Załącznik nr 1 do Zarządzenia nr 78/2016.
Wójta Gminy Szreńsk
z dnia 21.04.2016 r.

POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH

Dotyczy przetwarzania danych osobowych w formie tradycyjnej jak i za pośrednictwem systemów informatycznych.

Dokumentację opracowano zgodnie z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*t. j. Dz. U. 2015 r. poz. 2135 z późn. zm.*).

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne *(t. j. Dz. U. z 2014 r. poz. 1114 z późn. zm.)*

- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (*Dz. U. z 2004 r. nr 100, poz. 1024*) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

- Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. (*Dz. U. 2014 r. poz. 1934*) w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. *(Dz. U. 2015 r. poz. 719)* w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. *(Dz. U. 2015 r. poz. 745)* w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów

o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

- Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych *(t. j. Dz. U. z 2016 r. poz. 113)*

Sporządził

.....

Podpis Administratora
Bezpieczeństwa Informacji

Zatwierdził

W O J T

Marek Nitczyński

Podpis Administratora
Danych Osobowych

Spis treści:

POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH

w GMINIE SZREŃSK

ROZDZIAŁ I

Postanowienia ogólne

§ 1

Użyte w Polityce Bezpieczeństwa określenia oznaczają:

1) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
2) **Administrator Danych Osobowych (ADO)** – Gmina Szreńsk reprezentowana przez Wójta Gminy Szreńsk;
3) **Administrator Bezpieczeństwa Informacji (ABI)** - osoba powołana przez Administratora Danych Osobowych na podstawie art 36, ust. 1 Ustawy o Ochronie Danych Osobowych (*tekst jednolity: Dz.U. 2015 r. poz. 2135 z późn. zm.*) odpowiedzialna za bezpieczeństwo danych osobowych, przetwarzanych zarówno w formie tradycyjnej jak i za pomocą systemów informatycznych;
4) **Administrator Systemów Informatycznych (ASI)** – osoba powołana przez Administratora Danych Osobowych odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych za pomocą systemów informatycznych;
5) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;
7) **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie;
8) **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora

Bezpieczeństwa Informacji dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (*wzór upoważnienia stanowi* ***załącznik nr 7*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)* oraz wykazana w ewidencji upoważnień *(wzór ewidencji stanowi* ***załącznik nr 8*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych);*

9) **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym;

10) **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do wykonywania w jego imieniu określonych czynności;

11) **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*).

12) **Anonimizacja dokumentu** - polegająca na wykreśleniu z jego treści różnych elementów, aby uniemożliwić identyfikację występujących w dokumencie danych osobowych;

13) **Zbieranie danych (gromadzenie)**- czynność początkowa- wyli wejście w posiadanie danych osobowych w dowolny sposób;

14) **Usuwanie danych (niszczenie)**- czynność końcowa- czyli fizyczne niszczenie danych lub taka ich modyfikacja, która uniemożliwia ustalenie osoby, której dane dotyczą;

15) **Utrwalanie**- zapisanie informacji (danych osobowych) na materialnym nośniku (papier, dysk twardy);

16) **Zmienianie**- działanie polegające na weryfikacji i aktualizacji posiadanych danych osobowych

17) **Udostępnianie danych osobowych**- objęcie w posiadanie danych osobowych przez innego administratora danych osobowych;

18) **Opracowywanie danych osobowych**- wykorzystanie danych osobowych zawartych w zbiorze w celu uzyskania zamierzonego rezultatu;

19) **Przechowywanie danych osobowych**- posiadanie danych osobowych;

20) **Wgląd do danych osobowych**- fizyczne przeglądanie zawartości zbiorów danych osobowych bez wejścia w posiadanie przeglądanego zbioru.

21) **Poufność danych** – to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2

1. Najwyższe kierownictwo jest zaangażowane w zapewnienie bezpieczeństwa ochrony danych osobowych i w związku z tym:

   1) deklaruje, że zapewnienie realizacji działalności statutowej jednostki przy zachowaniu najwyższej staranności w zakresie bezpieczeństwa przetwarzania danych osobowych jest strategicznym celem jednostki;
   2) stosuje kompleksowe podejście do zagadnień związanych z bezpieczeństwem przetwarzania danych osobowych, gdyż tylko takie postępowanie gwarantuje skuteczność podejmowanych działań;
   3) podejmuje niezbędne działania w celu likwidacji słabych ogniw w systemie zabezpieczeń;
   4) śledzi osiągnięcia w dziedzinie bezpieczeństwa danych osobowych;
   5) wdraża nowe narzędzia i metody pracy mające na celu zwiększenie ochrony danych osobowych;
   6) śledzi środowisko wewnętrzne i zewnętrzne oraz związane z nimi zmiany ryzyka;
   7) dokonuje bieżącej aktualizacji wewnętrznych procedur działania w przypadku zmiany przepisów prawa lub zmiany stanu faktycznego;
   8) prowadzi ewidencję sprzętu oraz dokonuje inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
   9) podejmuje działania mające na celu zapewnienie, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   10) zobowiązuje każdego pracownika do zapoznania się z Polityką Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych;
   11) deklaruje, że Polityka Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych będzie podlegała ciągłemu doskonaleniu w oparciu o analizy i oceny będące wynikiem sprawdzeń w zakresie przestrzegania w powyższym zakresie unormowań. Niezbędna aktualizacja będzie dokonywana również w wyniku zmian w przepisach prawnych, rozwoju technologii, a także zmian organizacyjnych warunkujących dokonanie takiej aktualizacji;
   12) ustala zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
   13) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
      a) dbałości o aktualizację oprogramowania,
      b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

2. Realizując Politykę bezpieczeństwa i ochrony przetwarzania danych osobowych podmiot opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniając:

1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
2) integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
7) niezawodność – zamierzone zachowania i skutki są spójne.

3. Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych ma na celu wyeliminowanie lub w przypadku braku możliwości, zmniejszenie prawdopodobieństwa zdarzenia oraz minimalizowania skali oddziaływania w przypadku ich wystąpienia w zakresie:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone podmiotowi;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji podmiotu;
4) strat finansowych ponoszonych w wyniku nałożonych kar;
5) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 3

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:

    1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
    2) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (*np. zmian zawartości danych, utrata bądź przejęcie całości lub części danych*);
    3) naruszenie lub próby naruszenia integralności systemu;
    4) zmianę lub utratę danych zapisanych na kopiach zapasowych;
    5) naruszenie lub próby naruszenia poufności danych lub ich części;
    6) nieuprawniony dostęp (*sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu*);
    7) udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
    8) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji zmierzające do zakłócenia działania bądź pozyskania w sposób niedozwolony (*lub w celach niezgodnych z przeznaczeniem*) danych zawartych w systemach informatycznych lub kartotekach;
    9) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

3. Naruszenia ochrony danych osobowych o których mowa w §3 ust. 1 dokonywane są przez:
    a) monitorowanie dostępu do informacji,
    b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
    c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

§ 4

W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, użytkowników oraz oprogramowanie systemowe i aplikacje w przypadku przetwarzania danych za pomocą systemu informatycznego.

ROZDZIAŁ II
Zarządzanie bezpieczeństwem danych osobowych

§ 5

1. Za przetwarzanie danych osobowych niezgodne z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w Kodeksie pracy.

2. **Administrator Danych Osobowych (ADO):**

   1) Jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa przetwarzania danych osobowych;
   2) Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   3) Prowadzi dokumentację opisującą ww. środki oraz sposób przetwarzania danych;
   4) Zapewnia kontrolę nad tym jakie dane, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
   5) Wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności (*wzór upoważnienia określa* ***załącznik nr*** *7 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*);
   6) Dokonuje bezzwłocznej zmiany uprawnień określonych w upoważnieniu pracownika uczestniczącego w procesie przetwarzania informacji w przypadku zmiany zakresu jego obowiązków;
   7) Zapoznaje osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

8) Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych;
9) Odpowiada za zgodne z prawem przetwarzanie danych osobowych;
10) Formułuje odpowiednie zapisy w umowach serwisowych podpisanych ze stronami trzecimi, które gwarantują odpowiedni poziom bezpieczeństwa informacji.

3. Zgodnie z art. 36 a ust. 1 Ustawy Administrator Danych Osobowych powołuje Administratora Bezpieczeństwa Informacji *(wzór powołania Administratora Bezpieczeństwa Informacji określa **załącznik nr 1** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).* Osoba pełniąca tę funkcję:
1) posiada pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
3) nie była kara za umyślne przestępstwo.

4. Osoba powołana na stanowisko ABI potwierdza spełnienie w/w warunków poprzez złożenie stosownych oświadczeń (oświadczenia o niekaralności, oświadczenie o pełnej zdolności do czynności prawnych i korzystania z pełni praw publicznych oraz oświadczenie o posiadaniu odpowiedniej wiedzy w zakresie ochrony danych osobowych).

5. **Administrator Bezpieczeństwa Informacji (ABI)**:

1) Zapewnia przestrzeganie przepisów o ochronie danych osobowych, w szczególności przez:
   1. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   2. nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 Ustawy, oraz przestrzegania zasad w niej określonych,
   3. zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2) Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7;
3) Zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych oraz przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji poprzez stałe nadzorowanie jego poziomu, zmniejszanie prawdopodobieństwa jego zaistnienia oraz minimalizowania skali jego oddziaływania w przypadku gdy zaistniało;
4) Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (*wzór ewidencji stanowi **załącznik nr 8** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*), która zawiera:

a) nazwę zbioru,
b) imię i nazwisko osoby upoważnionej,
c) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
d) numer upoważnienia,
e) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.

5) Ewidencjonuje oświadczenia osób upoważnionych i zaznajomionych z zasadami zachowania bezpieczeństwa danych (*wzór ewidencji określa* ***załącznik nr 10*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*);
6) Określa potrzeby w zakresie stosowanych zabezpieczeń. Wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia;
7) Bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.
8) Współpracuje z ASI w zakresie zapewnienia bezpieczeństwa i ochrony przetwarzania danych osobowych w systemach informatycznych;
9) Wnioskuje do Administratora Danych Osobowych celem wyznaczania osobom upoważnionym wykonywanie określonych zadań;
10) Zapewnia zapoznanie pracowników upoważnionych do przetwarzania informacji z przepisami o ochronie danych osobowych m.in. poprzez prowadzenie szkoleń w celu uaktualnienia i utrwalenia informacji. ze szczególnym uwzględnieniem takich zagadnień jak:
    a) zagrożenia bezpieczeństwa informacji,
    b) skutki naruszenia zasad bezpieczeństwa informacji,
    c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,

    Szkolenia powinny być przeprowadzane co najmniej raz w roku oraz przy każdej zmianie w przepisach prawa mających wpływ na bezpieczeństwo.

6. Administrator Danych Osobowych powołuje Administratora Systemów Informatycznych *(wzór powołania Administratora Bezpieczeństwa Informacji określa* ***załącznik nr 2*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).*

7. **Administrator Systemów Informatycznych (ASI):**
    1) Nadaje uprawnienia do przetwarzania danych osobowych w systemach informatycznych,
    2) Prowadzi i aktualizuje rejestr nadanych uprawnień do przetwarzania danych w systemach informatycznych,
    3) Nadzoruje stosowanie środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, w szczególności przeciwdziałających dostępowi

osób niepowołanych do tych systemów,

4) Podejmuje działania w przypadku wykrycia naruszeń w systemie zabezpieczeń,
5) Identyfikuje i analizuje zagrożenia oraz ocenia ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
6) Sprawuje nadzór nad przechowywanymi kopiami zapasowymi,
7) Inicjuje i nadzoruje wdrażanie nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych,
8) Współpracuje z ABI w zakresie zapewnienia bezpieczeństwa i ochrony przetwarzania danych osobowych w systemach informatycznych;

8. **Pracownik przetwarzający dane**:

1) Zapoznaje się z zasadami określonymi w Polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym oraz składa oświadczenie o znajomości zawartych w nich przepisów;
2) Chroni prawo do prywatności osób powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i ochrony przetwarzania danych osobowych;
3) Przestrzega przepisów o ochronie danych osobowych, a także ściśle współpracuje z Administratorem Danych Osobowych, Administratorem Bezpieczeństwa Informacji oraz Administratorem Systemów Informatycznych;
4) Ma ukończone szkolenie w zakresie ochrony danych osobowych (*lista uczestników szkolenia z zakresu ochrony danych osobowych znajduje się w* ***załączniku nr 11*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*);
5) Informuje Administratora Bezpieczeństwa Informacji o wszystkich zauważonych nieprawidłowościach;
6) Zgłasza Administratorowi Bezpieczeństwa Informacji zamiar utworzenia nowego bądź modyfikacji istniejącego zbioru danych osobowych podając przy tym informacje na temat struktury i rodzaju danych tego zbioru.
7) Występuje z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

9. Pracownik nie przetwarzający danych, ale mający dostęp do pomieszczeń w których są przetwarzane dane osobowe (tj. pracownicy porządkowi, konserwatorzy):

1) zobowiązuje się do zachowania w tajemnicy wszelkich informacji poprzez podpisanie klauzuli poufności, *której wzór określony jest w* ***załączniku nr 3*** *dokumentacji Polityki*

Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

2) W przypadku znalezienia dokumentacji zawierającej dane osobowe, panie sprzątające lub każdy pracownik przekazuje dokumenty do AD lub do ABI

ROZDZIAŁ III
Identyfikacja zagrożeń bezpieczeństwa przetwarzania danych osobowych

§ 6

Na podstawie przeprowadzonej identyfikacji zagrożeń przy przetwarzaniu danych osobowych wykazano następujące zagrożenia:

1) włamania od strony okien – wybite szyby, niedomknięte skrzydła;
2) włamania od strony drzwi – uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach;
3) oddziaływanie czynników zewnętrznych – pożar, zalanie pomieszczeń, katastrofa budowlana;
4) pozostawienie niezamkniętych drzwi – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych;
5) pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach;
6) pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy;
7) pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze;
8) pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe;
9) przechowywanie dokumentów w miejscach do tego nieprzeznaczonych;
10) wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie;
11) przetwarzanie danych przez osoby nieuprawione;
12) nieuzasadnione sporządzanie kserokopii danych;
13) dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych;
14) dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią;

15) sporządzanie kopii danych w sytuacjach niewynikających z zakresu obowiązków służbowych;

16) utrata kontroli nad kopią danych osobowych;

17) podmiana lub zniszczenie nośników z danymi osobowymi;

18) pozostawienie zapisanego hasła dostępu do bazy danych;

19) samodzielne instalowanie oprogramowania, którego instalacja nie jest wymagana w celu umożliwienia wykonywania obowiązków służbowych;

20) obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania;

21) opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych;

22) odczytywanie nośników przed sprawdzeniem ich programem antywirusowym;

23) dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych;

24) ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym;

25) ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej;

26) dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe;

27) awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich;

28) nieoczekiwane, niedające się wyjaśnić zmiany zawartości bazy danych;

29) niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych;

30) próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej;

31) dopuszczanie aby osoby inne niż ADO, ABI lub osoby przez nich uprawnione podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji;

32) manipulacja przy układach sieci komputerowej lub komputerach;

33) obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.

ROZDZIAŁ IV
Ocena ryzyka

§ 7

1. W celu zminimalizowania ryzyka, czyli możliwości wykorzystania podatności przez zagrożenie w celu spowodowania utraty zachowania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności danych osobowych, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na jednostkę dokonano oceny poziomu ryzyka.

2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

3. Sposób oceny prawdopodobieństwa wystąpienia zdarzenia:

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysokie	5	Przewiduje się, że zdarzenie objęte ryzykiem będzie powtarzalne w ciągu roku.
Wysokie	4	Przewiduje się, że zdarzenie objęte ryzykiem wystąpi kilkakrotnie w ciągu roku.
Średnie	3	Przewiduje się, że zdarzenie objęte ryzykiem będzie występowało okazjonalnie, bądź w wyniku równoczesnego występowania różnych problemów i okoliczności.
Niskie	2	Przewiduje się, że zdarzenie objęte ryzykiem wystąpi raz w ciągu roku.
Bardzo niskie	1	Przewiduje się, że zdarzenie objęte ryzykiem nie wystąpi w ciągu roku.

4. Ocena skutków dokonywana jest w skali od 1 do 5, oceniając niżej wymienione kryteria:

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo Duży	5	Bardzo duży i trwały wpływ na finanse. Utrata wizerunku i zaufania do jednostki organizacyjnej. Zdarzenie uniemożliwia realizację zadania, zagraża realizacji celu
Duży	4	Duży wpływ na finanse, którego zminimalizowanie wymaga

		zaangażowania znaczącego zasobu czasu lub środków. Sytuacje i zjawiska prowadzące do zmniejszenia zaufania w niektórych obszarach. Zdarzenie wpływa na przekroczenie mierników realizacji zadania.
Średni	3	Średni skutek finansowy. Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielki negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego.
Mały	2	Niewielki wpływ na finanse, wymagający podjęcia działań, w wyniku których zakłócenie w realizacji zadania zostanie zneutralizowane. Sporadyczne, krótkotrwałe sygnały dotyczące pojedynczych zdarzeń, niewpływające na wizerunek całej jednostki organizacyjnej. Zdarzenie utrudnia realizację zadania.
Bardzo mały	1	Znikomy wpływ na finanse, niewymagający podejmowania reakcji związanej z realizacją zadania. Brak negatywnych reakcji zewnętrznych na działania jednostki organizacyjnej. Zdarzenie nie wpływa na realizację zadania.

5. Poziom ryzyka to iloczyn prawdopodobieństwa wystąpienia zdarzeń określonych w § 6 oraz skali oddziaływania (skutków) w przypadku ich wystąpienia.

Prawdopodo-bieństwo	5 Bardzo wysokie	5	10	15	20	25
	4 Wysokie	4	8	12	16	20
	3 Średnie	3	6	9	12	15
	2 Niskie	2	4	6	8	10
	1 Bardzo niskie	1	2	3	4	5
		1 Bardzo mały	2 Mały	3 Średni	4 Duży	5 Bardzo duży
		Skutek				

Poziom ryzyka określa zależność:

R=P*O

gdzie:

R – poziom ryzyka,
P – prawdopodobieństwo wystąpienia zdarzenia,
O – skala oddziaływania w przypadku wystąpienia zdarzenia,

6. Poziom Istotności Ryzyka:

1) Z punktu widzenia jednostki najbardziej istotne są obszary, w których poziom ryzyka wynosi więcej niż 15. Jest to ryzyko nieakceptowalne, które musi zostać zmniejszone i stale monitorowane. W przypadku wystąpienia takiego poziomy przetwarzanie danych zostaje wstrzymane do momentu jego zmniejszenia.
2) Poziom ryzyka w skali od 4 do 14 oznaczono obszar średniego zagrożenia.
3) Poziom ryzyka od 1 do 3 to obszar ryzyka, w którym zmaterializowanie się zdarzeń jest mało prawdopodobne, lub ich wpływ na jednostkę jest niewielki.

§ 8

Zagrożenie:	Prawdopodobieństwo:	Oddziaływanie:	Poziom ryzyka:
włamania od strony okien	1	3	3
włamania od strony drzwi	1	3	3
oddziaływanie czynników zewnętrznych	1	3	3
pozostawienie niezamkniętych drzwi	1	3	3
pozostawienie bez nadzoru osób nieuprawnionych do przebywania	1	2	2

w pomieszczeniach			
pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy	1	2	2
pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze	1	2	2
pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe	1	2	2
przechowywanie dokumentów w miejscach do tego nieprzeznaczonych	1	1	1
wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	1	2	2
przetwarzanie danych przez osoby nieuprawione	1	2	2
nieuzasadnione sporządzanie kserokopii danych	1	2	2
dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych	1	2	2
dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią	1	1	1

sporządzanie kopii danych w sytuacjach niewynikających z zakresu obowiązków służbowych	1	2	2
utrata kontroli nad kopią danych osobowych	1	2	2
podmiana lub zniszczenie nośników z danymi osobowymi	1	2	2
pozostawienie zapisanego hasła dostępu do bazy danych	1	3	3
samodzielne instalowanie oprogramowania, którego instalacja nie jest wymagana w celu umożliwienia wykonywania obowiązków służbowych	1	2	2
obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	1	2	2
opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych	1	2	2
odczytywanie nośników przed sprawdzeniem ich programem antywirusowym	1	2	2
dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych	1	3	3
ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń	1	2	2

osobom niepowołanym			
ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	1	2	2
dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	2	1	2
awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich	1	2	2
nieoczekiwane, niedające się wyjaśnić zmiany danych	1	2	2
niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych	1	2	2
próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej	1	2	2
dopuszczanie aby osoby inne niż ADO, ABI lub osoby przez nich uprawnione podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji	1	3	3
manipulacja przy układach sieci komputerowej lub komputerach	1	3	3
obecność nowych urządzeń i kabli o nieznanym przeznaczeniu	1	3	3

i pochodzeniu			

Jak przedstawia powyższa analiza, poziom ryzyka w jednostce jest niski (maksymalny poziom ryzyka wynikający z macierzy wynosi 3. Oznacza to więc, iż zastosowane środki techniczne oraz organizacyjne mające na celu zapewnienie bezpieczeństwa i ochronę danych osobowych są wystarczające.

Pomimo takiej oceny, nie należy zaprzestać analizowania jego poziomu. Trzeba aktualizować jego ocenę każdorazowo w przypadku jakiejkolwiek zmiany w sposobie przetwarzania danych osobowych lub zmianach spowodowanych wprowadzeniem nowych środków organizacyjnych lub technicznych określonych w niniejszej dokumentacji *(określonych w **załączniku nr 6** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).*

Obowiązkiem Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych jest również stałe podnoszenie wiedzy oraz umiejętności w celu wyeliminowania ryzyka szczątkowego, poprzez stałe prace nad zmniejszeniem prawdopodobieństwa zdarzenia oraz minimalizowania skali oddziaływania w przypadku ich wystąpienia.

ROZDZIAŁ V
Przetwarzanie danych osobowych

§ 9

1. Przetwarzanie danych osobowych ma miejsce wyłącznie gdy:

   1) jest to niezbędne do realizacji uprawnień, lub spełnienia obowiązków wynikających z przepisów prawa;
   2) jest to niezbędne do zrealizowania umowy, gdy osoba, której dane dotyczą jest jej stroną lub jest to konieczne do podjęcia działań przed zawarciem umowy;
   3) jest konieczne do wykonania określonych prawnie zadań realizowanych dla dobra publicznego;
   4) jest to konieczne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez jednostkę, a przetwarzanie nie narusza praw i wolności osób, której dane dotyczą;
   5) osoba, której dane dotyczą, wyrazi pisemną zgodę na przetwarzanie danych osobowych. Zgoda nie może być domniemana lub dorozumiana. Zgoda musi być dobrowolna i zawarta z zachowaniem równowagi pomiędzy dającym zgodę, a Administratorem Danych Osobowych.

2. W przypadku legalności przetwarzania danych wynikających z ust. 1, pkt 1 - 4 jednostka nie musi występować o zgodę na przetwarzanie danych osobowych.

3. Zabrania się przetwarzania danych wrażliwych, chyba że jest to dopuszczalne w oparciu o pisemną zgodę osoby, której dane dotyczą, bądź gdy przepis szczególny ustawy innej niż Ustawa o Ochronie Danych Osobowych i zachowana jest pełna gwarancja ochrony tych danych.

§ 10

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą Administrator Danych Osobowych informuje tę osobę o:

   1) pełnej nazwie i adresie siedziby Administratora Danych Osobowych;
   2) celu zbierania danych, w szczególności o znanych mu, w czasie udzielania informacji, odbiorcach lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
   3) prawie dostępu do treści swoich danych oraz ich poprawiania;
   4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Obowiązek informacyjny wypełniany jest w chwili zbierania danych.

3. Administrator Danych Osobowych posiada pisemne potwierdzenia spełnienia obowiązku informacyjnego. (*wzór informacji w przypadku zbierania danych osobowych od osoby, której one dotyczą określony jest w* ***załączniku nr 22*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*)

4. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą Administrator Danych Osobowych informuje tę osobę o:

   1) pełnej nazwie i adresie siedziby Administratora Danych Osobowych;
   2) celu zbierania danych, w szczególności o znanych mu, w czasie udzielania informacji, odbiorcach lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
   3) źródle danych;
   4) prawie dostępu do treści swoich danych oraz ich poprawiania;
   5) przysługującym prawie do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych Administratora, zgodnie z art. 32.1 Ustawy.

5. Administrator Danych Osobowych posiada potwierdzenia spełnienia obowiązku informacyjnego w postaci wiadomości elektronicznej lub potwierdzenia nadania listu (*wzór informacji w przypadku zbierania danych osobowych nie od osoby, której one dotyczą określony jest w* ***załączniku nr 23*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*) . (proszę o zweryfikowanie rzeczywistego faktu spełniania obowiązku informacyjnego).

6. Obowiązku informacyjnego nie wypełnia się jeśli:

   1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
   2) osoba, której dane dotyczą, posiada informacje, o których mowa w §10 ust. 1.

§ 11

1. Na wniosek osoby, której dane dotyczą, Administrator Danych zobowiązany jest w ciągu 30 dni poinformować tę osobę na piśmie o prawach jej przysługujących oraz udzielić odnośnie jej danych osobowych informacji:

   1) o tym jakie dane osobowe zawiera zbiór;
   2) kto jest administratorem danych;
   3) jaki jest cel, zakres i sposób przetwarzania danych zawartych w zbiorze;
   4) terminie od kiedy przetwarza się w zbiorze dane jej dotyczące;
   5) źródle, z którego pochodzą dane jej dotyczące, chyba, że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
   6) o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane;
   7) przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2 Ustawy.

2. Informacje, o których mowa w ust. 1 pkt 1-6 może otrzymać osoba zainteresowana nie częściej niż raz na 6 miesięcy.

3. Administrator Danych odmawia osobie, której dane dotyczą udzielenia ww. informacji, jeżeli spowodowałoby to:

   1) ujawnienie wiadomości zawierających informacje niejawne;
   2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
   3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
   4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

4. Wzór informacji o zawartości zbioru danych osobowych określa ***załącznik nr 16*** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

Rozdział VI

Udostępnianie oraz powierzanie przetwarzania danych osobowych

§ 12

1. Udostępnianie danych osobowych:

   1) dane osobowe mogą być udostępniane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
   2) *wzór wniosku o udostępnienie danych ze zbioru danych osobowych określa* ***załącznik nr 18*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych;*
   3) Administrator Danych Osobowych zachowuje szczególną staranność i nadzór w zakresie udostępniania danych osobowych;
   4) udostępnienie danych nie może naruszać praw i wolności osób, których one dotyczą;
   5) Administrator Danych Osobowych może odmówić udostępnienia danych osobowych jeżeli może to naruszyć bezpieczeństwo i ochronę danych;
   6) w celu nadzoru nad udostępnianiem danych osobowych prowadzona jest ewidencja udostępniania danych osobowych, *której wzór określony jest w* ***załączniku nr 19*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.*

2. Jeżeli w udostępnianych dokumentach zawarte są dane osobowe niemające bezpośredniego związku z celem udostępniania, dokonuje się ich anonimizacji.

3. Administrator Bezpieczeństwa Informacji jest zobowiązany do uzupełnienia uaktualnienia, sprostowania lub usunięcia danych osobowych które są niekompletne, nieaktualne, nieprawdziwe, zebrane z naruszeniem Ustawy o Ochronie Danych Osobowych lub zbędne co do realizacji celu dla którego zostały zebrane.

§ 13

Powierzanie przetwarzania danych osobowych:

1) Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze pisemnej umowy;
2) do umów zawieranych z podmiotami zewnętrznymi zostają włączone klauzule dotyczące:
   a) obowiązku ochrony tych informacji przez strony umowy zarówno w trakcie trwania umowy jak i po jej ustaniu,
   b) ograniczenia dostępu do informacji wyłącznie do osób związanych z realizacją umowy,
   c) zakazu ujawniania danych,
   d) odpowiedzialności w przypadku naruszenia bezpieczeństwa danych zarówno przez podmiot jak i zatrudnionych pracowników.
3) Umowy powierzenia przetwarzania danych zawierają:
   a) określenie celu i zakresu powierzenia przetwarzania danych osobowych,
   b) zasady przetwarzania i ochrony danych zgodnie z Ustawą,
   c) spełnienie wymogów wynikających z Ustawy,
   d) prawo kontroli spełnienia wymogów podmiotu, któremu powierzono dane,
   e) odpowiedzialność podmiotu i jego pracowników z tytułu powierzenia przetwarzania danych osobowych,
   f) obowiązek poinformowania o wszelkich naruszeniach w zakresie przetwarzania danych osobowych oraz kontrolach uprawnionych instytucji zewnętrznych,
   g) skutki naruszenia zasad przetwarzania danych osobowych,
   h) obowiązki podjęcia działań mających na celu zapobiegnięcie naruszenia ochrony danych osobowych oraz wdrożenie środków zapobiegawczych mających na celu brak możliwości wystąpienia naruszeń w przyszłości,
   i) informację o zwrocie danych osobowych w momencie zakończenia obowiązywania umowy,

j) prawo do natychmiastowego rozwiązania umowy w przypadku braku przestrzegania jej postanowień

4) Podmiot, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie, ponosi również odpowiedzialność za zachowanie wszelkich wymogów wynikających z przepisów prawa w zakresie ochrony danych osobowych, w szczególności zastosowanie wymogów technicznych i organizacyjnych do zabezpieczenia przedmiotowych danych.

§ 14

1. Przetwarzanie danych osobowych w formie tradycyjnej oraz w systemach informatycznych odbywa się na obszarze wyznaczonym przez Administratora Danych Osobowych (*wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa* ***załącznik nr 4*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

2. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych Osobowych.

3. Administrator Bezpieczeństwa Informacji razem z Administratorem Systemów Informatycznych opracowuje i wdraża zasady postępowania w przypadku przetwarzania danych osobowych poza obszarem wyznaczonym przez Administratora Danych Osobowych z uwzględnieniem środków ochrony nośników danych przed zniszczeniem oraz przed dostępem do informacji osób trzecich. (*Zasady postępowania w przypadku przetwarzania danych osobowych poza obszarem wyznaczonym przez Administratora Danych Osobowych określa* ***załącznik nr 24*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

4. Przy przetwarzaniu mobilnym Administrator Systemów Informatycznych zapewnia przestrzeganie zasad określonych w procedurze, o której mowa w ust. 3.

§ 15

1. W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych ustalono następujące zasady:

   1) Osoby pracujące w danym pomieszczeniu posiadają klucz, który nie jest zdawany po zakończonej pracy
   2) pracownicy Administratora Danych Osobowych są zobowiązani do przestrzegania zasad

określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe, tzn.:

a) stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko osoby upoważnione,
b) przebywanie osób upoważnionych po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych Osobowych bądź Administratora Bezpieczeństwa Informacji,
c) wszyscy pracownicy zobowiązani są do zwracania uwagi na zachowanie osób wchodzących i wychodzących z jednostki,
d) przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności osób upoważnionych lub za pisemną zgodą Administratora Danych Osobowych.

2. Dostęp osób trzecich do pomieszczeń, w których przetwarzane są dane osobowe jest możliwy podczas wykonywanych prac remontowych lub budowlanych wyłącznie pod nadzorem upoważnionego pracownika. Jeżeli jednak przebywanie w pomieszczeniu stwarza zagrożenie zdrowia lub życia pracownika, osoby trzecie mogą samodzielnie przebywać w tych pomieszczeniach. W tym przypadku akta, dokumenty oraz urządzenia i nośniki komputerowe zawierające dane osobowe powinny zostać przeniesione do innego pomieszczenia, bądź zabezpieczone w sposób zapewniający brak dostępu do nich osób trzecich.

§ 16

1. W celu ochrony przed dostępem osób nieuprawnionych do informacji znajdujących się na nośnikach, stacje robocze zabezpiecza się hasłem, które znane jest jedynie pracownikom zaangażowanym w proces przetwarzania informacji. Dodatkowo na monitorach zainstalowane są wygaszacze ekranu z których wybudzenie wymaga wprowadzenia hasła użytkownika.

2. W celu zabezpieczenia danych przed utratą wprowadza się w Instrukcji Zarządzania Systemem Informatycznym zapisy regulujące sposoby zarządzania kopiami zapasowymi.

§ 17

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa ***załącznik nr 4*** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

§ 18

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych oraz sposób przepływu danych określa ***załącznik nr 5*** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

Rozdział VII
Sprawdzanie zgodności przetwarzania danych osobowych

§ 19

1. Administrator Bezpieczeństwa Informacji zapewnia przestrzeganie zasad ochrony danych osobowych.

2. Administrator Bezpieczeństwa Informacji dokonuje okresowych sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.

3. Sprawdzenie przeprowadzane jest w trybie:

   1) sprawdzenia planowego - według planu sprawdzeń określającego przedmiot, zakres oraz termin przeprowadzania poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania (*wzór planu sprawdzeń określa **załącznik nr 12** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*);
   2) sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez Administratora Bezpieczeństwa Informacji wiadomości o naruszeniu ochrony danych osobowych (*wzór zgłoszenia podejrzenia naruszenia ochrony danych osobowych określa **załącznik nr 17** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*) lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
   3) w związku z art. 19 b ust. 1 ustawy - w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.

4. Ze sprawdzeń, o których mowa w ust. 3, sporządza się sprawozdanie (w postaci papierowej bądź elektronicznej), które przechowuje Administrator Danych Osobowych (*wzór sprawozdania określa **załącznik nr 13** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*). Sprawozdania

te przekazuje Administratorowi Danych w terminie:

1) ze sprawdzenia planowego - nie później niż 30 dni od zakończenia sprawdzenia;
2) ze sprawdzenia doraźnego - niezwłocznie po zakończeniu sprawdzenia;
3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor - zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19 b ust. 1 ustawy.

5. Sprawdzenia, o których mowa w ust. 3 są ewidencjonowane (*rejestr sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz zasad postępowania w przypadku naruszenia ochrony danych osobowych określa* ***załącznik nr 15*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

6. Administrator Bezpieczeństwa Informacji w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

1) z zasadami, o których mowa w art. 23- 37 i art. 31- 35 Ustawy;
2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37- 39 Ustawy, w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3) z zasadami przekazywania danych osobowych, o których mowa w art. 47- 48 ustawy;
4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

7. Plan sprawdzeń przygotowywany jest przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan ten przedstawiany jest Administratorowi Danych nie później niż 2 tygodnie przed dniem rozpoczęcia okresu objętego planem i zawiera co najmniej jedno sprawdzenie.

8. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem raz na pięć lat.

9. Sprawdzenie doraźne przeprowadza się niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

10. Administrator Bezpieczeństwa Informacji zawiadamia Administratora Danych o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia, o dokonanie którego zwrócił się Generalny Inspektor, przed podjęciem pierwszej czynności w toku sprawdzenia.

11. Administrator Bezpieczeństwa Informacji dokumentuje czynności zgodnie z § 4 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

12. W celu zapewnienia prawidłowości przeprowadzania sprawdzeń, zgodność przetwarzania danych osobowych przetwarzanych w systemach informatycznych wraz z Administratorem Bezpieczeństwa Informacji sprawdza Administrator Systemów Informatycznych.

Rozdział VIII

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 20

1. Przed przystąpieniem do pracy osoba upoważniona zobowiązana jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik systemu zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.

3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych Osobowych.

4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w formie tradycyjnej.

5. W przypadku podejrzenia naruszenia ochrony danych osobowych przetwarzanych za pośrednictwem systemów informatycznych Administrator Bezpieczeństwa Informacji informuje Administratora Systemów Informatycznych.

§ 21

1. Do czasu przybycia Administratora Bezpieczeństwa Informacji zgłaszający:

   1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów bądź innych dowodów;
   2) zabezpiecza elementy systemu informatycznego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
   3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 22

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji po przybyciu na miejsce:

   1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu;
   2) wysłuchuje relacji osoby, która dokonała powiadomienia;
   3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

2. W uzasadnionych przypadkach w razie stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji niezwłocznie powiadamia o tym fakcie Administratora Danych Osobowych.

§ 23

Administrator Bezpieczeństwa Informacji sporządza z przebiegu zdarzenia sprawozdanie (*wzór sprawozdania określa* ***załącznik nr 13*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*), w którym powinny się znaleźć w szczególności informacje o:

1) dacie i godzinie powiadomienia;
2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;
3) sytuacji, jaką zastał;
4) podjętych działaniach i ich uzasadnieniu.

§ 24

1. Administrator Bezpieczeństwa Informacji podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

   1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;
   2) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych Osobowych dyscypliny pracy, Administrator Bezpieczeństwa Informacji wnioskuje do Administratora Danych Osobowych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec osób, które dopuściły się tego uchybienia.

§ 25

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji.

§ 26

1. W przypadku zaginięcia komputera lub nośników, na których były zgromadzone dane osobowe, użytkownik systemu niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

2. W sytuacji, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.

3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym lub elektronicznym Administrator Danych Osobowych podejmuje działania zmierzające do odzyskania utraconych danych oraz monitoruje proces przebiegu wyjaśnienia sprawy.

§ 27

Osoba zatrudniona przy przetwarzaniu danych osobowych odpowiedzialna za naruszenie obowiązków wynikających z niniejszej Polityki bezpieczeństwa oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie pracy, Kodeksie pracy oraz wynikających z ustawy o ochronie danych osobowych.

ROZDZIAŁ IX

Postępowanie w wypadku klęski żywiołowej

§ 28

Klęską żywiołową jest katastrofa spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 29

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 30

1. Każda osoba, która będzie świadkiem zbliżania się lub działania zagrożeń określonych w §28 zobowiązana jest powiadomić Administratora Bezpieczeństwa Informacji w każdy możliwy sposób. W razie niemożności skontaktowania się z nim zawiadamia Administratora Danych Osobowych.

2. Numery telefonów Administratora Bezpieczeństwa Informacji, Administratora Systemów Informatycznych oraz Administratora Danych Osobowych są znane pracownikom.

§ 31

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w §15.

§ 32

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1) zamknięcia systemu informatycznego;
2) zabezpieczenia danych osobowych przetwarzanych tradycyjnie.

§ 33

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych, Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe.

2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych Osobowych obecnych przy akcji ratunkowej.

ROZDZIAŁ X
Niszczenie danych osobowych

§ 34

1. Usuwanie danych osobowych, polega na:

    1) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod;
    2) anonimizacji zbiorów danych osobowych polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

2. Procedura niszczenia danych osobowych:

    1) niszczenie danych osobowych następuje wyłącznie na wniosek Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji;
    2) sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii;
    3) niszczenie danych osobowych musi odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji;
    4) zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu (*wzór protokołu określa **załącznik nr 20** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

3. Usuwanie danych osobowych jest zależne od rodzaju nośnika, na którym są przechowywane.

    1) Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) niezawierająca danych wrażliwych – przy użyciu niszczarki kategorii P-3 lub wyższej (zgodnie z normą **DIN 66399**);
    2) Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) zawierająca dane wrażliwe – przy użyciu niszczarki kategorii P-4 (zgodnie z normą **DIN 66399**);
    3) Nośniki optyczne (płyty CD/DVD/BLU-RAY – analogicznie do dokumentacji tradycyjnej, za pomocą niszczarek, przy czym do danych niewrażliwych kategorii O-3 lub wyższej, a do danych wrażliwych kategorii O-4 (zgodnie z normą **DIN 66399**);
    4) Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – korzystając z jednej z dwóch metod:
        a) niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
        b) niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń,

5) Nośniki magnetyczne (dyskietki/dyski twarde HDD) – korzystając z jednej z trzech metod:
   a) niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
   b) niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń, oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych,
   c) demagnetyzacji nośników.

ROZDZIAŁ XI
Postanowienia końcowe

§ 35

Polityka Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 36

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych oraz do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień w nich zawartych.

2. Osoba upoważniona zobowiązana jest złożyć oświadczenie o tym, że została zaznajomiona z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką Bezpieczeństwa służącymi do przetwarzania danych osobowych (*wzór oświadczenia stanowi* ***załącznik nr 9*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

3. Oświadczenia przechowywane są w aktach osobowych pracownika.

4. Wszyscy pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych procedur i zasad zawartych w niniejszej dokumentacji.

....., dn. ..... r.

.....
(Pieczęć)

POWOŁANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*) z dniem ..... - ..... - ..... powołuje się:

Pana / Panią

.....

na ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

Równocześnie nadaje się Administratorowi Bezpieczeństwa Informacji upoważnienie do przetwarzania danych osobowych w zakresie niezbędnym do realizacji obowiązków wynikających z zawartej umowy, do których należą:

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych.
2. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
3. Nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 Ustawy, oraz przestrzegania zasad w niej określonych,
4. Zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
5. Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
6. Zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych, poprzez stałe nadzorowanie jego poziomu, zmniejszanie prawdopodobieństwa jego zaistnienia oraz minimalizowania skali jego oddziaływania w przypadku gdy zaistniało.
7. Ewidencjonowanie oświadczenia osób upoważnionych i zaznajomionych z zasadami zachowania

bezpieczeństwa danych.

8. Określanie potrzeb w zakresie stosowanych zabezpieczeń oraz wnioskowanie do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia.
9. Uczestniczenie w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe i zapewnianie odpowiedniego poziomu przeszkolenia w tym zakresie.
10. Upoważnianie do przetwarzanie danych osobowych oraz określanie zakresu upoważnień,
11. Ewidencjonowanie upoważnień,

.....	.....
data i podpis	data i podpis
Administratora Danych Osobowych	Administratora Bezpieczeństwa Informacji

Załącznik nr 2
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

....., dn. .....r.

.....
(Pieczęć)

POWOŁANIE ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Z dniem ..... - ..... - ..... powołuje się:

Pana / Panią

.....

na ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH.

Równocześnie nadaje się Administratorowi Systemów Informatycznych upoważnienie do przetwarzania danych osobowych w zakresie niezbędnym do realizacji obowiązków wynikających z zawartej umowy, do których należą:

2. Nadawanie uprawnień do przetwarzania danych osobowych w systemach informatycznych,
3. Prowadzenie i aktualizacja rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
4. Pełnienie nadzoru nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
5. Podejmowanie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń,
6. Identyfikacja i analiza zagrożenia oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
7. Sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi,
8. Inicjacja i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych,
9. Współprac z ABI w zakresie zapewnienia bezpieczeństwa i ochrony przetwarzania danych osobowych w systemach informatycznych;

.....
data i podpis
Administratora Danych Osobowych

.....
data i podpis
Administratora Systemów Informatycznych

Klauzula poufności danych

.....

(Dane pracownika)

dnia ....., zobowiązuje się do zachowania w tajemnicy wszelkich informacji dotyczących Gminy Szreńsk.

przez okres trwania stosunku pracy oraz po jego ustaniu w związku z wykonywaniem obowiązków służbowych.

Zachowanie w tajemnicy oznacza jednak możliwość ujawnienia takich informacji Wójtowi Gminy Szreńsk.

Powyższe zobowiązanie nie narusza ujawnienia informacji:

1) dostępnych publicznie;
2) uzyskanych niezależnie z innych źródeł;
3) których ujawnienie może być wymagane na podstawie przepisów prawa.

....

data i miejsce podpis

Załącznik nr 4
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

WYKAZ ZBIORÓW DANYCH PRZETWARZANYCH TRADYCYJNIE I W SYSTEMIE INFORMATYCZNYM ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH I MIEJSCEM PRZETWARZANIA

l.p.	Nazwa zbioru danych	Lokalizacja zbioru danych osobowych (budynek, pomieszczenie)	Nazwa programu zastosowanego do przetwarzania danych oraz autor programu
1.	Rejestr najemców lokali mieszkalnych i użytkowych	Pokój nr 17 -Stanowisko ds. geodezji gospodarki nieruchomościami i drogownictwa.	
2.	Dzierżawa gruntów i opłat za użytkowanie wieczyste	Pokój nr 17 -Stanowisko ds. geodezji gospodarki nieruchomościami i drogownictwa.	
3.	Rejestr wydanych decyzji na usunięcie drzew i krzewów	Pokój nr 17 -Stanowisko ds. geodezji gospodarki nieruchomościami i drogownictwa.	
4.	Ewidencja podziałów nieruchomości	Pokój nr 17 -Stanowisko ds. geodezji gospodarki nieruchomościami i drogownictwa.	
5.	Numeracja porządkowa, zmiana numeracji porządkowej nieruchomości	Pokój nr 17 -Stanowisko ds. geodezji gospodarki nieruchomościami i drogownictwa.	
6.	Inwentaryzacja wyrobów zawierających azbest	Pokój nr 17- Referat Inwestycji, Planowania przestrzennego i Rolnictwa- infrastruktura, zamówienia publiczne i rolnictwo	Platforma internetowa bazaazbestowa.pl
7.	Utrzymanie czystości i porządku w gminie	Pokój nr 17- Referat Inwestycji, Planowania przestrzennego i Rolnictwa- infrastruktura, zamówienia publiczne i rolnictwo	
8.	Rejestr Decyzji o warunkach zabudowy i zagospodarowania terenu.	Pokój nr 17- Referat Inwestycji, Planowania przestrzennego i Rolnictwa- infrastruktura, zamówienia publiczne i rolnictwo	
9.	Rejestr uzgadniania, opiniowania i zatwierdzania planów zagospodarowania przestrzennego	Pokój nr 17- Referat Inwestycji, Planowania przestrzennego i Rolnictwa- infrastruktura, zamówienia publiczne i rolnictwo	

10.	Ewidencja podatników, płatników i dłużników	Pokój nr 8,9 - Referat Finansowy- podatki i opłaty	PODATKI
11.	Ewidencja podatników, płatników i dłużników	Pokój nr 8,9 - Referat Finansowy- podatki i opłaty	PODATKI
12.	Zwrot podatku akcyzowego	Pokój nr 8,9 - Referat Finansowy- podatki i opłaty	Podatki
13.	Ewidencja ludności Gminy Szreńsk	Pokój nr 7- Urząd Stanu Cywilnego	PESEL- powszechny elektroniczny system ewidencji ludności (źródło)
14.	Rejestr wyborców	Pokój nr 7- Urząd Stanu Cywilnego	„ SEL-WIN"
15.	Ewidencja wydanych i unieważnionych dowodów osobistych	Pokój nr 7- Urząd Stanu Cywilnego	RDO Rejestr dowodów osobistych (źródło)
16.	Urząd Stanu Cywilnego w Szreńsku	Pokój nr 7- Urząd Stanu Cywilnego	BUSC Baza Usług Stanu Cywilnego (źródło)
17.	Wnioski o udostępnianie informacji publicznej	Pokój nr 10 - sekretariat Wójta	
18.	Prowadzenie książek ewidencyjnych osób będących w formacjach obrony cywilnej	Pokój nr 15- stanowisko d. obronnych, obrony cywilnej i zarządzania kryzysowego spraw p.poż raz obsługa Rady Gminy	
19.	Rejestr mężczyzn (kobiet) objętych rejestracją	Pokój nr 15- stanowisko d. obronnych, obrony cywilnej i zarządzania kryzysowego spraw p.poż raz obsługa Rady Gminy	
20.	Lista stawiennictwa osób kwalifikacji wojskowej	Pokój nr 15- stanowisko d. obronnych, obrony cywilnej i zarządzania kryzysowego spraw p.poż raz obsługa Rady Gminy	
21.	Zamówienia publiczne	Pokój nr 16 Referat inwestycji Planowania Przestrzennego i Rolnictwa Kierownik pozyskiwania funduszy pomocowych	Platforma internetowa Urzędu Gminy Szreńsk oraz Biuletyn Informacji Publicznej Urzędu Gminy Szreńsk
22.	Akta osobowe	Pokój nr 18 Stanowisko ds. organizacyjnych i kadr	
23.	Praktyki uczniowskie i studenckie	Pokój nr 18 Stanowisko ds. organizacyjnych i kadr	

24.	Ewidencja skarg i wniosków	Pokój nr 18 Stanowisko ds. organizacyjnych i kadr	
25.	Rejestr umów cywilnoprawnych	Pokój nr 18 Stanowisko ds. organizacyjnych i kadr	
26.	Płace	Pokój nr 12 Referat finansowy- księgowość budżetowa	Kadry i płace
27.	Ubezpieczenia pracowników w ZUS	Pokój nr 12 Referat finansowy- księgowość budżetowa	Płatnik
28.	Księgowość Budżetowa	Pokój nr 12 Referat finansowy- księgowość budżetowa	„ Groszek" FK- budżet
29.	Ewidencja osób odpracowujących kary nałożone przez sądy	Pokój nr 5-stanowisko ds. administracyjno -biurowych	
30.	Zbiór wniosków o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej	Pokój nr 15 stanowisko ds. gospodarczych i działalności	CEIDG
31.	Stypendia i zasiłki szkolne	Pokój nr 21 stanowisko ds. kancelaryjnych i zasiłków szkolnych	
32.	Osoby korzystające z pomocy Gminnej Komisji Rozwiązywania Problemów Alkoholowych	Pokój nr 17	
33.			
34.			
35.			
36.			
37.			
38.			

Załącznik nr 5
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

OPIS STRUKTURY ZBIORU DANYCH OSOBOWYCH PRZETWARZANYCH TRADYCYJNIE I W SYSTEMACH INFORMATYCZNYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

Lp.	Nazwa zbioru danych	Opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze	Opis przepływu danych
1.	Rejestr najemców lokali mieszkalnych i użytkowych	Imiona, nazwisko, adres zamieszkania, seria i numer dowodu osobistego, PESEL, nazwa i numer lokalu, numer ewidencyjny działki	
2.	Dzierżawa gruntów i opłat za użytkowanie wieczyste	Imiona, nazwisko, PESEL, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer ewidencyjny działki, numer Księgi wieczystej, kwota należności, numer telefonu	
3.	Rejestr wydanych decyzji na usunięcie drzew i krzewów	Imiona, nazwisko, adres zamieszkania, numer telefonu, oznaczenie działki nieruchomości w ewidencji gruntów	
4.	Ewidencja podziałów nieruchomości	Imiona, nazwisko, adres zamieszkania lub pobytu, PESEL, NIP, seria i numer dowodu osobistego, numer obrębu, działki, budynku, lokalu, jednostka rejestrowa, karta mapy, numer księgi wieczystej, informacja o użytkach i klasach	
5.	Ewidencja podatników, płatników i dłużników	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, numer konta, położenie gruntów, powierzchnia użytkowna nieruchomości, numer rejestracyjny pojazdu	
6.	Ewidencja ludności Gminy Szreńsk	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, stan cywilny, miejsce i kraj urodzenia, data zameldowania i wymeldowania, stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer książeczki wojskowej, seria, numer, wystawca dokumentu tożsamości, numer, rodzaj, miejsce wydania wizy, płeć, data zawarcia małżeństwa, data zgonu	1
7.	Prowadzenie książek ewidencyjnych	Imiona, nazwisko, data urodzenia, miejsce urodzenia,	

	osób będących w formacjach obrony cywilnej	adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego, numer i seria książeczki wojskowej, kategoria zdrowia	
8.	Rejestr wyborców	Imiona, nazwisko, data urodzenia, adres zameldowania na pobyt stały, adres przebywania, PESEL, seria i numer dowodu osobistego, obywatelstwo, data i numer decyzji o wpisie do rejestru wyborców	
9.	Ewidencja wydanych i unieważnionych dowodów osobistych	Imiona, nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego, wzrost, kolor oczu, płeć, wizerunek, podpis, numer i seria poprzednich dowodów osobistych w tym daty ich wydania oraz ważności i oznaczenie organu, który je wydał	
10.	Rejestr uzgadniania, opiniowania i zatwierdzania planów zagospodarowania przestrzennego	Imiona, nazwisko, adres zamieszkania lub pobytu, numer ewidencyjny działku, numer obrębu, numer telefonu	
11.	Numeracja porządkowa, zmiana numeracji porządkowej nieruchomości	Imiona, nazwisko, miejsce położenia działku	
12.	Ewidencja skarg i wniosków	Imiona, nazwisko, adres zamieszkania lub pobytu	
13.	Urząd Stanu Cywilnego w Szreńsku	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, zawód, wykształcenie, seria i numer dowodu osobistego, miejsce i godzina urodzenia, data i miejsce zgonu, data i miejsce zawarcia małżeństwa, numer i miejsce wydania dowodu osobistego, data unieważnienia aktu małżeństwa, urodzenia, zgonu, ustalenie ojcostwa	
14.	Sporządzanie list poborowych	Imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania lub pobytu, adres do korespondencji, PESEL, seria i numer dowodu osobistego, numer i seria książeczki wojskowej, kategoria zdrowia	
15.	Zwrot podatku akcyzowego	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, powierzchnia gospodarstwa, numer konta bankowego	
16.	Wnioski o udostępnianie informacji publicznej	Imiona, nazwisko, adres zamieszkania lub pobytu, numer telefonu, adres poczty elektronicznej	
17.	Zamówienia publiczne	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, nazwa prowadzonej działalności gospodarczej, informacja z Krajowego Rejestru	

		Karnego, numer telefonu	
18.	Inwentaryzacja wyrobów zawierających azbest	Imiona, nazwisko, adres zamieszkania, miejsce położenia nieruchomości, numer dowodu osobistego, numer telefonu	
19.	Utrzymanie czystości i porządku w gminie	Imiona, nazwisko, adres zamieszkania lub pobytu, PESEL, miejsce położenia nieruchomości	
20.	Akta osobowe	Imiona, nazwisko, PESEL, NIP, stan rodzinny, data urodzenia, stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer specjalności wojskowej, numer książeczki wojskowej, seria i numer dowodu osobistego, miejsce zamieszkania, rodzaj i czas wykonywanej pracy, stanowisko, miejsce wykonywania pracy, wymiar czasu pracy, wynagrodzenie, informacja o wartości i powierzchni domu lub mieszkania, miejsce położenia nieruchomości, udziały w spółkach handlowych, data nabycia mienia, absencje w pracy, numer telefonu, okres zasiłków chorobowych i opiekuńczych, przebieg dotychczasowego zatrudnienia, wykształcenie, wysokość nagrody	
21.	Płace	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i numer dowodu osobistego, numer konta bankowego	
22.	Ubezpieczenia pracowników w ZUS	Imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania lub pobytu, PESEL	
23.	Księgowość budżetowa	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, NIP, miejsce pracy, seria i numer dowodu osobistego, numer konta bankowego	
24.	Stypendia i zasiłki szkolne	Imiona, nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego, numer telefonu, wysokość dochodów rodziny, nazwa i rodzaj szkoły, numer rachunku bankowego	
25.	Zbiór wniosków o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, adres głównego miejsca wykonywania działalności, PESEL, NIP, REGON, nazwa i rodzaj prowadzonej działalności, data rozpoczęcia działalności, data zakończenia działalności, seria i numer dokumentu tożsamości, płeć, obywatelstwo, adres poczty elektronicznej, informacja o małżeńskiej	

		wspólności majątkowej, numer rachunku bankowego	
26.	Rejestr umów cywilnoprawnych	Imiona, nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i numer dowodu osobistego	
27.	Ewidencja osób odpracowujących kary nałożone przez sądy	Imiona, nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, rodzaj wymierzonej kary, wysokość wymierzonej kary	
28.	Osoby korzystające z pomocy Gminnej Komisji Rozwiązywania Problemów Alkoholowych	Imiona, nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, numer telefonu	
29.	Praktyki uczniowskie i studenckie	Imiona, nazwisko, PESEL, rok studiów, kierunek studiów, czas trwania praktyki, nazwa i adres szkoły / uczelni	

Załącznik nr 6
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

WYKAZ ŚRODKÓW TECHNICZNYCH ZASTOSOWANYCH W CELU ZAPEWNIENIA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH:

Nazwa pomieszczenia	Zabezpieczenia pomieszczenia	Zabezpieczenia zbiorów	Zabezpieczenia komputerów
13 – Referat Finansowy - Skarbnik	Drzwi antywłamaniowe		
8, 9 – Referat Finansowy – podatki i opłaty	Zamek na klucz		
12 – Referat Finansowy – księgowość budżetowa	Zamek na klucz		
6 – Referat Finansowy – Kasa	Drzwi antywłamaniowe, kraty na szybach, okna antywłamaniowe , sejf		
16 – Referat Inwestycji, Planowania Przestrzennego i Rolnictwa – Kierownik; Pozyskiwania funduszy pomocowych	Zamek na klucz		
17 – Referat Inwestycji, Planowania Przestrzennego i Rolnictwa – infrastruktura, zamówienia publiczne i rolnictwo	Zamek na klucz		
19 – informatyk	Zamek na klucz		
7 – Urząd Stanu Cywilnego; Stanowisko ds. ewidencji ludności i dowody osobiste	Drzwi antywłamaniowe, okna antywłamaniowe szafa pancerna		
18 – Stanowisko ds. organizacyjnych i kadr	Szafa pancerna, zamek na klucz		
17 – Stanowisko ds. geodezji, gospodarki nieruchomościami i drogownictwa	Zamek na klucz		
15 – Stanowisko ds. obronnych, obrony cywilnej i zarządzania kryzysowego, spraw p.poż oraz obsługa Rady Gminy; Stanowisko ds.	Zamek na klucz		

gospodarczych i działalności gospodarczej			
21 – Stanowisko ds. kancelaryjnych i zasiłków szkolnych	Zamek na klucz		
5 – Stanowisko ds. administracyjno-biurowych	Zamek na klucz, szafa pancerna		
10 – Sekretariat Wójta	Drzwi antywłamaniowe		
1,2,3,4- Gminny Ośrodek Pomocy Społecznej	Zamek na klucz		

Załącznik 7
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk
. . . . . , dnia . . . . . .

. . . . . .
(pieczątka)

Upoważnienie nr . . . . . .

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. 2015, poz. 2135 z pózn. zm.) upoważniam:

Pana / Panią . . . . . .

Adres:	Stanowisko:

do przetwarzania danych osobowych w następującym zakresie:
(nazwy zbiorów oraz zakres upoważnienia) [zbieranie/utrwalanie/przechowywanie/opracowywanie/zmienianie/udostępnianie/usuwanie/wgląd]

Nazwa zbioru:	Identyfikator*:	Zakres upoważnienia

Upoważnienie udzielane jest na czas pełnienia obowiązków pracowniczych od dnia . . . . r.

Upoważniony zobowiązuje się do przestrzegania zasad panujących w zakresie ochrony danych osobowych a w szczególności Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych oraz respektowania zapisów Ustawy o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.)
Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w jednostce oraz sposobów zabezpieczeń.

* uzupełnić w przypadku gdy zbiór przetwarzany jest w systemie informatycznym.

. . . . . .

(data i podpis Administratora Danych Osobowych)

. . . . . .

(data i podpis upoważnionego)

Załącznik nr 8
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko i imię / identyfikator	Numer upoważnienia	Data nadania (*modyfikacji*) upoważnienia	Data utraty ważności upoważnienia	Zbiór danych osobowych oraz zakres upoważnienia do przetwarzania danych osobowych
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

.....
(dane pracownika)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do ich przestrzegania (*Dz. U. 2004 r. Nr 100, poz. 1024*).

Oświadczam ponadto, że zapoznałem(łam) się z Polityką Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych w Gminie Szreńsk wprowadzoną dnia ..... przez Wójta Gminy Szreńsk.

Równocześnie oświadczam, iż znane są mi telefoniczne numery kontaktowe do Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji praz Administratora Systemów Informatycznych.

Zobowiązuję się do:

1) stosowania określonych przez ADO, ABI oraz ASI zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
2) należyte zabezpieczanie danych osobowych przed ich udostępnianiem osobom nieupoważnionym,
3) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
4) zachowania tajemnicy danych oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy.

.....
(data i podpis)

Załącznik nr 10

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

EWIDENCJA OSÓB

zapoznanych z „Polityką Bezpieczeństwa Przetwarzania i Ochrony Danych Osobowych" w Gminie Szreńsk i zapisami zawartymi w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997r. (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*) oraz 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 osobowych.

PRZYJĄŁEM/AM DO WIADOMOŚCI I STOSOWANIA ZAPISY POLITYKI BEZPIECZEŃSTWA I INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Lp.	Nazwisko i imię	Data i podpis

Załącznik nr 11
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

LISTA UCZESTNIKÓW SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Prowadzący: .....

Miejsce i data szkolenia: .....

L.p.	Imię uczestnika:	Nazwisko uczestnika:	Podpis:

Załącznik nr 12

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

PLAN SPRAWDZEŃ W .....

NA OKRES .....

Plan określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń w rozumieniu art. 36c ustawy o ochronie danych osobowych oraz ich zakres.

Lp.	Przedmiot sprawdzenia:	Zakres sprawdzenia:	Termin sprawdzenia:	Sposób dokumentowania:	Zakres dokumentowania:

Dokumentowanie czynności w toku sprawdzenia zawiera w szczególności:

1. Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
2. Odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
3. Sporządzeniu kopii otrzymanego dokumentu, sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
4. Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

.....

(Data i podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 13
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

....., dn. .....r.

Sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1. Oznaczenie administratora danych i adres jego siedziby:

Gmina Szreńsk

Plac Kanoniczny 10

06-550 Szreńsk
(pełna nazwa oraz adres)

2. Imię i nazwisko administratora bezpieczeństwa informacji:

.....

3. Wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

.....

.....

.....

.....

.....

.....

4. Datę rozpoczęcia i zakończenia sprawdzenia:

.....

5. Określenie przedmiotu i zakresu sprawdzenia:

……

6. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……

……

……

……

……

……

……

……

……

……

……

7. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

……

……

……

8. Wyszczególnienie załączników stanowiących składową część sprawozdania:

……

……

.....

Data, miejsce i podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 14
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

....., dn. .....r.

SPRAWOZDANIE

ze sprawdzenia i oceny funkcjonowania mechanizmów zabezpieczeń oraz zasad postępowania w przypadku naruszenia ochrony danych osobowych.

W dniu ....., sprawdzający .....
/imię, nazwisko i stanowisko służbowe/

w obecności osób asystujących: .....
.....

dokonał sprawdzenia w .....
.....

W czasie kontroli stwierdzono i zalecono:
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

/tu należy omówić wyniki sprawdzenia, np.: stanu zabezpieczenia systemów informatycznych oraz innych zbiorów danych jak i przestrzegania obowiązujących przepisów/procedur itp./.

Niniejsze sprawozdanie sporządzono w dwóch jednobrzmiących egzemplarzach i po odczytaniu podpisano.

.....
(podpisy osób asystujących)

.....
(podpis i pieczątka osoby przeprowadzającej sprawdzenie)

Załącznik nr 15
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

REJESTR SPRAWDZEŃ I OCENY FUNKCJONOWANIA MECHANIZMÓW ZABEZPIECZEŃ ORAZ ZASAD POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH W GMINIE SZREŃSK

L.p.	Nazwa sprawdzanego działu	Nazwisko, imię i stanowisko osoby przeprowadzającej sprawdzenie	Czas trwania sprawdzenia	Uwagi	Podpis osoby przeprowadzającej sprawdzenie

....., dn. .....r.

.....
(pieczątka)

.....
(imię i nazwisko)
.....
.....
.....
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia ..... r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Gminie Szreńsk działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe:

.....
.....
.....
.....

Powyższe dane przetwarzane są w .....
.....

w celu .....

z zachowaniem wymaganych zabezpieczeń i zostały uzyskane .....
.....

Powyższe dane nie były/były udostępniane .....

w celu .....

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach kreślonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis Administratora Danych Osobowych)

ZGŁOSZENIE
naruszenia bezpieczeństwa danych osobowych

w .....

1. Data: ..... Godzina: .....
(dd.mm.rr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię i nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia :

.....

4. Opis zaistniałej sytuacji wpływającej na bezpieczeństwo danych osobowych:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....
godz. i data przyjęcia zgłoszenia

.....
Podpis osoby zgłaszającej

podpis Administratora
Bezpieczeństwa Informacji

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do: Gminy Szreńsk, Plac Kanoniczny 10, 06-550 Szreńsk

2. Wnioskodawca .....

.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy ew. NIP oraz REGON)

3. Podstawa prawna upoważniająca do pozyskania danych:

.....

.....

4. Wskazanie przeznaczenia dla udostępnionych danych osobowych:

.....

.....

5. Oznaczenia lub nazwa zbioru, z którego mają być udostępnione dane osobowe:

.....

.....

6. Zakres żądanych informacji ze zbioru:

.....

.....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych:

.....

.....

.....
(data i podpis wnioskodawcy)

Załącznik nr 19
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

EWIDENCJA UDOSTĘPNIENIA DANYCH OSOBOWYCH W GMINIE SZREŃSK

L.p.	Data wydania	Dane odbiorcy	Zakres udostępnionych danych	Podpis osoby udostępniającej dane osobowe

Załącznik nr 20
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

.....
Pieczątka

Protokół zniszczenia danych osobowych

nr: .....

1. Data operacji: .....
2. Nazwa zbioru danych osobowych, z którego pochodzą dane: .....
.....
3. Powód zniszczenia danych osobowych: .....
.....
4. Rodzaj nośnika z kopią zapasową: .....
.....
5. Sposób zniszczenia: .....

Skład komisji:

Imię i nazwisko:	Imię i nazwisko:	Imię i nazwisko:
..... (podpis)	..... (podpis)	..... (podpis)

Załącznik nr 21
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

....., dn. .....r.

PROTOKÓŁ
PRZEKAZANIA/ZDANIA KLUCZY

Data, godzina i miejsce odbioru: .....

1) Obecni :

a) ze strony powierzającego: .....
(imię i nazwisko)

.....
(stanowisko)

b) ze strony odbierającego: .....
(imię i nazwisko)

.....
(stanowisko)

2) Przedmiot odbioru :

.....

.....

.....
(np. jeden komplet kluczy - 4 sztuki z czego 2 sztuki do kraty zabezpieczającej znajdującej się przed magazynem z zewnątrz i 2 sztuki do drzwi wejściowych do magazynu)

Niniejszym zobowiązuję się do nieudostępniania ich osobom trzecim.

Przejęcie kluczy zobowiązuje mnie do odpowiedzialności materialnej podczas pobytu poza godzinami pracy.

Na tym protokół zakończono i po przeczytaniu podpisano

....
Strona powierzająca Strona odbierająca

Załącznik nr 22
do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

Spełnienie obowiązku informacyjnego
(przy zbieraniu danych od osób, których one dotyczą)

W związku z treścią art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2015 r poz. 2135 z późn. zm.) informuję, iż administratorem przekazanych przez Panią/Pana danych osobowych jest:

Gmina Szreńsk, Plac Kanoniczny 10, 06-550 Szreńsk

(wpisać pełną nazwę oraz adres siedziby administratora danych).

Pani/Pana dane osobowe będą przetwarzane w celu .....

Dane osobowe nie będą udostępnianie podmiotom innym niż uprawnione na mocy przepisów prawa.

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania. Zebrane dane osobowe zostały przez Panią/Pana podane dobrowolnie/ w związku z obowiązkiem wynikającym z .....

(podstawa prawna)

Zostałem poinformowany

.....

(data i podpis osoby informowanej)

Załącznik nr 23

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych
w Gminie Szreńsk

Spełnienie obowiązku informacyjnego
(przy zbieraniu danych nie od osób, których one dotyczą)

W związku z treścią art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2015 r poz. 2135 z późn. zm.) informuję, iż administratorem Pani/Pana danych osobowych jest :

Gmina Szreńsk, Plac Kanoniczny 10, 06-550 Szreńsk

(wpisać pełną nazwę oraz adres siedziby administratora danych).

Pani/Pana dane osobowe będą przetwarzane w celu .....

i pochodzą od/ z .....

(źródło danych)

Dane osobowe nie będą udostępnianie podmiotom innym niż uprawnione na mocy przepisów prawa.

Posiada Pani/Pan prawo:

- dostępu do treści swoich danych oraz ich poprawiania;

- wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania swoich danych ze względu na swoją szczególną sytuację;

- wniesienia sprzeciwu wobec przetwarzania swoich danych gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania swoich danych innemu administratorowi.

Zasady postępowania w przypadku przetwarzania danych osobowych poza obszarem wyznaczonym przez Administratora Danych Osobowych

1. Przetwarzanie dokumentów zawierających dane osobowe za pomocą zaszyfrowanych i zabezpieczonych hasłem urządzeń przenośnych, w których zastosowane jest szyfrowanie nośnika, poza obszarem przetwarzania danych jest możliwe tylko po uzyskaniu zgody Administratora Danych Osobowych.
2. Po każdorazowym użyciu ww. urządzenia poza obszarem przetwarzania danych na koniec dnia tworzy się kopię zapasową.
3. Pracownicy, przetwarzający dane poza obszarem wyznaczonym są zobowiązani:
   1) Pilnować i nie dopuścić do sytuacji, w której akta lub dokumenty pozostawione są bez dozoru w czasie ich przenoszenia oraz przetwarzania poza obszarem wyznaczonym przez Administratora Danych Osobowych.
   2) dołożyć wszelkich starań, aby osoby postronne, nie mogły mieć dostępu do dokumentów,
   3) przechowywać dokumenty w sposób zabezpieczający je przed przypadkowym uzyskaniem do nich wglądu przez osoby nieupoważnione;
   4) po zakończeniu wykonywania pracy w terenie niezwłocznie zwrócić dokumenty do Jednostki, a jeśli nie jest to możliwe przechować je w domu. Przechowywanie dokumentów w domu następuje poprzez ich zamknięcie w sposób uniemożliwiający dostęp osób innych niż upoważniony pracownik.
4. Pracownicy, wynoszący dokumenty do domu, są obowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają karze zgodnie z art. 51 ustawy ochrony danych osobowych.