczenie)
    b. Unikanie - eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar urzędu)
    c. Redukcja - zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrive z danymi wynoszonych poza urząd)
3. Przykładowe zabezpieczenia:

- instrukcja ochrony danych osobowych,
- szkolenia pracowników,
- kontrole,
- ograniczenie dostępu do pomieszczeniem osobom nieupoważnionym,
- zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucze, kraty w oknach),
- system p.poż.
- system UPS,
- systemy antywirusowe,
- zmiana domyślnych haseł,
- wymuszanie zmiany hasła,
- częstotliwość zmiany haseł,
- wygaszacze ekranów,
- niszczenie nośników, dokumentów tylko w urządzeniach do tego przeznaczonych,
- stosowanie umów powierzenia.

6 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

7 PONOWNA ANALIZA RYZYKA

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 3 lata.

5a- Formularz rejestracji incydentu

Data i godzina zdarzenia	Ilość osób dotkniętych incydentem/ naruszeniem	Opis incydentu/naruszenia	Skutki incydentu/naruszenia	Działania naprawcze	Data rozpoczęcia wdrożenia działania	Data zakończenia wdrożenia działania	Osoba odpowiedzialna za wdrożenie działań

6a - Instrukcja Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie

Niniejsza instrukcja stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

1 DEFINICJE ZAWARTE W INSTRUKCJI

1. Ilekroć w Instrukcji jest mowa o:
   a) administratorze – rozumie się przez to Wójta Gminy Rogowo,
   b) jednostce – rozumie się przez to Urząd Gminy w Rogowie,
   c) danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
   d) zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest zcentralizowany, czy rozproszony funkcjonalnie lub graficznie,
   e) przetwarzaniu danych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
   f) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
   g) identyfikator użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważniona do przetwarzania danych osobowych w systemie informatycznym,
   h) hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie upoważnionej do pracy w systemie informatycznym,
   i) Administrator Systemów Informatycznych (ASI) – zwany także Administratorem Systemu rozumie się przez to osobę - informatyka, upoważnionego prze Administratora Danych Osobowych do realizacji zadań związanych z zarządzaniem systemem informatycznym,
   j) Użytkownik systemu informatycznego – rozumie się przez to upoważnionego przez Administratora Danych Osobowych pracownika urzędu do przetwarzania danych osobowych w systemie informatycznym.

2 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu.**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe,
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa.

3 ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-Administratorów Systemów informatycznych.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows 7/10.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

4 POLITYKA HASEŁ

1. Hasła powinny składać się z np. 12 znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co 60 / 90 dni.

7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

5 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. **„Polityki czystego biurka"**. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych lub w lesie.

6 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA URZĄD

1. Użytkownicy nie mogą wynosić na zewnątrz urzędu wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy. Do takich nośników zalicz się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza urząd muszą być zaszyfrowane (szyfrowane dyski, za hasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

7 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ASI i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza urząd może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza urząd należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
7. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości - UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
12. Użytkownicy powinni okresowo kasować niepotrzebne maile.

13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
17. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
18. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
19. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

9 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI.

10 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest niezwłocznie do powiadomienia Pracodawcy / Inspektora Ochrony Danych Osobowych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b. dokumentacja jest niszczona bez użycia niszczarki,
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy,
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   h. telefoniczne próby wyłudzenia danych osobowych,
   i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
   j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   l. hasła do systemów przyklejone są w pobliżu komputera.

11 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę zadaniach,
   b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

2. Osoba upoważniona do przetwarzania danych osobowych odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

12 WYREJESTROWANIE UŻYTKOWNIKA

1. Każdą z osób upoważnionych do przetwarzania danych osobowych jest zobowiązany do Wyrejestrowania z systemu informatycznego Administrator Systemu na wniosek kierownika referatu.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:

a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

a) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
b) zawieszenie w pełnieniu obowiązków służbowych,
c) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

13. KOPIE ZAPASOWE

1. Kopie awaryjne tworzy się z następującą częstotliwością:

a) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
b) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.
6. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
7. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

8. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
9. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

13 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Potwierdzam własnoręcznym podpisem, iż zapoznałem /łam się z powyższą instrukcją oraz zobowiązać się do stosowania zasad w nim zawartych.		
Lp.	Nazwisko i imię	Czytelny podpis

Potwierdzam własnoręcznym podpisem, iż zapoznałem /łam się z powyższą instrukcją oraz zobowiązać się do stosowania zasad w nim zawartych.

Lp.	Nazwisko i imię	Czytelny podpis

6b- Oświadczenie tajności

OŚWIADCZENIE

Imię i nazwisko	
Stanowisko służbowe	

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Ustawy o Ochronie Danych Osobowych oraz odnośnymi wymaganiami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych *)
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych a następnie przekazanie ich do dyspozycji osób upoważnionych
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Ustawy o Ochronie Danych osobowych a od dn. 25.05.2018 Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

.....
(data i podpis składającego oświadczenie)

6b- Oświadczenie tajności uniwersalne

OŚWIADCZENIE

Imię i nazwisko	
Stanowisko służbowe	
Nazwa referatu	

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Ustawy o Ochronie Danych Osobowych oraz odnośnymi wymaganiami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Ustawy o Ochronie Danych osobowych a od dn. 25.05.2018 Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

....

(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

(data i podpis składającego oświadczenie)

7a - Plan szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia.....
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z Internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

Lista uczestników szkolenia z zakresu Ochrony Danych Osobowych

Prowadzący:

Miejsce i data szkolenia:

L.P.	Imię uczestnika	Nazwisko uczestnika	Podpis

9	10	11	12	13	14	15	16
[illegible]	Nazwa podmiotu przetwarzającego i dane kontaktowe	Kategorie odbiorców	Nazwa systemu lub oprogramowania	Opisy środków technicznych i organizacyjnych	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer (art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
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

9a - Procedura kontroli

Celem kontroli wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Kontrole prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie kontrolują własnej pracy.

1. Administrator (ewentualnie IOD) jest odpowiedzialny za planowanie i przeprowadzanie kontroli wewnętrznych z roczną częstotliwością lub częściej
2. Administrator (ewentualnie IOD) opracowuje programy kontroli biorąc pod uwagę ważność procesów przetwarzania oraz kontrolowanych obszarów, jak też wyniki wcześniejszych kontroli. Określa on kryteria kontroli, jego cel, zakres i ewentualnie metody.
3. Audytor jest zobowiązany do przygotowania się do przeprowadzenia kontroli, zapoznając się z opisem kontrolowanego obszaru, stosowanych procedur i wyników poprzednich kontroli
4. Audytor realizuje działania kontrolne mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO
5. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
6. Wynik kontroli zostaje udokumentowany przez audytora i przekazany Administratorowi
7. Administrator wraz z IOD dokonuje przeglądu i analizy wyniku kontroli oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

10a - Plan ciągłości działania

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

11a- Wykaz zabezpieczeń

Kondygnacja	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
	wszystkie	sprzątaczka	drzwi zamykane na klucze, kraty	Dostęp do pomieszczeń
PIWNICA		Archiwum Urzędu Gminy w Rogowie	drzwi zamykane na klucze, kraty	
PARTER	*nr 1*	*Referat Spraw Obywatelskich*	*drzwi zamykane na klucze*	
	nr 2	Referat Spraw Obywatelskich	drzwi zamykane na klucze	
	nr 6	Referat Spraw Obywatelskich	drzwi zamykane na klucze	
I PIĘTRO	nr 8	Urząd Stanu Cywilnego	drzwi zamykane na klucze	
	nr 10	Sekretariat	drzwi zamykane na klucze	
	nr 10	Wójt	drzwi zamykane na klucze	
	nr 10	Z-ca Wójta, Sekretarz Gminy	drzwi zamykane na klucze	
	nr 11	Referat Finansowy	drzwi zamykane na klucze, roleta anty włamaniowa, alarm	
	Nr 12	Referat Spraw Obywatelskich	drzwi zamykane na klucze	
II PIĘTRO	nr 13	Referat Finansowy	drzwi zamykane na klucze	
	nr 14	Referat Finansowy	drzwi zamykane na klucze	

Kondygnacja	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
	nr 15	Referat Finansowy	drzwi zamykane na klucze	
	nr 16	Referat Ogólny	drzwi zamykane na klucze	
	nr 17	Referat Ogólny	drzwi zamykane na klucze	
	nr 18	Referat Spraw Obywatelskich Referat Ogólny	drzwi zamykane na klucze	
	nr 19	Samodzielne Stanowisko ds. Informatyki	drzwi zamykane na klucze	
	nr 20	Samodzielne Stanowisko Referat Finansowy	drzwi zamykane na klucze	