WÓJT GMINY OLSZÓWKA
62-641 OLSZÓWKA
powiat kolski

ZARZĄDZENIE NR 5/2017
WÓJTA GMINY OLSZÓWKA
z dnia 01 marca 2017 r.

w sprawie ustalenia dokumentacji dotyczącej ochrony danych osobowych w postaci Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Olszówce

Na podstawie art. 36a ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późn. zm.) oraz §3 ust. 3, § 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Ustalam „Politykę Bezpieczeństwa Danych Osobowych" stanowiącą załącznik Nr 1 do zarządzenia.

§ 2. Ustalam „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik Nr 2 do zarządzenia.

§ 3. Zobowiązuję pracowników i osób współpracujących z Urzędem Gminy w Olszówce do stosowania zasad określonych w „Polityce Bezpieczeństwa Danych Osobowych" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 4. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 5. Traci moc Zarządzenie Nr 9/2010 z dnia 01 października 20110 r. ze zmianami.

§ 6. Zarządzenie podlega ogłoszeniu i wchodzi w życie z dniem podjęcia.

WÓJT
Włodzimierz Praszczyk

(podpis Wójta)

Załącznik nr 1
do zarządzenia nr 5/2017
z dnia 01.03.2017 r.
Wójta Urzędu Gminy w Olszówce

Polityka Bezpieczeństwa Danych Osobowych

URZĄD GMINY W OLSZÓWCE

Wersja nr 3		**Pieczęć:** URZĄD GMINY w OLSZÓWCE OLSZÓWKA 15 62-641 Olszówka NIP 666-14-02-313, R.000549329 tel. 63 273 90 10, fax 63 273 90 30	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Administrator Bezpieczeństwa informacji	01.03.2017 r.	Administrator Danych	01.03.2017 r.
Ilość stron: 26 (+ 20 załączników)			

Spis treści

1. Wstęp

Celem Polityki Bezpieczeństwa Danych Osobowych jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd Gminy w Olszówce.

Niniejsza Polityka określa obowiązki Administratora Danych w zakresie zabezpieczenia danych osobowych o których mowa w art. 36 Ustawy o Ochronie Danych Osobowych.

Niniejsza Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych podczas ich przetwarzania w postaci tradycyjnej (papierowej) oraz z wykorzystaniem systemów informatycznych.

Polityka Bezpieczeństwa Danych Osobowych została opracowana zgodnie z wymogami określonymi w § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) oraz z uwzględnieniem wytycznych GIODO oraz dobrych praktyk.

Polityka Bezpieczeństwa Danych Osobowych obowiązuje wszystkich pracowników Urzędu Gminy w Olszówce. Zasady określone w Polityce Bezpieczeństwa Danych Osobowych znajdują również odpowiednie zastosowanie do podmiotów współpracujących z Administratorem Danych na podstawie umowy, w tym dostawców usług.

Ochrona danych osobowych jest realizowana poprzez zastosowanie środków bezpieczeństwa fizycznego, informatycznego i procedury organizacyjne. System ochrony danych osobowych jest nadzorowany przez Administratora Bezpieczeństwa Informacji, który podlega oraz ściśle współpracuje w tym zakresie z Administratorem Danych.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

a. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
b. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
c. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
d. integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek nieautoryzowanej modyfikacji.

2. Podstawy prawne

Polityka Bezpieczeństwa Danych Osobowych jest zgodna z następującymi aktami prawnymi:

a. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., Nr 78, poz. 483 z późniejszymi zmianami),
b. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późniejszymi zmianami),
c. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024),
d. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536),
e. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014 r. poz. 1934).
f. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r. poz. 719).
g. Rozporządzenie 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 (Dz. U. z 2015 r. poz. 745).

3. Deklaracja ochrony

Administrator Danych świadomy wagi zagrożeń prywatności, w tym zagrożeń danych osobowych przetwarzanych w Urzędzie Gminy w Olszówce, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania m. in. takim zagrożeniom, jak:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne,
2. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne),
3. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą Administratora Danych,
4. naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
5. ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych przez Administratora Danych,
6. celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego Administratora Danych,
7. ataki z Internetu,
8. naruszenia zasad określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem zasad ochrony danych, w tym zwłaszcza:
   a. niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy,
   b. naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   c. ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych u Administratora Danych,
   d. ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora Danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru w niedostatecznie nadzorowanych pomieszczeniach Administratora Danych,
   e. niewykonywanie stosownych kopii zapasowych,
   f. przetwarzanie danych osobowych niezgodnie z celem Administratora Danych, w tym w celach prywatnych,
   g. wprowadzanie zmian do systemu informatycznego Administratora Danych i instalowanie programów bez zgody Administratora Systemu Informatycznego.

4. Postanowienia ogólne

4.1. Definicje

Ilekroć w niniejszej Polityce Bezpieczeństwa Danych Osobowych jest mowa o:

1. **Polityce** – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych, która została przyjęta jako obowiązujący dokument w Urzędzie Gminy w Olszówce.
2. **Instrukcji** – rozumie się przez to Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która została przyjęta jako obowiązujący dokument w Urzędzie Gminy w Olszówce,
3. **Ustawie** – rozumie się przez to Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późniejszymi zmianami),
4. **Rozporządzeniu** – rozumie się przez to Rozporządzenie 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 (Dz. U. z 2004 r. Nr 100, poz. 1024),
5. **Administratorze Danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych; w przypadku niniejszej Polityki Administratorem Danych jest Urząd Gminy w Olszówce reprezentowany przez Wójta; Wójt wykonuje obowiązki Administratora Danych, zwanego w dalszej części Polityki AD,
6. **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to osobę, którą AD powołał w drodze pisemnego zarządzenia, w celu nadzorowania systemu ochrony danych osobowych funkcjonującego w Urzędzie Gminy w Olszówce, zwaną w dalszej części Polityki ABI; Administratorem Bezpieczeństwa Informacji w Urzędzie Gminy w Olszówce jest Elwira Nita; Administrator Bezpieczeństwa Informacji został zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz spełnia wymogi określone w art. 36a pkt. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r., poz. 922 z późniejszymi zmianami),
7. **Administratorze Systemu Informatycznego** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego AD oraz wykonującą w nim czynności wymagające specjalnych uprawnień administracyjnych, zwaną w dalszej części Polityki ASI; Administratorem Systemu Informatycznego w Urzędzie Gminy w Olszówce jest Pan Piotr Łoboda,
8. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań; danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie

tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia,

9. **danych wrażliwych** – rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,
10. **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
11. **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
12. **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
13. **integralności systemu** – rozumie się przez to właściwość zapewniającą nienaruszalność systemu, niemożność jakiejkolwiek nieautoryzowanej modyfikacji,
14. **nośniku danych** – rozumie się przez to nośnik służący do zapisu i przechowywania informacji, np. taśmy, płyty, dyski twarde,
15. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a. osoby, której dane dotyczą,
    b. osoby upoważnionej do przetwarzania danych,
    c. przedstawiciela, o którym mowa w art. 31a Ustawy,
    d. podmiotu, o którym mowa w art. 31 Ustawy,
    e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
16. **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
17. **powierzeniu przetwarzania danych osobowych** – rozumie się przez to zlecenie wykonania czynności przetwarzania danych osobowych przez procesora na rzecz AD na podstawie stosownego zapisu w umowie zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Ustawy i Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z art. 31 Ustawy,
18. **procesorze** – rozumie się przez to osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której ustawa przyznaje zdolność prawną, której powierza się przetwarzanie danych osobowych na podstawie stosownego postanowienia umowy zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Ustawy i Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z art. 31 Ustawy,
19. **pracowniku** – rozumie się przez to każdą osobę zatrudnioną w Urzędzie Gminy w Olszówce w ramach stosunku pracy, na postawie umów cywilnoprawnych, pracowników tymczasowych oraz osoby odbywające praktyki, staże,

20. **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika, który został upoważniony na piśmie przez AD do przetwarzania danych osobowych w Urzędzie Gminy w Olszówce,
21. **użytkowniku** – rozumie się przez to pracownika upoważnionego na piśmie do przetwarzania danych osobowych, któremu ASI nadał identyfikator i przyznał hasło,
22. **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
23. **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
24. **sieci publicznej** – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 Ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489 z późniejszymi zmianami),
25. **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 Ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489 z późniejszymi zmianami),
26. **systemie informatycznym Administratora Danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, zasad przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
27. **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
28. **udostępnianiu danych osobowych** – rozumie się przez to przekazywanie, ujawnianie, rozpowszechnianie danych osobowych odbiorcy danych,
29. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
30. **anonimizacji** – rozumie się przez to takie przekształcenie danych osobowych, po którym niemożliwe jest przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej,
31. **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu,
32. **zabezpieczeniu systemu informatycznego** – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
33. **zbieraniu danych osobowych** – rozumie się przez to pozyskiwanie danych od osoby, której one dotyczą lub z innych źródeł,
34. **zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
35. **zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych osoby składającej oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści.

4.2. Cel Polityki Bezpieczeństwa Danych Osobowych

1. Wdrożenie Polityki u AD ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych poprzez wykonanie obowiązków wynikających z Ustawy i Rozporządzenia.
2. W związku z tym, że w zbiorach AD przetwarzane są między innymi dane wrażliwe, a system informatyczny posiada szerokopasmowe połączenie z Internetem, Polityka służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 Rozporządzenia.
3. Polityka opisuje niezbędny do uzyskania wymaganego poziomu bezpieczeństwa zbiór zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

4.3. Zakres stosowania

1. Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny, w tym w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorami AD.
2. Zasady określone w Polityce stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych oraz podmiotów przetwarzających dane osobowe w imieniu i na rzecz AD.

5. Organizacja przetwarzania danych osobowych

5.1. Administrator Danych

AD realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1. prowadzi dokumentację opisującą sposób przetwarzania danych osobowych, w szczególności:
   a. Politykę,
   b. Instrukcję,
2. zapewnia legalność przetwarzania danych osobowych,
3. nadzoruje i dba o zgodne z prawem powierzenie przetwarzania danych osobowych,
4. odpowiada za realizację obowiązków określonych w Rozdziale 4 Ustawy,
5. zapewnia odpowiednie środki techniczne i organizacyjne służące ochronie przetwarzanych danych osobowych, adekwatne do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczające dane przed:
   a. udostępnieniem osobom nieupoważnionym,
   b. zabraniem przez osobę nieuprawnioną,
   c. zmianą, utratą, uszkodzeniem lub zniszczeniem,
6. wyznacza ABI oraz określa zakres jego zadań i czynności wg wzoru stanowiącego załącznik nr 1.1,
7. wyznacza ASI jako osobę odpowiedzialną za bezpieczeństwo systemów informatycznych służących do przetwarzania danych osobowych oraz określa zakres jego zadań i czynności (wzór powołania ASI stanowi załącznik nr 1.3),
8. upoważnia poszczególne osoby do przetwarzania danych osobowych w indywidualnie określonym zakresie, odpowiadającym zakresowi ich obowiązków, bądź wyznacza w tym celu osobę, która na mocy pełnomocnictwa będzie odpowiedzialna za realizację tego działania,
9. nadzoruje prowadzenie przez ABI ewidencji osób upoważnionych do przetwarzania danych osobowych,
10. nadzoruje zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
11. zapewnia użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem przetwarzanie danych osobowych,
12. odpowiada za spełnienie obowiązku rejestracji zbioru danych w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych,
13. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania danych osobowych,
14. nadzoruje przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych,
15. w sytuacji przekazywania danych osobowych do państwa trzeciego, stosuje się uregulowania wynikające z Rozdziału 7 Ustawy,
16. Administrator Danych na piśmie wyznacza osobę zastępującą go w czynnościach AD na wypadek jego nieobecności lub niemożliwości pełnienia przez niego tej funkcji.

5.2. Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji przedkłada Administratorowi Danych oświadczenie według wzoru stanowiącego załącznik nr 1.2, o spełnieniu warunków określonych w Ustawie w art. 36a ust. 5 t.j.:

1. posiadaniu pełnej zdolności do czynności prawnych oraz korzystaniu z pełni praw publicznych,
2. posiadaniu odpowiedniej wiedzy w zakresie ochrony danych osobowych,
3. niekaralności za umyślne przestępstwo.

ABI zobowiązany jest do zgłoszenia każdej zmiany powodującej unieważnienie przedłożonego oświadczenia.

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

1) sprawuje nadzór nad bezpieczeństwem i ochroną danych osobowych zgodnie z wymogami Ustawy i Rozporządzenia,
2) zapewnia przetwarzanie danych zgodnie z przepisami Polityki i Instrukcji,
3) sprawuje nadzór nad wdrożeniem i funkcjonowaniem adekwatnych środków ochrony fizycznej, a także środków organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych,
4) przygotowuje upoważnienia do przetwarzania danych osobowych oraz je anuluje oraz sprawuje nadzór nad ich podpisaniem przez AD, bądź wyznaczoną w tym celu osobę, która na mocy pełnomocnictwa będzie odpowiedzialna za realizację tego działania,
5) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych wg wzoru stanowiącego załącznik nr 1.6,
6) przeprowadza wewnętrzne audyty (sprawdzenia) przestrzegania przepisów Ustawy i Rozporządzenia oraz przestrzegania zasad wynikających z Polityki i Instrukcji,
7) opracowują sprawozdania (1 w roku) z działalności dla AD oraz dla GIODO na każde żądanie stanowiące załącznik nr 1.18,
8) nadzoruje udostępnianie danych osobowych,
9) nadzoruje powierzenie przetwarzania danych osobowych,
10) nadzoruje spełnianie wymagań Ustawy i Rozporządzenia przez procesora,
11) opracowuje nowe i aktualizuje istniejące wnioski rejestracyjne zgłaszane do GIODO oraz prowadzą wewnętrzny jawny rejestr zbiorów danych osobowych wg wzoru stanowiącego załącznik nr 1.19,
12) prowadzi korespondencję z GIODO,
13) przygotowuje wzory dokumentów dotyczące ochrony danych osobowych,
14) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, w tym Politykę i Instrukcję,
15) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych u AD,
16) wspólnie z AD podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych ze szczególnym uwzględnieniem systemu informatycznego,

17) przygotowuje regulamin ochrony danych osobowych, dostosowany do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,
18) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych lub współpracują w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym,
19) współpracuje z ASI.

ABI ma prawo:
1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych osobowych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z Ustawą,
2) żądania od pracowników, użytkowników, osób upoważnionych złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego dotyczącego przetwarzania danych i ich zabezpieczenia,
3) występowania w porozumieniu z AD do procesora o wyjaśnienia i informacje dotyczące powierzonego przetwarzania danych,
4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5) żądania udostępnienia do kontroli dokumentacji, urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych u AD oraz u procesorów,
6) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych u AD,
7) wydawania pracownikom wiążących poleceń dotyczących zasad przetwarzania i ochrony danych osobowych u AD.

ABI odpowiada za zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych z uwzględnieniem następujących zasad:
1) ABI opracowuje regulamin ochrony danych osobowych, z którym każdy nowozatrudniony pracownik zobowiązany jest zapoznać się przed nadaniem mu upoważnienia do przetwarzania danych osobowych,
2) ABI dokonuje przeszkolenia pracowników zgodnie z przyjętym planem szkoleń,
3) ABI prowadzi dokumentację dotyczącą przeprowadzonych szkoleń,
4) tematyka szkoleń obejmuje w szczególności:
   a) przepisy dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, które one dotyczą,
   c) obowiązki osób upoważnionych do przetwarzania danych osobowych,
   d) zasady określone w Polityce,
   e) zasady określone w Instrukcji,
5) w celu zapewnienia wysokiego poziomu bezpieczeństwa ABI zapoznaje z zasadami ochrony danych osobowych, a zwłaszcza zabezpieczeń tych danych pracowników, którzy nie przetwarzają danych osobowych, ale z racji realizowanych przez nich zadań mogą

przyczynić się do zapewnienia wysokiego poziomu bezpieczeństwa danych, w tym personelu sprzątającego i ochrony,

6) w celu przeprowadzenia szkolenia ABI może korzystać z pomocy zewnętrznego podmiotu posiadającego odpowiednio wysoki poziom wiedzy i kwalifikacji do prowadzenia szkoleń z zakresu ochrony danych osobowych.

ABI nadzoruje przestrzeganie zasad ochrony danych osobowych zwłaszcza poprzez:

1) prowadzenie kontroli planowych i doraźnych oraz dokumentowanie czynności kontrolnych według wzoru stanowiącego załącznik nr 1.17,
2) coroczne opracowywanie planu kontroli w zakresie ochrony danych osobowych w Urzędzie Gminy w Olszówce; plan kontroli obejmuje rok kalendarzowy,
3) przeprowadzanie audytu systemu informatycznego,
4) przeprowadzanie audytu zabezpieczeń fizycznych,
5) pisemne informowanie AD o wynikach przeprowadzonych kontroli i audytów.

5.3. Administrator Systemu Informatycznego

ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym AD w tym zwłaszcza:

1. wdraża zasady ochrony danych osobowych określone w Polityce oraz Instrukcji i dokumentach z nimi związanych,
2. zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora,
3. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
4. przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w Instrukcji,
5. nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
6. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
7. wyrejestrowuje użytkowników na polecenie AD lub ABI,
8. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje AD o naruszeniu oraz współdziała z nimi przy usuwaniu skutków naruszenia,
9. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10. wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe,
11. wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
12. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych

urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

5.4. Obowiązki i odpowiedzialność pracownika Urzędu Gminy w Olszówce

1. Pracownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez AD i tylko w celu wykonywania powierzonych mu obowiązków.
2. Pracownik przetwarzający dane w systemie informatycznym, w tym przetwarzający dane w zbiorach danych, zostaje przypisany do indywidualnego i niepowtarzalnego identyfikatora użytkownika, niezbędnego do pracy w systemie.
3. Pracownik, który nie przetwarza danych osobowych a posiada wiedzę o sposobach zabezpieczenia danych osobowych, zobowiązany jest do podpisania oświadczenia zobowiązującego do zachowania w tajemnicy zastosowanych u AD środków bezpieczeństwa wg wzoru stanowiącego załącznik nr 1.5.
4. Pracownik zobowiązany jest do zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym z wyciągami z niniejszej Polityki i Instrukcji oraz Regulaminem ochrony danych osobowych.
5. Pracownik zobowiązany jest do stosowania określonych przez AD, ABI oraz ASI zasad oraz wytycznych mających na celu zgodne z prawem przetwarzanie danych osobowych.
6. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieuprawnionym.
7. Pracownik, który dopuści się naruszenia zasad bezpiecznego przetwarzania, w szczególności świadomie udostępni dane osobie nieuprawnionej, może zostać pociągnięty do odpowiedzialności skutkującej rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

Ponadto każdy pracownik upoważniony do przetwarzania danych osobowych ma obowiązek:

1. nieużywania powtórnego jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe,
2. zachowania tajemnicy danych przetwarzanych w siedzibie AD, w tym także wobec osób najbliższych,
3. pilnego strzeżenia nośników danych, w tym akt, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie,
4. ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
5. zabezpieczenie nośnika, na którym zapisano hasła, w taki sposób by był niedostępny dla osób trzecich,
6. niepodłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia,
7. dbania o prawidłową wentylację komputerów,

8. przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ABI oraz ASI,
9. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe pod nieobecność osoby upoważnionej do przetwarzania danych osobowych,
10. opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób,
11. udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej,
12. wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz wypisów z nich wyłącznie w postaci zaszyfrowanej,
13. wykonywania kopii roboczych przetwarzanych danych tak często, aby zapobiec ich utracie,
14. kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera,
15. chowania do szaf zamykanych na klucz wszelkich akt i wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy,
16. usuwania przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy,
17. zamykania okien w razie różnych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
18. zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
19. zamykania drzwi na klucz i zabierania ze sobą w przypadku czasowego opuszczenia pomieszczenia, które pozostaje bez dozoru,
20. niepozostawiana kluczy w drzwiach od strony zewnętrznej pomieszczeń, w których przetwarza się dane osobowe, także podczas obecności wewnątrz osób upoważnionych,
21. zamykania drzwi na klucz po zakończeniu pracy w danym dniu,
22. umieszczaniu kluczy do pomieszczeń i szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy i nieujawnianie osobom nieupoważnionym informacji o miejscu przechowywania kluczy.

6. Infrastruktura przetwarzania danych osobowych

6.1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Szczegółowe informacje na temat obszarów, w których są przechowywane zbiory danych osobowych prowadzonych w formie papierowej i elektronicznej, zawierającej dane osobowe, opisane zostały w załączniku nr 1.7 pt. „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe".

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe prowadzi i aktualizuje ABI.

6.2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz zbiorów danych osobowych prowadzonych w postaci dokumentacji papierowej oraz w formie elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany został w załączniku nr 1.8 pt. „Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych".

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych prowadzi i aktualizuje ABI.

6.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbiorów danych osobowych prowadzonych w postaci dokumentacji papierowej oraz w formie elektronicznej wraz ze wskazaniem pól informacyjnych, opisany został w załączniku nr 1.9 pt. „Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi".

Opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi dokonuje i aktualizuje ABI.

6.4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Sposób przepływu danych pomiędzy poszczególnymi systemami, opisany został w załączniku nr 1.10 pt. „Sposób przepływu danych pomiędzy poszczególnymi systemami ".

Sposób przepływu danych pomiędzy poszczególnymi systemami opisuje i aktualizuje ABI.

7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

7.1. Środki ochrony fizycznej

Szczegółowy wykaz środków ochrony fizycznej zawarty jest w Instrukcji.

7.2. Środki sprzętowe, informatyczne i telekomunikacyjne

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis środków ochrony w ramach systemu operacyjnego oraz środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych zawarty jest w Instrukcji.

7.3. Środki organizacyjne

1. Powołano ABI.
2. Opracowano i wdrożono Politykę oraz Instrukcję.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
4. Do danych osobowych mają dostęp jedynie osoby posiadające pisemne upoważnienie nadane przez AD.
5. Osoby zatrudnione przy przetwarzaniu danych są zaznajamiane z przepisami dotyczącymi ochrony danych osobowych.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich oraz sposobów ich zabezpieczenia w tajemnicy.
7. Powierzenie danych osobowych do podmiotów trzecich jest nadzorowane oraz odbywa się na podstawie pisemnej umowy powierzenia przetwarzania danych.
8. Podpisano klauzule poufności z podmiotami zewnętrznymi mającymi dostęp do danych osobowych w Urzędzie Gminy w Olszówce.
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej oraz w warunkach zapewniających bezpieczeństwo danych.
10. Zbiory danych osobowych podlegające zgłoszeniu zostały zgłoszone do rejestru prowadzonego przez GIODO.
11. Prowadzony jest wewnętrzny jawny rejestr zbiorów danych osobowych przez ABI.

12. ABI przeprowadza regularne przeglądy Polityki oraz Instrukcji oraz sprawdzenia w zakresie stosowania przyjętych zasad przez osoby upoważnione.

8. Zasady przetwarzania danych osobowych

8.1. Procedura nadawania upoważnień do przetwarzania danych osobowych

1. Pracownik dopuszczony do przetwarzania danych osobowych przed przystąpieniem do czynności powinien posiadać stosowane upoważnienie nadawane w formie pisemnej przez AD. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik 1.4.
2. Przed wydaniem upoważnienia do przetwarzania danych osobowych osoba upoważniona zostaje zaznajomiona z zasadami bezpieczeństwa i ochrony danych osobowych.
3. Upoważnienia do przetwarzania danych osobowych opracowuje i wystawia ABI,
4. Upoważnienie udzielane jest na czas wykonywania przez osobę upoważnioną czynności przetwarzania danych na powierzonym jej stanowisku pracy lub na czas realizacji powierzonego zadania.
5. Utrata uprawnień do przetwarzania danych osobowych zawartych w upoważnieniu może nastąpić z następujących powodów:
   a. rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z AD,
   b. zmiany stanowiska pracy u AD, na którym nie ma konieczności posiadania dostępu do zbiorów danych osobowych, a nowy zakres czynności nie wykazuje obowiązków służbowych związanych z przetwarzaniem danych osobowych,
   c. umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, Rozporządzeniu, Polityce, Instrukcji .
6. W przypadku utraty uprawnień do przetwarzania danych osobowych AD zobowiązany jest do niezwłocznego anulowania upoważnienia do przetwarzania danych osobowych.
7. Anulowanie upoważnienia odnotowywane jest przez ABI w ewidencji osób upoważnionych do przetwarzania danych osobowych.
8. Jeżeli nadanie, zmiana lub utrata uprawnień wiąże się z przetwarzaniem danych w zbiorze za pośrednictwem systemu informatycznego szczegóły trybu postępowania precyzuje Instrukcja.

8.2. Procedura informowania o powstaniu nowego zbioru danych osobowych

1. Decyzję o zbieraniu danych osobowych oraz stworzeniu nowego zbioru danych osobowych podejmuje AD.
2. Pracownik wnioskuje do ABI o utworzenie nowego zbioru danych osobowych. Wniosek musi być złożony na 30 dni przed rozpoczęciem zbierania danych osobowych na wzorze dokumentu stanowiącego załącznik 1.15.

3. Po otrzymaniu wniosku ABI określa możliwość i celowość utworzenia zbioru, formę i tryb wykonania obowiązku informacyjnego oraz rozstrzyga kwestię rejestracji zbioru w ewidencji GIODO lub wpisania zbioru do jawnego rejestru prowadzonego przez ABI. Jeżeli zbiór podlega rejestracji w rejestrze GIODO, rozpoczęcie zbierania danych możliwe jest dopiero po zgłoszeniu zbioru, a jeżeli w zbiorze przetwarzane są także dane wrażliwe, po zgłoszeniu i wpisie zbioru do rejestru GIODO.
4. ABI przedstawia wniosek wraz z opinią do akceptacji AD.
5. W przypadku konieczności zbierania nowego rodzaju danych do istniejącego zbioru stosuje się zasady opisane powyżej.

8.3. Procedura udostępniania danych osobowych

1. Udostępnianie danych osobowych odbiorcom danych może nastąpić w przypadku spełnienia jednej z przesłanek określonych w art. 23 ust. 1 pkt 1-5 Ustawy oraz w art. 27 ust. 2 pkt 1-10 Ustawy:
   a. osoba, której dane dotyczą wyrazi na to zgodę,
   b. jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
   c. jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   d. jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   e. jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą,
   f. osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
   g. przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
   h. przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
   i. jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
   j. przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

k. przetwarzanie jest niezbędne do wykonania zadań AD odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w Ustawie,
l. przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
m. przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
n. jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
o. przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

2. W procesie opiniowania dokumentacji pod kątem zasadności udostępniania danych osobowych uczestnicy AD oraz ABI.
3. Udostępnianie danych osobowych może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
   a. oznaczenie wnioskodawcy,
   b. wskazanie przepisów uprawniających do dostępu do informacji,
   c. określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
   d. wskazanie imienia, nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.
4. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania.
5. Osoba udostępniająca dane osobowe jest obowiązana zażądać od osoby uprawnionej pokwitowania udostępnienia danych zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.
6. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie otrzymania informacji. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
7. Jeśli osoba uprawniona pouczyła osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.
8. ABI prowadzi rejestr udostępnień danych osobowych w celu zapewnienia kontroli procesu udostępnień wg. załącznika nr 1.13. Za prowadzenie rejestru udostępnień danych osobowych odpowiedzialny jest ABI.

8.4. Procedura powierzenia przetwarzania danych osobowych

1. AD może powierzyć przetwarzanie danych osobowych innemu podmiotowi zewnętrznemu w drodze umowy zawartej na piśmie. Ogólny wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 1.11.
2. AD oraz ABI opiniują umowy pod kątem powierzenia przetwarzania danych osobowych.
3. Szczegółowy wykaz zbiorów danych osobowych oraz podmiotów, którym dane osobowe są powierzane do przetwarzania jest prowadzony przez ABI wg załącznika nr 1.12 „Ewidencja podmiotów, którym powierzono przetwarzanie danych osobowych".
4. Procesor, któremu powierzono przetwarzanie danych obowiązany jest między innymi do:
   a. stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
   b. wykorzystania powierzonych mu danych wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie, jak również zachować poufność danych osobowych powierzonych mu do przetwarzania,
   c. opracowania dokumentacji dotyczącej przetwarzania danych osobowych,
   d. zapewnienia, aby do przetwarzania danych mogły być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD,
   e. zapewnienia kontroli nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
   f. prowadzenia ewidencji osób upoważnionych do ich przetwarzania,
   g. obowiązania osób, które zostały upoważnione do przetwarzania danych do zachowania w tajemnicy tych danych osobowych oraz sposobów i zabezpieczania,
   h. poinformowania AD o sytuacji podpowierzenia oraz wskazania w umowie nazwy podmiotu wraz z danymi teleadresowymi, któremu zostaną podpowierzone dane osobowe,
   i. zwrotu wszelkich powierzonych danych osobowych do AD oraz usunięcia ze swoich zbiorów wszystkich danych osobowych, które przetwarzał w związku z wykonywaniem czynności na rzecz AD, na podstawie sporządzonego protokołu usunięcia danych osobowych, którego wzór stanowi załącznik nr 1.16.

8.5. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   a. nieautoryzowany dostęp do danych,
   b. utrata nośników,
   c. nieautoryzowane modyfikacje lub zniszczenie danych,
   d. udostępnianie danych nieautoryzowanym podmiotom,
   e. nielegalne ujawnianie danych,
   f. pozyskiwanie danych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony w Urzędzie Gminy w Olszówce jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego, który zobowiązany jest do pisemnego bądź e-mailowego poinformowania o zgłoszeniu AD oraz ABI.
3. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a. opis symptomów naruszenia ochrony danych osobowych,
   b. określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   c. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia,
   d. określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. ASI, ABI lub inna upoważniona przez nich osoba podejmuje wszelkie działania mające na celu:
   a. minimalizację negatywnych skutków zdarzenia,
   b. wyjaśnienie okoliczności zdarzenia,
   c. zabezpieczenie dowodów zdarzenia,
   d. umożliwienie dalszego bezpiecznego przetwarzania danych.
5. W celu realizacji procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych ASI, ABI lub inna upoważniona przez nich osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a. żądania wyjaśnień od pracowników,
   b. korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów),
   c. nakazanie przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
6. Odmowa udzielenia wyjaśnień lub współpracy z ASI lub ABI traktowana będzie jako naruszenie obowiązków pracowniczych.

7. ABI po stwierdzeniu naruszenia bezpieczeństwa danych osobowych opracowuje raport końcowy na podstawie wzoru wg załącznika nr 1.14, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.
8. Nieprzestrzeganie zasad określonych niniejszą Polityką stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności porządkowej określonej w Kodeksie Pracy.
9. Jeżeli skutkiem działania określonego w ustępie 8 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w Kodeksie Pracy.
10. Jeżeli skutkiem działania określonego w ustępie 8 jest ujawnienie informacji osobie nieuprawnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.
11. Jeżeli skutkiem działania określonego w ustępie 8 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w Kodeksie Pracy ora Prawa Cywilnego.

9. Przeglądy Polityki Bezpieczeństwa Informacji i audyty systemu

1. Polityka powinna być poddawana przeglądowi/sprawdzeniu (audytowi) przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych ABI może zarządzić przegląd Polityki stosownie do potrzeb.
2. Do kontroli stanu ochrony danych osobowych w Urzędzie Gminy w Olszówce upoważnieni są:
   a. AD,
   b. ABI,
   c. ASI,
   d. osoby wyznaczone przez AD.
3. ABI analizuje, czy Polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   a. zmian w budowie systemu informatycznego,
   b. zmian organizacyjnych AD, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   c. zmian w obowiązującym prawie.
4. Raz do roku kontroli podlegają systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. ABI przygotowuje plan kontroli uwzględniając zakres oraz potrzeby fizyczne, czasowe i osobowe.
6. Kontroli podlega sprzęt, system teleinformatyczny, realizacja zabezpieczeń przez pracowników Urzędu Gminy w Olszówce oraz przestrzeganie Polityki.
7. ABI po uzgodnieniu z AD może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

8. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z AD. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez ABI i przedstawiane w formie pisemnej do wiadomości AD.
9. AD biorąc pod uwagę wnioski administratorów, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.
10. Za wyniki przeprowadzonych audytów odpowiedzialność ponosi AD.

10. Postanowienia końcowe

1. Niniejsza Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Upoważnienie do przetwarzania danych osobowych przechowywane jest w aktach osobowych pracownika.
3. Pracownik, który nie przetwarza danych osobowych, a posiada wiedzę o sposobach zabezpieczenia danych osobowych zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z przepisami Ustawy oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u AD, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami Ustawy oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u AD, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
5. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
6. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
7. Niezastosowanie się do prowadzonej przez AD, której założenia określa niniejszy dokument i naruszenia procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51-52 Ustawy oraz art. 266 Kodeksu karnego.
8. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby z Ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
9. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Ustawy oraz wydanych na jej podstawie aktów wykonawczych.
10. Wprowadzenie jakichkolwiek zmian w Polityce lub wzorach załączników do Polityki, wymaga uzupełnienia załącznika nr 1.20.

11. Spis załączników

1. Załącznik 1.1 – Wzór powołania Administratora Bezpieczeństwa Informacji
2. Załącznik 1.2 – Wzór oświadczenia Administratora Bezpieczeństwa Informacji
3. Załącznik 1.3 – Wzór powołania Administratora Systemu Informatycznego
4. Załącznik 1.4 – Wzór upoważnienia do przetwarzania danych osobowych
5. Załącznik 1.5 – Wzór oświadczenia o wzięciu udziału w szkoleniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych
6. Załącznik 1.6 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
7. Załącznik 1.7 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
8. Załącznik 1.8 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
9. Załącznik 1.9 – Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
10. Załącznik 1.10 – Sposób przepływu danych pomiędzy poszczególnymi systemami
11. Załącznik 1.11 – Wzór umowy powierzenia przetwarzania danych osobowych
12. Załącznik 1.12 – Ewidencja podmiotów, którym powierzono przetwarzanie danych osobowych
13. Załącznik 1.13 – Rejestr udostępnień danych osobowych
14. Załącznik 1.14 – Wzór raportu z naruszenia bezpieczeństwa danych osobowych
15. Załącznik 1.15 – Wniosek o planowanym utworzeniu zbioru danych osobowych
16. Załącznik 1.16 – Wzór protokołu usunięcia danych osobowych ze zbioru
17. Załącznik 1.17 – Wzór notatki służbowej ABI
18. Załącznik 1.18 – Wzór sprawozdania dla AD
19. Załącznik 1.19 – Wzór jawnego rejestru zbiorów danych osobowych
20. Załącznik 1.20 – Historia zmian

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Urzędu Gminy w Olszówce

§1
REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. Na podstawie rozdziału 5.4 pkt 4. Polityki Bezpieczeństwa Danych Osobowych, wprowadza się w Urzędzie Gminy w Olszówce Regulamin Ochrony Danych Osobowych (zwany dalej „Regulaminem").
2. Regulamin stanowi wyciąg podstawowych obowiązków i uprawnień członków personelu Urzędu Gminy w Olszówce oraz procedur związanych z przetwarzaniem danych osobowych, określonych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wdrożonej do stosowania w Urzędzie Gminy w Olszówce.
3. Celem Regulaminu jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd Gminy w Olszówce poprzez określenie reguł dotyczących procedur zapewnienia bezpieczeństwa danych osobowych podczas ich przetwarzania w postaci tradycyjnej (papierowej) oraz z wykorzystaniem systemów informatycznych. Regulamin określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych w celu zabezpieczenia ich przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Niniejszy Regulamin obowiązuje wszystkich pracowników Urzędu Gminy w Olszówce. Zasady określone w Regulaminie znajdują również odpowiednie zastosowanie do podmiotów współpracujących z Administratorem Danych na podstawie umowy, w tym dostawców usług.

§2
DEFINICJE UŻYTE W REGULAMINIE

1. **Administrator Danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem Danych jest Urząd Gminy w Olszówce reprezentowany przez Wójta Gminy w Olszówce . Wójt Gminy w Olszówce wykonuje obowiązki Administratora Danych, zwanego w dalszej części Regulaminu AD.
2. **Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę, którą AD powołał w drodze pisemnego zarządzenia, w celu nadzorowania systemu ochrony danych osobowych funkcjonującego w Urzędzie Gminy w Olszówce zwaną w dalszej części Regulaminu ABI. Administratorem Bezpieczeństwa Informacji w Urzędzie Gminy w Olszówce jest Pani Elwira Nita,
3. **Administrator Systemu Informatycznego** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego AD oraz wykonującą w nim czynności wymagające specjalnych uprawnień administracyjnych, zwaną w dalszej części Regulaminu ASI. Administratorem Systemu Informatycznego w Urzędzie Gminy w Olszówce jest Pan Piotr Łoboda,
4. **Dane osobowe** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to poniesienia nadmiernych kosztów, czasu i działań. Danymi osobowymi będą zatem, zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.
5. **Pracownik** – rozumie się przez to każdą osobę zatrudnioną w Urzędzie Gminy w Olszówce w ramach stosunku pracy, na postawie umów cywilnoprawnych oraz osoby odbywające praktyki, staże.
6. **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to pracownika, który został upoważniony na piśmie przez AD do przetwarzania danych osobowych w Urzędzie Gminy w Olszówce.

§3
ODPOWIEDZIALNOŚĆ PRACOWNIKA PRZETWARZAJĄCEGO DANE OSOBOWE

1. Pracownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez AD i tylko w celu wykonywania powierzonych mu obowiązków.
2. Pracownik przetwarzający dane w systemie informatycznym, w tym przetwarzający dane w zbiorach danych, zostaje przypisany do indywidualnego i niepowtarzalnego identyfikatora użytkownika, niezbędnego do pracy w systemie.
3. Pracownik upoważniony do przetwarzania danych osobowych zobowiązany jest do podpisania oświadczenia zobowiązującego do zachowania w tajemnicy danych osobowych oraz przestrzegania zasad ich bezpiecznego przetwarzania, a także zachowania w tajemnicy zastosowanych u AD środków bezpieczeństwa.
4. Pracownik, który nie przetwarza danych osobowych, a posiada wiedzę o sposobach zabezpieczenia danych osobowych, zobowiązany jest do podpisania oświadczenia zobowiązującego do zachowania w tajemnicy zastosowanych u AD środków bezpieczeństwa.
5. Pracownik zobowiązany jest do zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym z niniejszym Regulaminem.
6. Pracownik zobowiązany jest do stosowania określonych przez AD oraz ABI zasad oraz wytycznych mających na celu zgodne z prawem przetwarzanie danych osobowych.
7. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieuprawnionym.
8. Pracownik, który dopuści się naruszenia zasad bezpiecznego przetwarzania, w szczególności świadomie udostępni dane osobie nieuprawnionej, może zostać pociągnięty do odpowiedzialności skutkującej rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

§4
ODPOWIEDZIALNOŚĆ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Niezastosowanie się do prowadzonej przez AD Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji zarządzenia system informatycznym służącym do przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 Kodeksu Pracy. Niezależnie od rozwiązania stosunku pracy, osoby popełniające przestępstwo będą pociągnięte do odpowiedzialności karnej, zwłaszcza na podstawie art. 51.1-52 Ustawy o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.), oraz art. 266 Kodeksu karnego (Dz.U. z 2016r. poz. 1137). Każdy pracownik upoważniony do przetwarzania danych osobowych ma obowiązek:
   - nieużywania powtórnego jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe;
   - zachowania tajemnicy danych przetwarzanych w siedzibie AD, w tym także wobec osób najbliższych;
   - pilnego strzeżenia nośników danych, w tym akt, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie;
   - ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
   - zabezpieczenie nośnika, na którym zapisano hasła, w taki sposób by był niedostępny dla osób trzecich;
   - niepodłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia;
   - dbania o prawidłową wentylację komputerów;
   - przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ASI;

- niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe pod nieobecność osoby upoważnionej do przetwarzania danych osobowych;
- opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
- udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
- wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz wypisów z nich wyłącznie w postaci zaszyfrowanej;
- wykonywania kopii roboczych przetwarzanych danych tak często, aby zapobiec ich utracie;
- kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera;
- chowania do szaf zamykanych na klucz wszelkich akt i wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
- usuwania przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy, przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
- zamykania okien w razie różnych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
- zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
- zamykania drzwi na klucz i zabierania go ze sobą w przypadku czasowego opuszczenia pomieszczenia, które pozostaje bez dozoru;
- niepozostawiania kluczy w drzwiach od strony zewnętrznej pomieszczeń, w których przetwarza się dane osobowe, także podczas obecności wewnątrz osób upoważnionych;
- zamykania drzwi na klucz po zakończeniu pracy w danym dniu;
- umieszczaniu kluczy do pomieszczeń i szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy i nieujawnianie osobom nieupoważnionym informacji o miejscu przechowywania kluczy.

§5
PRZETWARZANIE DANYCH OSOBOWYCH PRZY UŻYCIU SYSTEMU INFORMATYCZNEGO

1. W ramach wykonywania obowiązków służbowych, pracownicy Urzędu Gminy w Olszówce korzystający z systemu informatycznego, w tym urządzeń elektronicznych, komputerów, laptopów, tabletów, programów lub aplikacji komputerowych oraz informatycznych nośników danych, zobowiązani są zapewnić bezpieczeństwo przetwarzanych danych osobowych poprzez bezwzględne przestrzeganie następujących zasad:
   - można korzystać wyłącznie z oprogramowania i systemów dopuszczonych przez ASI do eksploatacji, w szczególnych sytuacjach dopuszczone jest stosowanie lub wprowadzanie do systemu informatycznego aplikacji, pod warunkiem przestrzegania warunków umowy licencyjnej oraz uzyskania pisemnej lub e-mail zgody od ASI;
   - zabrania się korzystania z programów i systemów nie będących własnością Urzędu Gminy w Olszówce lub nie dopuszczonych przez ASI do użytkowania; instalacji, bądź deinstalacji oprogramowania może dokonać tylko ASI, bądź wyznaczona przez niego osoba; ASI zobowiązany jest do nadzorowania zgodności instalowanego oprogramowania z posiadanymi licencjami; zakupy oprogramowania muszą być zaakceptowane przez ADO i przez ASI.
2. Sprzęt IT jest narzędziem pracy pracownika Urzędu Gminy w Olszówce Użytkowanie sprzętu IT do wykonywania pracy dla innej firmy lub własnej działalności gospodarczej jest zabronione. Zabronione jest kopiowanie programów, danych oraz innych materiałów przy użyciu PC, poza prawnie dozwolonym, wykonywanym w celach służbowych. W szczególności należy przestrzegać poniższych zasad:
   - w pomieszczeniu, w którym są przetwarzane dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika z ważnym upoważnieniem do przetwarzania danych osobowych albo w obecności ABI;
   - ekrany komputerów powinny być zwrócone w stronę przeciwną do osoby obsługiwanej;
   - w przypadku opuszczenia stanowiska pracy, użytkownik zobowiązany jest aktywizować wygaszacz ekranu lub zablokować w inny sposób stację roboczą;

- wszystkich użytkowników systemu informatycznego obowiązuje zakaz samodzielnego instalowania oprogramowania;
- wszystkich użytkowników systemu informatycznego obowiązuje zakaz wykonywania kopii zbiorów danych osobowych; zbiory danych osobowych mogą być kopiowane tylko przez ASI lub automatycznie przez dedykowany system, z zachowaniem procedur ochrony danych osobowych.

3. W celu zapewnienia wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych zastosowano następujące środki bezpieczeństwa:
   - dostęp do systemów operacyjnych, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
   - zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
   - zastosowano ręczną okresową zmianę haseł;
   - zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
   - dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
4. Kopie bezpieczeństwa baz danych z jednostek tworzone są pod kontrolą ASI.

§6
KORZYSTANIE PRZEZ UŻYTKOWNIKÓW Z POCZTY ELEKTRONICZNEJ

1. Użytkownicy poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:
   - przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych, w przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z ASI;
   - użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu;
   - w przypadku przesyłania informacji wrażliwych poza Urząd Gminy w Olszówce, należy wykorzystywać mechanizmy kryptograficzne;
   - jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu; dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją;
   - użytkownicy nie powinni otwierać przesyłek mailowych od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi; w przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z ASI;
   - użytkownicy nie mogą uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną; w takim przypadku użytkownik powinien poinformować o zdarzeniu ASI, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji;
   - użytkownicy nie mogą rozsyłać za pośrednictwem poczty elektronicznej informacji, które mogą mieć wpływ na bezpieczeństwo i stabilność systemu informatycznego;
   - użytkownicy nie mogą rozsyłać wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów; określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej;
   - użytkownicy powinni okresowo usuwać niepotrzebne wiadomości pocztowe.

§7
KORZYSTANIE PRZEZ UŻYTKOWNIKÓW Z SIECI PUBLICZNEJ INTERNET

1. Użytkownicy Internetu zobowiązani są do przestrzegania następujących zasad:
   - zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawnie zabronionej, obscenicznej bądź pornograficznej;
   - do wymiany korespondencji w czasie korzystania z systemu informatycznego jest wykorzystywana tylko służbowa poczta elektroniczna;
   - użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane;
   - do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez ASI formy dostępu;
   - ASI może stosować mechanizmy monitorujące przeglądanie Internetu przez użytkowników.

§8
PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   - nieuprawnionego ujawniania danych osobowych;
   - udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym;
   - zabrania danych przez osobę nieupoważnioną;
   - uszkodzenia jakiegokolwiek elementu systemu informatycznego.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony w Urzędzie Gminy w Olszówce jest zobowiązany:
   - przerwać przetwarzanie danych osobowych;
   - niezwłocznie powiadomić o tym fakcie ABI oraz bezpośredniego przełożonego, a następnie stosować się do podjętych przez nich decyzji.
3. Odmowa udzielenia wyjaśnień lub współpracy z ASI lub ABI traktowana będzie jako naruszenie obowiązków pracowniczych.

§9
ODPOWIEDZIALNOŚĆ ZA NARUSZENIE REGULAMINU

1. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym Regulaminem.
2. Naruszenie obowiązków wynikających z niniejszego Regulaminu oraz przepisów o ochronie danych osobowych, może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51-52 Ustawy o ochronie danych osobowych.

Załącznik nr 1.1	Wzór powołania Administratora Bezpieczeństwa Informacji	Wersja 2

Działając na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.) z dniem .....

zarządzam, co następuje:

§ 1. Powołuję Pana/Panią* ..... PESEL ..... na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy w Olszówce.

§ 2. Ustalam zakres obowiązków Administratora Bezpieczeństwa Informacji oraz jego zastępcy w Urzędzie Gminy w Olszówce określony w załączniku Nr 1 do niniejszego zarządzenia.

§ 3. Zarządzenie podlega ogłoszeniu i wchodzi w życie z dniem podjęcia.

_____

(data, podpis Wójta)

_____

(data, podpis Administratora Bezpieczeństwa Informacji)

*niepotrzebne skreślić

Załącznik nr .....
do zarządzenia nr ..... z dnia .....
Wójta Urzędu Gminy w Olszówce

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad bezpieczeństwem i ochroną danych osobowych zgodnie z wymogami Ustawy i Rozporządzenia,
2) zapewnia przetwarzanie danych zgodnie z przepisami Polityki i Instrukcji,
3) sprawuje nadzór nad wdrożeniem i funkcjonowaniem adekwatnych środków ochrony fizycznej, a także środków organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych,
4) przygotowuje upoważnienia do przetwarzania danych osobowych oraz je anuluje oraz sprawuje nadzór nad ich podpisaniem przez AD, bądź wyznaczoną w tym celu osobę, która na mocy pełnomocnictwa będzie odpowiedzialna za realizację tego działania,
5) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych wg wzoru stanowiącego załącznik nr 1.6,
6) przeprowadza wewnętrzne audyty (sprawdzenia) przestrzegania przepisów Ustawy i Rozporządzenia oraz przestrzegania zasad wynikających z Polityki i Instrukcji,
7) opracowują sprawozdania (1 w roku) z działalności dla AD oraz dla GIODO na każde żądanie stanowiące załącznik nr 1.18,
8) nadzoruje udostępnianie danych osobowych,
9) nadzoruje powierzenie przetwarzania danych osobowych,
10) nadzoruje spełnianie wymagań Ustawy i Rozporządzenia przez procesora,
11) opracowuje nowe i aktualizuje istniejące wnioski rejestracyjne zgłaszane do GIODO oraz prowadzą wewnętrzny jawny rejestr zbiorów danych osobowych wg wzoru stanowiącego załącznik nr 1.19,
12) prowadzi korespondencję z GIODO,
13) przygotowuje wzory dokumentów dotyczące ochrony danych osobowych,
14) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, w tym Politykę i Instrukcję,
15) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych u AD,
16) wspólnie z AD podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych ze szczególnym uwzględnieniem systemu informatycznego,
17) przygotowuje regulamin ochrony danych osobowych, dostosowany do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,
18) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych lub współpracują w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym,
19) współpracuje z ASI.

Załącznik nr 1.2	Wzór oświadczenia Administratora Bezpieczeństwa Informacji	Wersja 1

Oświadczenie Administratora Bezpieczeństwa Informacji o spełnieniu warunków określonych w Ustawie o ochronie danych osobowych w art. 36a ust. 5.

Ja, niżej podpisany/podpisana ....., legitymujący/legitymująca się dowodem osobistym ..... niniejszym oświadczam, że spełniam warunki określone w Ustawie o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 poz.922 z późn. zm.) w art. 36a ust. 5 tj.:

a. mam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych,
b. posiadam odpowiednią wiedzę w zakresie ochrony danych osobowych,
c. nie byłem/byłam karany/karana za umyślne przestępstwo,
d. będę podlegał/podlegała bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

_____

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 1.3	Wzór powołania Administratora Systemu Informatycznego	Wersja 1

Działając na podstawie art. 36a ust. 1 i art. 38 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późn. zm.) z dniem .....

zarządzam, co następuje:

§ 1. Powołuję Pana/Panią* ..... na Administratora Systemu Informatycznego (ASI) w Urzędzie Gminy w Olszówce.

§ 2. Ustalam zakres obowiązków Administratora Systemu Informatycznego w Urzędzie Gminy w Olszówce określony w załączniku Nr 1 do niniejszego powołania.

§ 3. Zarządzenie podlega ogłoszeniu i wchodzi w życie z dniem podjęcia.

Wójt

.....

*niepotrzebne skreślić

Załącznik nr .....
do zarządzenia nr
..... z dnia .....

Wójta Urzędu Gminy w Olszówce

ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych w tym zwłaszcza:

1. wdraża zasady ochrony danych osobowych określone w Polityce oraz Instrukcji i dokumentach z nimi związanych,
2. zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora,
3. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
4. przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w Instrukcji,
5. nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
6. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
7. wyrejestrowuje użytkowników na polecenie AD lub ABI,
8. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje AD o naruszeniu oraz współdziała z nimi przy usuwaniu skutków naruszenia,
9. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10. wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe,
11. wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
12. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

Załącznik nr 1.4	Wzór upoważnienia do przetwarzania danych osobowych	Wersja 2

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* NR .....
do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2016 r., poz. 922) z dniem ..... upoważniam/anuluję* upoważnienie Panią/Pana* ....., zatrudnioną/ego* w Urzędzie Gminy w Olszówce na stanowisku ....., do przetwarzania danych osobowych zgodnie z załącznikiem A.

Zobowiązuję Panią/Pana* do:

a) zachowania w tajemnicy danych osobowych przetwarzanych u Administratora Danych oraz sposobów ich zabezpieczenia,
b) nieujawniania danych osobowych podmiotom nieuprawnionym w jakiejkolwiek formie bez zgody Administratora Danych,
c) przestrzegania Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
d) korzystania z oprogramowania Administratora Danych wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
e) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych,
f) niepodejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
g) wnoszenia, wynoszenia i użytkowania komputerów przenośnych, bądź innych nośników danych będących własnością Administratora Danych, wyłącznie za wiedzą i zgodą Administratora Danych lub Administratora Systemu Informatycznego,
h) należytej dbałości o sprzęt i oprogramowanie,
i) należytego zabezpieczania dokumentów papierowych przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem,
j) nie wykonywania kopii baz danych zawierających dane osobowe oraz inne informacje objęte tajemnicą przedsiębiorstwa,
k) należytego zabezpieczania pomieszczeń, w których przetwarza się dane osobowe.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w ww. Ustawie oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą do rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.
Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia również po odwołaniu upoważnienia, a także ustaniu stosunku pracy/rozwiązaniu umowy/zakończeniu realizacji zadań związanych z przetwarzaniem danych osobowych.

niejsze upoważnienie obowiązuje od daty wystawienia i traci moc najpóźniej z dniem ustania stosunku pracy lub z dniem zwolnienia wiadczenia pracy, jeżeli zostało zastosowane przed datą ustania stosunku pracy.
Upoważnienie może zostać również odwołane w każdym czasie w drodze oświadczenia złożonego przez Urząd Gminy w Olszówce.

.....
(podpis Administratora Danych)

Oświadczam, iż zostałam zapoznana z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych „Polityką Bezpieczeństwa Danych Osobowych" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

.....
(podpis osoby upoważnionej)

*niepotrzebne skreślić

Załącznik nr 1.4.	Wzór załącznika do upoważnienia do przetwarzania danych osobowych	Upoważnienie nr .....

ZAŁĄCZNIK DO UPOWAŻNIENIA Nr .....

Imię i nazwisko: .....

Lp.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Forma przetwarzania	Nazwa systemu informatycznego	Zakres czynności
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Załącznik nr 1.5	Oświadczenie o zachowaniu poufności	Wersja 1

Oświadczam, iż w dniu ..... zostałam/em* zapoznana/y* z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późn. zm.), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych „Polityką Bezpieczeństwa Danych Osobowych" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

1. Jednocześnie oświadczam, iż jestem zatrudniona/y* w Urzędzie Gminy w Olszówce będącym Administratorem Danych w rozumieniu art. 7 pkt 4 ww. Ustawy na podstawie umowy o pracę/umowy cywilno-prawnej*.

2. Zobowiązuję się do:
   a) zachowania w tajemnicy danych osobowych przetwarzanych u Administratora Danych oraz sposobów ich zabezpieczenia,
   b) nieujawniania danych osobowych podmiotom nieuprawnionym w jakiejkolwiek formie bez zgody Administratora Danych,
   c) przestrzegania Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   d) należytego zabezpieczania pomieszczeń, w których przetwarza się dane osobowe.

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą zastosowania kary porządkowej albo wypowiedzenie przez Pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy, bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 2016 r. poz. 1666 z późn. zm.). Naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność karną na zasadach określonych w Ustawie o ochronie danych osobowych lub przepisach odrębnych**

Naruszenie obowiązków wskazanych powyżej, może stanowić przyczynę uzasadniającą rozwiązanie umowy/zakończenie współpracy z Administratorem Danych. Naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność karną na zasadach określonych w Ustawie o ochronie danych osobowych lub przepisach odrębnych, jak również odpowiedzialność odszkodowawczą.***

.....

.....

(imię i nazwisko, podpis)

* niepotrzebne skreślić

** dotyczy osób zatrudnionych na podstawie umowy o pracę

*** dotyczy przedsiębiorców, stażystów, praktykantów, wolontariuszy itp.

		Ewidencja osób upoważnionych do przetwarzania danych osobowych		Stan na dzień	
L.p.	Nazwisko i imię osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator
	ROK 2016				
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					

29.					
30.					
31.					
32.					
33.					
34.					

Załącznik nr 1.7	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	Wersja 2

Budynek/ Kondygnacja	Numer pokoju	Opis

Załącznik nr 1.8	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Wersja 2

L.P.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Forma przetwarzania zbioru[1]	Zabezpieczenia informatyczne[2]	Zabezpieczenia fizyczne[3]	Zabezpieczenia organizacyjne[4]
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						

Legenda:

(1) papierowa, elektroniczna (nazwa systemu informatycznego)

(2) np.: (UPS) – zasilacz awaryjny, (LH) – indywidulny login i hasło do systemu operacyjnego (LHA) – indywidualne hasło dostępu do aplikacji, (SD) – szyfrowanie dysku twardego, (S) – szyfrowanie transmisji danych, (F) – wydzielona fizycznie sieć, (AV) – program antywirusowy, (FW) – zapora systemu (firewall)

(3) np.: (K) – kraty w oknach, (A) – alarm, (W) – wzmocnienie drzwi, (D) – dozór całodobowy, (KD) – kontrola dostępu, (KL) – klimatyzacja, (SP) – sygnalizacja PPOŻ, (ZP) – zamki patentowe, (SF) – Sejf, (SK) – szafa zamykana na klucz, (M) – monitoring, (G) – gaśnica, (N) – niszczarka

(4) np.: (UP) – upoważnienie do przetwarzania danych osobowych, (OP) – oświadczenie o zachowaniu poufności, (SZK) – szkolenie lub zapoznanie osoby z dokumentacją i przepisami

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

Lp.	Nazwa zbioru danych osobowych	Nazwa podzbioru zbioru danych osobowych	Forma przetwarzania zbioru[1]	Zabezpieczenia informatyczne[2]	Zabezpieczenia fizyczne[3]	Zabezpieczenia organizacyjne[4]
1.	**Zbiór danych osobowych pracowników**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - Płatnik	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

		Wykaz oświadczeń majątkowych pracowników	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
		Ewidencja osób posiadających podpis elektroniczny	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
		Ewidencja spraw socjalno-bytowych załatwianych w ramach ZFŚS	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
2.	**Dokumentacja BHP**	**Rejestr szkoleń**	Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
3.	**Akta osobowe kierowników jednostek organizacyjnych**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

			Papierowa Elektroniczna - Płatnik	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Wykaz oświadczeń majątkowych kierowników jednostek organizacyjnych	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
4.	**Zbiór danych osobowych Sołtysów**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
5.	**Zbiór danych osobowych Radnych i Przewodniczących Rad Sołeckich**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Wykaz oświadczeń majątkowych Radnych	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
6.	**Zbiór umów**	**Zbiór umów cywilno-prawnych z pracownikami**	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

			Papierowa Elektroniczna - Płatnik	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór umów cywilno-prawnych z nauczycielami	Papierowa			
			Papierowa Elektroniczna – RADIX (KADRY+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - Płatnik	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (PŁACE+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór umów dzierżaw	Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
		Rejestr umów do 30 tysięcy euro	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
7.	**Wykaz kandydatów do pracy**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
8.	**Rejestr skarg i wniosków**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
9.	**Rejestr korespondencji przychodzącej i wychodzącej**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
10.	**Ewidencja testamentów**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

11.	**Opłata skarbowa za poświadczanie dokumentów za zgodność z oryginałem**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
12.	**Opłata skarbowa za poświadczanie własnoręczności podpisów**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
13.	**Ewidencja ludności**	**Rejestr dowodów osobistych**	Papierowa Elektroniczna – Źródło-RDO	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - Źródło - PESEL	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
14.	**Rejestr wyborców**		Papierowa Elektroniczna – RADIX (WYB+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
15.	**Ewidencja wojskowa**	**Lista stawiennictwa osób do kwalifikacji wojskowej**	Papierowa Elektroniczna – RADIX	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

			(ELUD+)			
		Rejestr osób objętych rejestracją WKU	Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Wykaz osób o nieuregulowanym stosunku do obowiązku służby wojskowej	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
16.	**Akta Urzędu Stanu Cywilnego**		Papierowa Elektroniczna – RADIX (USC+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
17.	**Rejestr uznań i odmów**		Papierowa Elektroniczna – Źródło - BBUSC	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
18.	**Rejestr zapewnień i zaświadczeń wydawanych w trybie art.4 kodeksu rodzinnego i opiekuńczego**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
19.	**Ewidencja osób zobowiązanych do wykonywania świadczeń osobistych**	**Rejestr świadczeń rzeczowych i osobistych na potrzeby obronności**	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa		M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

20.	**Zbiór danych osobowych ubezwłasnowolnionych i skazanych/ aresztowanych**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
		Ewidencja osób skazanych, które wykonują nieodpłatną pracę na rzecz gminy	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
21.	**Ewidencja działalności gospodarczej**		Papierowa Elektroniczna – Centralna Ewidencja i Informacja o Działalności Gospodarczej	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
22.	**Zbiór zezwoleń na sprzedaż alkoholu**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
23.	**Zbiór danych osobowych osób objętych profilaktyką alkoholową i przeciwdziałaniu narkomanii**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
24.	**Dane osobowe płatników podatku**	**Zbiór płatników podatku rolnego**	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (POGRUN+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - dokument	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.

			tekstowy			
			Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór płatników podatku leśnego	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (POGRUN+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór płatników podatku od nieruchomości	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (POGRUN+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

			Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Deklaracje i informacje podatkowe w sprawie podatku rolnego, leśnego i od nieruchomości	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
		Zbiór płatników podatku od środków transportowych	Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór zaświadczeń o niezaleganiu w podatkach lub stwierdzające stan zaległości	Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Rejestr nadpłat i zaległości podatkowych	Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Windykacja podatków i opłat lokalnych	Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Zbiór zaświadczeń o figurowaniu w ewidencji podatkowej Gminy Olszówka	Papierowa Elektroniczna – RADIX (POGRUN+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
25.	**Rejestr wymiarowy podatków**		Papierowa Elektroniczna – RADIX	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

			(POGRUN+)			
26.	**Zbiór osób dotkniętych klęską żywiołową**		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
27.	**Rejestr zezwoleń na uprawę maku i konopi włóknistych**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
28.	**Dokumentacja finansowo – księgowa**	**Rejestr faktur**	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
29.	**Zbiór danych kontrahentów**	**Kartoteka kontrahentów**	Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
30.	**Dane osobowe osób ubezpieczonych**	**Ubezpieczenie grupowe**	Papierowa Elektroniczna – eRU	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Wykaz wydanych legitymacji ubezpieczeniowych	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
		Zbiór kart ubezpieczonych	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
31.	**Wykaz wydanych zaświadczeń o dochodach nauczyciela**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
32.	**Wykaz pracodawców ubiegających się o refundację kosztów kształcenia młodocianych pracowników**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
33.	**Rejestr aktów nadania stopni awansu zawodowego nauczycieli mianowanych**		Papierowa Elektroniczna – SIO	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

34.	Pomoc materialna dla uczniów		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – SPUTNIK	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Elektroniczna – SIO	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
		Wykaz uczniów korzystających z pomocy materialnej w postaci wyprawki szkolnej	Papierowa		M, K, SK, G, N.	UP, OP, SZK.
35.	Świadczenia opieki zdrowotnej finansowane ze środków publicznych		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
36.	Rejestr płatników czynszów za lokale mieszkalne		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
37.	Rejestr wniosków o wycinkę drzew i krzewów		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
38.	Rejestr decyzji zatwierdzających podział działek		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
39.	Rejestr wniosków dzierżawy i sprzedaży gruntów		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
40.	Rejestr spraw dotyczących czystości i porządku		Papierowa Elektroniczna – RADIX (GOK+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
41.	Rejestr działalności		Papierowa		M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

	regulowanej w zakresie odbierania odpadów komunalnych		Papierowa Elektroniczna – RADIX (GOK+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
42.	**Rejestr zezwoleń w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych**		Papierowa Elektroniczna – RADIX (GOK+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
43.	**Rejestr deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (GOK+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
44.	**Rejestr decyzji środowiskowych**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
45.	**Rejestr sprzedaży nieruchomości**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
46.	**Rejestr nabycia nieruchomości**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
47.	**Rejestr płatników czynszów za lokale użytkowe**		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
48.	**Rejestr wyrobów zawierających azbest**		Elektroniczna – panel administracyjny strony www.bazaazbestowa.pl	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
49.	**Rejestr numeracji porządkowej**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.

			Papierowa Elektroniczna – internetowy manager punktów adresowych – Olszówka – geodane przestrzenne	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
50.	**Rejestr wydanych decyzji o ustaleniu warunków zabudowy i zagospodarowania terenu**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
51.	**Rejestr celu publicznego**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
52.	**Ewidencja zamówień publicznych**		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
		Ewidencja zamówień publicznych do 30 tysięcy euro	Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
53.	**Ewidencja właścicieli, którzy przystąpią do budowy przydomowych oczyszczalni ścieków**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
54.	**Ewidencja właścicieli przykanalików**		Papierowa Elektroniczna – arkusz kalkulacyjny	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
55.	**Rejestr zaświadczeń o przeznaczeniu gruntów**		Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
56.	**Monitoring wizyjny**		Elektroniczna	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stan na dzień 01.03.2017 r.

			Papierowa		M, K, SK, G, N.	UP, OP, SZK.
57.	**Zbiór płatników opłaty za gospodarowanie odpadami komunalnymi**		Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa		M, K, SK, G, N.	UP, OP, SZK.
58.	**Zbiór odbiorców usług zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków**		Papierowa Elektroniczna – RADIX (WIP+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (EKO+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – RADIX (ELUD+)	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna – dokument tekstowy	UPS, AV, FW, LH.	M, K, SK, G, N.	UP, OP, SZK.
			Papierowa Elektroniczna - WODNIK	UPS, AV, FW, LH, LHA.	M, K, SK, G, N.	UP, OP, SZK.
59.	**Zbiór umów odbiorców zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków**		Papierowa		M, K, SK, G, N.	UP, OP, SZK.

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	**Stan na dzień 01.03.2017 r.**

Legenda:

(1) papierowa, elektroniczna (nazwa systemu informatycznego)

(2) np.: (UPS) – zasilacz awaryjny, (LH) – indywidulny login i hasło do systemu operacyjnego (LHA) – indywidualne hasło dostępu do aplikacji, (SD) – szyfrowanie dysku twardego, (S) – szyfrowanie transmisji danych, (F) – wydzielona fizycznie sieć, (AV) – program antywirusowy, (FW) – zapora systemu (firewall)

(3) np.: (K) – kraty w oknach, (A) – alarm, (W) – wzmocnienie drzwi, (D) – dozór całodobowy, (KD) – kontrola dostępu, (KL) – klimatyzacja, (SP) – sygnalizacja PPOŻ, (ZP) – zamki patentowe, (SF) – Sejf, (SK) – szafa zamykana na klucz, (M) – monitoring, (G) – gaśnica, (N) – niszczarka

(4) np.: (UP) – upoważnienie do przetwarzania danych osobowych, (OP) – oświadczenie o zachowaniu poufności, (SZK) – szkolenie lub zapoznanie osoby z dokumentacją i przepisami

Załącznik nr 1.9	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Wersja 2

Lp.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Pola informacyjne
1.			•
2.			•
3.			•
4.			•
5.			•
6.			•
7.			•
8.			•
9.			•
10.			•
11.			•
12.			•
13.			•
14.			•
15.			•
16.			•
17.			•
18.			•
19.			•
20.			•

	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Stan na dzień 01.03.2017 r.

Lp.	Nazwa zbioru danych osobowych	Nazwa podzbioru zbioru danych osobowych	Pola informacyjne
1.	**Zbiór danych osobowych pracowników**		• imię (imiona) i nazwisko; • miejsce urodzenia; • nazwisko rodowe • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • numer telefonu; • adres e-mail; • wykształcenie; • seria i numer dokumentu tożsamości; • numer telefonu; • miejsce pracy; • zawód; • zwolnienia lekarskie; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia; • stan cywilny; • podleganie służbie wojskowej; • posiadanie gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej; • stan rodziny (imię (imiona) i nazwisko, adres zamieszkania lub pobytu, data urodzenia); • dane osoby upoważnionej (imię (imiona) i nazwisko, adres zamieszkania lub pobytu); • stan zdrowia; • orzeczenie o niekaralności; • obywatelstwo; • rok ukończenia szkoły; • przebieg zatrudnienia; • znajomość języków obcych; • stosunek do służby wojskowej – obowiązek obrony, numer specjalności, przynależność do Wojskowej Komendy Uzupełnień, numer książeczki wojskowej; • informacje dot. posiadanego prawa jazdy; • wizerunek.

			• imię (imiona) i nazwisko; • miejsce urodzenia; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • numer rachunku bankowego; • seria i numer dokumentu tożsamości; • miejsce pracy; • zawód; • informacje dot. zwolnień lekarskich; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia; • informacje dot. posiadanego gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej.
			• imię (imiona) i nazwisko; • miejsce urodzenia; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • numer rachunku bankowego; • seria i numer dokumentu tożsamości; • miejsce pracy; • zawód; • informacje dot. zwolnień lekarskich; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia; • informacje dot. posiadanego gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej.
			• imię (imiona) i nazwisko; • adres zamieszkania; • adres korespondencyjny; • numer PESEL;

			• płeć; • data urodzenia; • obywatelstwo; • nazwisko rodowe; • data zatrudnienia; • dane członków rodziny (imię (imiona) i nazwisko, adres zamieszkania lub pobytu, numer PESEL, data urodzenia, stopień pokrewieństwa); • data zgłoszenia do ZUS; • dane płatnika składek (nazwa i siedziba, numer NIP, numer REGON).
		Wykaz oświadczeń majątkowych pracowników	• imię (imiona) i nazwisko; • nazwisko rodowe; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • miejsce pracy; • stanowisko; • funkcja; • zasoby pieniężne; • posiadane nieruchomości; • posiadane udziały; • posiadane akcje; • nabyte mienie od Skarbu Państwa; • informacje dot. prowadzenia działalności gospodarczej; • członkostwo w spółkach handlowych; w spółdzielniach, w fundacjach; • osiągane dochody; • składniki mienia ruchomego; • zobowiązania pieniężne; • miejsce położenia nieruchomości.
		Ewidencja osób posiadających podpis elektroniczny	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • numer PESEL; • rodzaj dokumentu tożsamości; • seria i numer dokumentu tożsamości; • adres korespondencyjny; • dane reprezentowanego podmiotu (nazwa, siedziba, numer NIP, numer REGON, numer telefonu, adres e-mail); • numer karty.

		Ewidencja spraw socjalno-bytowych załatwianych w ramach ZFŚS	• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • wysokość średniego miesięcznego dochodu na osobę w rodzinie.
2.	**Dokumentacja BHP**	**Rejestr szkoleń**	• imię (imiona) i nazwisko; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • miejsce pracy; • zawód; • data zatrudnienia.
3.	**Akta osobowe kierowników jednostek organizacyjnych**		• imię (imiona) i nazwisko; • miejsce urodzenia; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • seria i numer dokumentu tożsamości; • numer telefonu; • miejsce pracy; • zawód; • informacje dot. zwolnień lekarskich; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia; • stan cywilny; • podleganie służbie wojskowej; • informacje dot. posiadanego gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej; • stan rodziny (imię (imiona) i nazwisko, adres zamieszkania lub pobytu, data urodzenia członków rodziny); • dane osoby upoważnionej (imię (imiona) i nazwisko, adres zamieszkania lub pobytu); • stan zdrowia; • orzeczenie o niekaralności; • obywatelstwo;

			• rok ukończenia szkoły; • przebieg zatrudnienia; • znajomość języków obcych; • stosunek do służby wojskowej – obowiązek obrony, numer specjalności, przynależność do Wojskowej Komendy Uzupełnień, numer książeczki wojskowej; • prawo jazdy.
			• imię (imiona) i nazwisko; • miejsce urodzenia; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • numer rachunku bankowego; • seria i numer dokumentu tożsamości; • miejsce pracy; • zawód; • informacje dot. zwolnień lekarskich; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia; • informacje dot. posiadanego gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej.
			• imię (imiona) i nazwisko; • miejsce urodzenia; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • numer rachunku bankowego; • wykształcenie; • seria i numer dokumentu tożsamości; • miejsce pracy; • zawód; • informacje dot. zwolnień lekarskich; • nazwa i siedziba urzędu skarbowego; • wysokość wynagrodzenia;

			• informacje dot. posiadanego gospodarstwa rolnego; • warunki zatrudnienia; • historia przebiegu pracy zawodowej.
			• imię (imiona) i nazwisko; • nazwisko rodowe; • adres zamieszkania; • adres korespondencyjny; • numer PESEL; • płeć; • data urodzenia; • obywatelstwo; • data zatrudnienia; • dane członków rodziny (imię (imiona) i nazwisko, adres zamieszkania lub pobytu, numer PESEL, data urodzenia, stopień pokrewieństwa); • data zgłoszenia do ZUS; • dane płatnika składek (nazwa i siedziba, numer NIP, numer REGON).
		Wykaz oświadczeń majątkowych kierowników jednostek organizacyjnych	• imię (imiona) i nazwisko; • nazwisko rodowe; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • miejsce pracy; • stanowisko; • funkcja; • zasoby pieniężne; • posiadane nieruchomości; • posiadane udziały; • posiadane akcje; • nabyte mienie od Skarbu Państwa; • prowadzenie działalności gospodarczej; • członkostwo w spółkach handlowych, w spółdzielniach, w fundacjach; • osiągane dochody; • składniki mienia ruchomego; • zobowiązania pieniężne; • miejsce położenia nieruchomości.
4.	**Zbiór danych osobowych Sołtysów**		• Imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL;

			• numer telefonu; • adres e-mail; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL; • numer telefonu; • adres e-mail; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL; • numer telefonu; • seria i numer dokumentu tożsamości.
5.	**Zbiór danych osobowych Radnych i Przewodniczących Rad Sołeckich**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL; • numer telefonu; • adres e-mail; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL; • numer telefonu; • adres e-mail; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • stanowisko; • miejsce pracy; • numer PESEL; • numer telefonu; • seria i numer dokumentu tożsamości.
		Wykaz oświadczeń majątkowych Radnych	• imię (imiona) i nazwisko; • nazwisko rodowe; • data urodzenia;

			• miejsce urodzenia; • adres zamieszkania lub pobytu; • miejsce pracy; • stanowisko; • funkcja; • zasoby pieniężne; • posiadane nieruchomości; • posiadane udziały; • posiadane akcje; • nabyte mienie od Skarbu Państwa; • prowadzenie działalności gospodarczej; • członkostwo w spółkach handlowych; • osiągane dochody; • składniki mienia ruchomego; • zobowiązania pieniężne; • miejsce położenia nieruchomości.
6.	**Zbiór umów**	**Zbiór umów cywilno-prawnych z pracownikami**	• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • seria i numer dokumentu tożsamości; • numer telefonu; • rok ukończenia szkoły.
			• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • płeć; • data urodzenia; • obywatelstwo; • nazwisko rodowe; • data zatrudnienia;

			• dane członków rodziny (imię (imiona) i nazwisko, adres zamieszkania, numer PESEL, data urodzenia, stopień pokrewieństwa); • data zgłoszenia do ZUS; • dane płatnika składek (nazwa i siedziba, numer NIP, numer REGON).
			• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • numer rachunku bankowego; • seria i numer dokumentu tożsamości.
		Zbiór umów cywilno-prawnych z nauczycielami	• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • wykształcenie; • seria i numer dokumentu tożsamości; • numer telefonu; • rok ukończenia szkoły.
			• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • seria i numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • płeć; • data urodzenia; • obywatelstwo;

			• nazwisko rodowe; • data zatrudnienia; • dane członków rodziny (imię (imiona) i nazwisko, adres zamieszkania, numer PESEL, data urodzenia, stopień pokrewieństwa); • data zgłoszenia do ZUS; • dane płatnika składek (nazwa i siedziba, numer NIP, numer REGON).
			• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • adres zamieszkania lub pobytu; • adres zameldowania; • numer PESEL; • numer NIP; • numer rachunku bankowego; • seria i numer dokumentu tożsamości.
		Zbiór umów dzierżaw	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • seria i numer dokumentu tożsamości; • stan majątkowy; • dane współmałżonka (imię (imiona) i nazwisko, data i miejsce urodzenia, numer PESEL, adres zamieszkania lub pobytu);
		Rejestr umów do 30 tysięcy euro	• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer NIP; • przedmiot umowy; • czas trwania umowy (od dnia .... do dnia ...); • wartość umowy.
7.	**Wykaz kandydatów do pracy**		• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • obywatelstwo; • miejsce zamieszkania lub pobytu; • adres korespondencyjny; • wykształcenie;

			• przebieg zatrudnienia; • informacja o zdolności do czynności prawnych, o korzystaniu z pełni praw publicznych, czy kandydat był/nie był skazany wyrokiem sądowym, bądź za umyślne przestępstwa skarbowe.
8.	**Rejestr skarg i wniosków**		• imię (imiona) i nazwisko petenta (nazwa instytucji); • adres petenta (instytucji); • przedmiot odwołania skargi i zażalenia; • inne dane (daty wpływu, termin, sposób załatwienia sprawy).
9.	**Rejestr korespondencji przychodzącej i wychodzącej**		• imię (imiona) i nazwisko; • adres zamieszkania/pobytu/ korespondencyjny; • treść otrzymanej korespondencji.
10.	**Ewidencja testamentów**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • data urodzenia; • numer PESEL; • stan majątkowy.
11.	**Opłata skarbowa za poświadczanie dokumentów za zgodność z oryginałem**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer PESEL.
12.	**Opłata skarbowa za poświadczanie własnoręczności podpisów**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer PESEL.
13.	**Ewidencja ludności**	**Rejestr dowodów osobistych**	• imię (imiona) i nazwisko oraz podpis posiadacza dokumentu; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • nazwisko rodowe matki; • kolor oczu; • wzrost; • adres zameldowania; • numer PESEL; • seria i numer dokumentu tożsamości; • płeć; • stan cywilny; • wizerunek twarzy posiadacza; • data wydania dokumentu; • termin ważności dokumentu.

			• imię (imiona) i nazwisko; • nazwisko rodowe; • poprzednie nazwiska; • data, miejsce i numer aktu urodzenia; • imiona rodziców; • nazwiska rodowe rodziców; • numer PESEL; • adres zamieszkania lub pobytu; • adresy wcześniejszego zamieszkiwania; • seria i numer dokumentu tożsamości; • data i numer aktu zgonu; • stan cywilny; • data zawarcia związku małżeńskiego i numer aktu małżeństwa; • dane współmałżonka (imię (imiona) i nazwisko, nazwisko rodowe, numer PESEL); • obywatelstwo; • wykształcenie; • uprawnienia do wyborów; • numer książeczki wojskowej.
			• imię (imiona) i nazwisko; • nazwisko rodowe; • poprzednie nazwiska; • data, miejsce i numer aktu urodzenia; • imiona rodziców; • nazwiska rodowe rodziców; • numer PESEL; • adres zamieszkania lub pobytu; • seria i numer dokumentu tożsamości; • data i numer aktu zgonu; • stan cywilny; • data zawarcia związku małżeńskiego i numer aktu małżeństwa; • imię (imiona) i nazwisko małżonka; • nazwisko rodowe małżonka; • numer PESEL małżonka; • obywatelstwo.
			• imię (imiona) i nazwisko; • nazwisko rodowe; • poprzednie nazwiska; • data, miejsce i numer aktu urodzenia;

			• imiona rodziców; • nazwiska rodowe rodziców; • numer PESEL; • adres zamieszkania lub pobytu; • seria i numer dokumentu tożsamości; • imię (imiona) i nazwisko małżonka; • nazwisko rodowe małżonka; • numer PESEL małżonka; • obywatelstwo.
14.	**Rejestr wyborców**		• imię (imiona) i nazwisko; • adres zameldowania; • imię ojca; • numer PESEL; • data urodzenia.
15.	**Ewidencja wojskowa**	**Lista stawiennictwa osób do kwalifikacji wojskowej**	• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • miejsce pobytu stałego lub czasowego trwającego powyżej trzech miesięcy; • numer PESEL; • data ujęcia w rejestrze; • data stawiennictwa do kwalifikacji wojskowej i WKU; • seria i numer książeczki wojskowej; • kategoria zdolności do czynnej służby wojskowej.
		Rejestr osób objętych rejestracją WKU	• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • miejsce pobytu stałego lub czasowego trwającego powyżej trzech miesięcy; • numer PESEL; • data ujęcia w rejestrze; • data stawiennictwa do kwalifikacji wojskowej i WKU; • seria i numer książeczki wojskowej; • kategoria zdolności do czynnej służby wojskowej.
		Wykaz osób o nieuregulowanym stosunku do obowiązku służby wojskowej	• pozycja z rejestru; • pozycja z listy stawiennictwa do kwalifikacji wojskowej; • imię (imiona) i nazwisko;

			• imię ojca; • wyznaczony termin stawiennictwa; • przyczyna niezgłoszenia się; • faktyczna data stawiennictwa; • miejsce zgłoszenia się; • miejsce pobytu stałego lub czasowego trwającego powyżej trzech miesięcy; • seria i numer książeczki wojskowej oraz kategoria wojskowa; • zastosowane sankcje karne; • podstawa skreślenia.
16.	**Akta Urzędu Stanu Cywilnego**		• imię (imiona) i nazwisko; • nazwisko rodowe; • imiona i nazwiska rodowe rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • stan cywilny; • data zawarcia związku małżeńskiego; • miejsce zawarcia związku małżeńskiego; • data zgonu; • miejsce zgonu; • świadkowie; • numer PESEL; • seria i numer dokumentu tożsamości; • numer telefonu; • numer aktu urodzenia; • numer aktu wcześniejszego małżeństwa; • dane sądu udzielającego rozwodu; • sygnatura wyroku; • dane z aktu zgonu małżonka; • imię (imiona), nazwisko i nazwisko rodowe osoby, z którą planowany jest ślub; • oświadczenie o nie pozostawaniu w innym związku małżeńskim; • oświadczenie o braku pokrewieństwa lub powinowactwa w linii prostej, braku stosunku przysposobienia, braku pokrewieństwa typu rodzeństwo rodzone lub przyrodnie; • oświadczenie dotyczące zmiany nazwiska po ślubie;

			• oświadczenie o nadaniu nazwiska dzieciom po urodzeniu.
17.	**Rejestr uznań i odmów**		• Imię (imiona) i nazwisko rodziców; • nazwisko rodowe matki; • numer PESEL rodziców; • numer PESEL dziecka; • imię i nazwisko dziecka; • data urodzenia dziecka; • adres zamieszkania lub pobytu; • adres korespondencyjny; • obywatelstwo rodziców; • obywatelstwo dziecka.
18.	**Rejestr zapewnień i zaświadczeń wydawanych w trybie art.4 kodeksu rodzinnego i opiekuńczego**		• imię (imiona) i nazwisko osoby składającej zapewnienie; • adres zamieszkania lub pobytu osoby składającej zapewnienie; • data złożenia zapewnień; • data zawarcia zawiązku małżeńskiego; • data złożenia podania o wystawienie zaświadczenia; • informacje dot. wystawionego zaświadczenia (data wydania, numer, termin ważności); • zawiadomienie o zawarciu związku małżeńskiego (data wpływu/wysłania, nazwa USC, numer aktu); • związek małżeński w formie wyznaniowej zawarto na terenie gminy (data otrzymania zaświadczenia, data sporządzenia aktu).
19.	**Ewidencja osób zobowiązanych do wykonywania świadczeń osobistych**	**Rejestr świadczeń rzeczowych i osobistych na potrzeby obronności**	• imię (imiona) i nazwisko; • imię ojca; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer telefonu.
			• imię (imiona) i nazwisko; • imię ojca; • adres zamieszkania lub pobytu; • miejsce pracy; • miejsce świadczenia; • rodzaj przedmiotu świadczenia; • nazwa podmiotu; • adres podmiotu; • numer NIP; • numer REGON.
20.	**Zbiór danych osobowych osób**		• imię (imiona) i nazwisko; • data urodzenia;

	ubezwłasnowolnionych i skazanych/ aresztowanych		• miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • imiona rodziców; • powód skazania; • wyznaczona kara; • podstawa prawna kary; • podmiot nakładający karę; • sygnatura akt sprawy; • imię i nazwisko sędziego; • adres sądu; • określenie sądu (wydział).
		Ewidencja osób skazanych, które wykonują nieodpłatną pracę na rzecz gminy	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • sygnatura akt sprawy; • numer wyroku sądowego); • wysokość zasądzonego wyroku.
21.	**Ewidencja działalności gospodarczej**		• seria i numer dokumentu tożsamości; • numer PESEL; • numer NIP; • numer REGON; • imię (imiona) i nazwisko; • nazwisko rodowe; • imię (imiona) rodziców; • miejsce urodzenia; • data urodzenia; • obywatelstwo; • adres zamieszkania lub pobytu; • adres zameldowania; • numer telefonu; • płeć; • nazwa działalności gospodarczej; • data rozpoczęcia działalności gospodarczej; • rodzaj działalności gospodarczej; • adres głównego miejsca wykonywania działalności; • adres korespondencyjny; • numer faksu; • adres e-mail.
22.	**Zbiór zezwoleń na sprzedaż alkoholu**		• imię (imiona) i nazwisko przedsiębiorcy; • siedziba przedsiębiorstwa; • numer NIP; • numer telefonu; • adres zamieszkania lub pobytu;

			• adres punktu składowania alkoholi; • imiona i nazwiska pełnomocników podmiotu; • adres punktu sprzedaży.
23.	**Zbiór danych osobowych osób objętych profilaktyką alkoholową i przeciwdziałaniu narkomanii**		• imię (imiona) i nazwisko; • imiona rodziców; • numer PESEL; • adres zamieszkania lub pobytu; • adres zameldowania; • data urodzenia.
24.	**Dane osobowe płatników podatków**	**Zbiór płatników podatku rolnego**	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny;

			• numer PESEL; • numer dokumentu tożsamości.
		Zbiór płatników podatku leśnego	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer dokumentu tożsamości.
		Zbiór płatników podatku od nieruchomości	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny;

			• numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer dokumentu tożsamości.
		Deklaracje i informacje podatkowe w sprawie podatku rolnego, leśnego i od nieruchomości	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • stan majątkowy; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer REGON; • numer księgi wieczystej; • miejsce położenia przedmiotów opodatkowania i numery działek.
		Zbiór płatników podatku od środków transportowych	• imię (imiona) i nazwisko właściciela i współwłaściciela;

			• nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • imię i nazwisko podatnika; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer rejestracyjny pojazdu; • data pierwszej rejestracji na terytorium RP; • marka, typ, model pojazdu; • rok produkcji; • dopuszczalna masa całkowita; • masa własna ciągnika siodłowego; • dopuszczalna masa całkowita zespołu pojazdu; • liczba osi; • rodzaj zawieszenia; • opis rodzaju zawieszenia; • liczba miejsc do siedzenia; • wpływ pojazdu silnikowego na środowisko naturalne; • kwota podatku; • kwota podatku zapłaconego; • numer nadwozia; • data nabycia/zbycia/czasowego wyłączenia z ruchu pojazdu; • rok produkcji; • dane dotyczące własności lub współwłasności; • rodzaj środka transportowego; • numer dokumentu tożsamości.
		Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer PESEL; • numer NIP; • numer dokumentu tożsamości; • imiona rodziców; • powierzchnia gruntów; • numer telefonu; • numer rachunku bankowego.
		Zbiór zaświadczeń o niezaleganiu w podatkach lub stwierdzające stan zaległości	• imię (imiona) i nazwisko; • adres zamieszkania; • numer PESEL; • numer NIP; • data urodzenia;

			• kwota zaległości podatkowych; • kwota odsetek za zwłokę.
		Rejestr nadpłat i zaległości podatkowych	• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • kwota zaległości; • kwota odsetek za zwłokę.
		Windykacja podatków i opłat lokalnych	• imię (imiona) i nazwisko; • nazwa przedsiębiorstwa; • adres zamieszkania lub pobytu; • siedziba przedsiębiorstwa; • numer PESEL; • numer REGON; • imiona rodziców; • data urodzenia; • miejsce pracy; • numer rachunku bankowego; • dane finansowe (kwoty zaległości, odsetek, koszty upomnień; • numer NIP.
		Zbiór zaświadczeń o figurowaniu w ewidencji podatkowej Gminy Olszówka	• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • numer PESEL; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • adres zamieszkania lub pobytu; • adres korespondencyjny; • stan majątkowy.
25.	**Rejestr wymiarowy podatków**		• imię (imiona) i nazwisko; • adres zamieszkania; • powierzchnia posiadanego gospodarstwa; • wysokość rat podatku i terminy płatności.
26.	**Zbiór osób dotkniętych klęską żywiołową**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • dane dotyczące produkcji roślinnej i zwierzęcej; • numer telefonu.
27.	**Rejestr zezwoleń na uprawę maku i konopi włóknistych**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer telefonu.
28.	**Dokumentacja finansowo – księgowa**	**Rejestr faktur**	• imię (imiona) i nazwisko; • nazwa przedsiębiorstwa; • adres zamieszkania lub pobytu;

			• siedziba przedsiębiorstwa; • numer NIP; • numer REGON; • numer rachunku bankowego; • numer KRS.
29.	**Zbiór danych kontrahentów**	**Kartoteka kontrahentów**	• imię (imiona i nazwisko); • nazwa przedsiębiorstwa; • adres zamieszkania lub pobytu; • siedziba przedsiębiorstwa; • numer NIP; • numer REGON; • numer rachunku bankowego; • numer KRS.
30.	**Dane osobowe osób ubezpieczonych**	**Ubezpieczenie grupowe**	• imię (imiona) i nazwisko; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • numer PESEL; • seria i numer dokumentu tożsamości; • numer telefonu.
		Wykaz wydanych legitymacji ubezpieczeniowych	• imię (imiona) i nazwisko rodzica; • imię i nazwisko dziecka; • adres zamieszkania.
		Zbiór kart ubezpieczonych	• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • adres korespondencyjny; • stan majątkowy; • kwota wpłaconych składek; • data urodzenia; • imiona rodziców; • miejsce pracy; • okres zatrudnienia; • miejsce nauki; • seria i numer dokumentu tożsamości; • numer PESEL.
31.	**Wykaz wydanych zaświadczeń o dochodach nauczyciela**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer PESEL; • numer NIP.
32.	**Wykaz pracodawców ubiegających się o refundację kosztów kształcenia młodocianych pracowników**		• imię (imiona) i nazwisko; • nazwa przedsiębiorstwa pracodawcy; • numer NIP; • numer REGON; • adres zamieszkania lub pobytu; • siedziba przedsiębiorstwa.
33.	**Rejestr aktów nadania stopni awansu**		• imię (imiona) i nazwisko;

	zawodowego nauczycieli mianowanych		• data urodzenia; • numer PESEL; • stopień awansu zawodowego; • data wydania aktu; • wykształcenie.
34.	**Pomoc materialna dla uczniów**		• imię (imiona) i nazwisko ucznia; • imię (imiona) i nazwisko (nazwiska) rodziców; • adres zamieszkania lub pobytu; • data urodzenia; • miejsce urodzenia; • numer PESEL; • numer telefonu; • klasa i szkoła, do której uczęszcza dziecko; • stopień pokrewieństwa; • miejsce zatrudnienia/nauki; • rodzaj pomocy; • wysokość dochodów.
			• imię (imiona) i nazwisko ucznia; • imię (imiona) i nazwisko (nazwiska) rodziców; • adres zamieszkania lub pobytu; • data urodzenia; • miejsce urodzenia; • numer PESEL; • klasa i szkoła, do której uczęszcza dziecko.
			• imię (imiona) i nazwisko ucznia; • imię (imiona) i nazwisko (nazwiska) rodziców; • adres zamieszkania lub pobytu; • data urodzenia; • miejsce urodzenia; • numer PESEL; • numer telefonu; • klasa i szkoła, do której uczęszcza dziecko; • stopień pokrewieństwa; • miejsce zatrudnienia/nauki; • rodzaj pomocy.
		Wykaz uczniów korzystających z pomocy materialnej w postaci wyprawki szkolnej	• imię (imiona) i nazwisko; • imiona rodziców; • adres zamieszkania lub pobytu; • klasa i szkoła uczęszczania; • numer rachunku bankowego.
35.	**Świadczenia opieki zdrowotnej finansowane ze środków publicznych**		• imię (imiona) i nazwisko.
36.	**Rejestr płatników**		• imię (imiona) i nazwisko;

	czynszów za lokale mieszkalne		• adres zamieszkania lub pobytu; • seria i numer dokumentu tożsamości.
37.	Rejestr wniosków o wycinkę drzew i krzewów		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu.
38.	Rejestr decyzji zatwierdzających podział działek		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu.
39.	Rejestr wniosków dzierżawy i sprzedaży gruntów		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu.
40.	Rejestr spraw dotyczących czystości i porządku		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer PESEL; • numer NIP; • numer REGON.
41.	Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer NIP; • numer REGON.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer NIP; • numer REGON.
42.	Rejestr zezwoleń w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer NIP; • numer REGON.
43.	Rejestr deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • imiona rodziców; • data urodzenia; • numer PESEL; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer REGON.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • imiona rodziców; • data urodzenia; • numer PESEL;

			• nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer REGON.
44.	**Rejestr decyzji środowiskowych**		• nazwa inwestora; • siedziba inwestora; • numer NIP; • nazwa inwestycji.
45.	**Rejestr sprzedaży nieruchomości**		• imię i nazwisko nabywcy nieruchomości; • numer działki; • powierzchnia działki; • numer aktu notarialnego; • data podpisania aktu notarialnego.
46.	**Rejestr nabycia nieruchomości**		• imię i nazwisko zbywającego nieruchomość; • numer działki; • powierzchnia działki; • numer aktu notarialnego; • data podpisania aktu notarialnego.
47.	**Rejestr płatników czynszów za lokale użytkowe**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa.
48.	**Rejestr wyrobów zawierających azbest**		• nazwa wyrobu; • miejsce występowania; • jednostka miary; • ilość; • stopień pilności.
49.	**Rejestr numeracji porządkowej**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer ewidencyjny działki; • miejsce położenia nieruchomości; • miejscowość; • numer posesji; • numer obrębu; • numer geodezyjny działki.
			• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • numer ewidencyjny działki; • miejsce położenia nieruchomości; • miejscowość; • numer posesji; • numer obrębu; • numer geodezyjny działki.
50.	**Rejestr wydanych decyzji o ustaleniu warunków zabudowy i zagospodarowania terenu**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer decyzji;

			• data wniosku/ wydania; • rodzaj inwestycji; • oznaczenie nieruchomości; • streszczenie ustaleń; • numer geodezyjny działki.
51.	**Rejestr celu publicznego**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • numer decyzji; • data wydania wniosku; • rodzaj inwestycji; • oznaczenie nieruchomości; • streszczenie ustaleń; • numer geodezyjny działki.
52.	**Ewidencja zamówień publicznych**		• numer sprawy; • data ogłoszenia; • nazwa zadania; • forma zamówienia; • ilość ofert; • nazwa przedsiębiorstwa; • siedziba przedsiębiorstwa; • data umowy.
		Ewidencja zamówień publicznych do 30 tysięcy euro	• imię (imiona) i nazwisko; • adres zamieszkania; • numer NIP.
53.	**Ewidencja właścicieli, którzy przystąpią do budowy przydomowych oczyszczalni ścieków**		• imię (imiona) i nazwisko; • miejscowość; • numer ewidencyjny działki; • numer posesji; • data akceptacji wniosku; • data oddania do użytku.
54.	**Ewidencja właścicieli przykanalików**		• imię (imiona) i nazwisko; • miejscowość; • numer posesji; • data podłączenia.
55.	**Rejestr zaświadczeń o przeznaczeniu gruntów**		• imię (imiona) i nazwisko; • adres zamieszkania lub pobytu; • przeznaczenie działki; • numery działek.
56.	**Monitoring wizyjny**		• wizerunek.
57.	**Zbiór płatników opłaty za gospodarowanie odpadami komunalnymi**		• imię (imiona) i nazwisko; • adres zamieszkania; • data urodzenia; • numer PESEL; • liczba osób zamieszkujących we wspólnym gospodarstwie domowym;

			• dane finansowe.
			• imię (imiona) i nazwisko; • adres zamieszkania; • data urodzenia; • numer NIP; • numer PESEL; • liczba osób zamieszkujących we wspólnym gospodarstwie domowym; • dane finansowe.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • dane finansowe.
58.	**Zbiór odbiorców usług zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków**		• imię (imiona) i nazwisko; • adres zamieszkania; • data urodzenia; • nazwa podmiotu; • siedziba podmiotu; • numer PESEL; • numer NIP; • numer REGON; • dane finansowe.
			• imię (imiona) i nazwisko; • adres zamieszkania; • data urodzenia; • nazwa podmiotu; • siedziba podmiotu; • numer PESEL; • numer NIP; • numer REGON; • dane finansowe.
			• imię (imiona) i nazwisko; • adres zamieszkania;

			• numer PESEL; • dane finansowe; • wielkość zużycia/dane odczytowe z wodomierzy.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer dokumentu tożsamości.
			• imię (imiona) i nazwisko; • imiona rodziców; • data urodzenia; • miejsce urodzenia; • adres zamieszkania lub pobytu; • adres korespondencyjny; • numer PESEL; • numer NIP; • numer telefonu; • numer dokumentu tożsamości; • stan majątkowy.
			• imię (imiona) i nazwisko; • adres zamieszkania; • wielkość zużycia; • dane finansowe.
59.	**Zbiór umów odbiorców zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków**		• imię (imiona) i nazwisko; • adres zamieszkania; • adres korespondencyjny; • nazwa podmiotu; • siedziba podmiotu; • numer PESEL; • numer NIP; • numer REGON; • numer rachunku bankowego; • dane finansowe.

Załącznik nr 1.10	Sposób przepływu danych pomiędzy poszczególnymi systemami	Wersja 2

System / Moduł „A”	System / Moduł „B”	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych

Załącznik nr 1.10	Sposób przepływu danych pomiędzy poszczególnymi systemami	Stan na dzień 01.03.2017 r.

System / Moduł „A”	System / Moduł „B”	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
PFRON	PFRON (serwer)	A do B	Poczta / Elektronicznie
Płatnik (baza pracowników urzędu i jednostek organizacyjnych)	ZUS	A do B	Internet
Płatnik (baza nauczycieli i pracowników szkół)	ZUS	A do B	Internet
Deklaracje vat7			
jpk			
źródło			
SIO			
CEiDG			
Radix Kadry (baza pracowników urzędu i jednostek organizacyjnych)	Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	A do B	Elektroniczne
Radix Kadry (baza nauczycieli i pracowników szkół)	Radix Płace (baza nauczycieli i pracowników szkół)	A do B	Elektronicznie
Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	Urząd Skarbowy	A do B	Poczta
Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	Płatnik (baza pracowników urzędu i jednostek organizacyjnych)	A do B	Manualnie
Radix Płace (baza nauczycieli i pracowników szkół)	Płatnik (baza nauczycieli i pracowników szkół)	A do B	Elektronicznie
Radix Płace (baza nauczycieli i pracowników szkół)	Urząd Skarbowy	A do B	Poczta
Radix Płace (baza nauczycieli i pracowników szkół)	Bank	A do B	Poczta
Radix Pogrun	Radix WIP	A do B	Elektronicznie
Radix ELUD	Radix Pogrun	A do B	Elektronicznie
Radix ELUD	Radix WIP	A do B	Elektronicznie
Radix ELUD	Ośrodek Informatyki w Poznaniu	A do B	Poczta
Radix ELUD	PESEL MSWiA	A do B	Internet
Radix ELUD	Urząd Skarbowy	A do B	Poczta

Podmioty do których przekazywane są dane to:

- Zakład Ubezpieczeń Społecznych
- Powszechny Zakład Ubezpieczeń
- Urząd Skarbowy
- Podmioty zewnętrzne na podstawie odrębnych umów

Podmiotom powyższym dane te są przesyłane teletransmisyjnie lub w formie tradycyjnej za pośrednictwem Internetu i/lub poczt elektronicznych, mogą także być przekazywane na nośnikach danych takich jak np.: płyty CD. Przy użyciu Internetu realizowane są także przelewy bankowe i międzybankowe.

W związku z tym, iż w Urzędzie Gminy w Olszówce, dane osobowe przetwarzane są w komputerach posiadających połączenie z siecią publiczną (Internetem) stosowane są środki bezpieczeństwa na poziomie wysokim.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w ..... w dniu ..... roku pomiędzy:

Urzędem Gminy w Olszówce z siedzibą w Olszówce (...-.....), Olszówka 15, NIP ....., REGON .....,

reprezentowanym przez:
.....
zwanym dalej „**Administratorem**" lub „**Zleceniodawcą**"

a
..... prowadzącym działalność gospodarczą pod firmą ..... z siedzibą w ....., ul. ....., posiadającym NIP: ....., REGON: .....,

lub
..... z siedzibą w ....., ul. ....., wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy .....w ..... Wydział Gospodarczy KRS pod numerem ....., NIP ....., REGON .....

reprezentowaną przez:
.....
Zwaną/zwanym dalej „**Zleceniobiorcą**" lub „**Procesorem**",

o treści następującej:

§ 1 Definicje

1. **Procesor** – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą,
2. **Administrator Danych** – Urząd Gminy w Olszówce,
3. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5. **Ustawa** – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922 z późn. zm.),
6. **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024),
7. **Podprocesor** – podmiot, któremu Procesor powierzył w całości lub częściowo przetwarzanie danych osobowych, jako konsekwencję realizowania swojej umowy powierzenia ze Zleceniodawcą,
8. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

§ 2 Przedmiot Umowy

1. Przedmiotem Umowy jest powierzenie Procesorowi przez Zleceniodawcę przetwarzania danych osobowych, ujętych w zbiorze o nazwie.....
2. Celem przetwarzania danych osobowych jest realizacja postanowień umowy z dnia ....., w tym w szczególności świadczenie usług .....
3. Zakres przetwarzania obejmuje w szczególności: *zbieranie, archiwizowanie, przechowywanie, utrwalanie, opracowywanie* danych osobowych, w tym następujących danych: *Zakres danych*.

§ 3 Zobowiązania Procesora

1. Procesor zobowiązuje się przetwarzać powierzone dane wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Procesor zobowiązuje się przed przystąpieniem do przetwarzania danych powierzonych przez Zleceniodawcę wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki techniczne i organizacyjne, przewidziane w art. 36-39 Ustawy.
3. Procesor zobowiązuje się przed przystąpieniem do przetwarzania danych powierzonych przez Zleceniodawcę spełnić wymagania określone w przepisach, o których mowa w art. 39a Ustawy.
4. Procesor zobowiązuje się do nadzoru nad przestrzeganiem zasad ochrony, o których mowa w punkcie 3 powyżej lub wyznacza do tego Administratora Bezpieczeństwa Informacji.
5. Procesor zobowiązuje się do dopuszczania do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Procesora.
6. Procesor zobowiązuje się do zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
7. Procesor zobowiązuje się do prowadzenia ewidencji osób upoważnionych do ich przetwarzania.
8. Procesor zobowiązuje się do zapewnienia, że osoby, które zostały przez niego upoważnione do przetwarzania danych, zachowywały w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
9. Procesor zobowiązuje się do opracowania, wdrożenia i utrzymywania przez cały czas obowiązywania niniejszej umowy Polityki bezpieczeństwa danych osobowych, zgodnie z wymaganiami Rozporządzenia.
10. Procesor zobowiązuje się do opracowania, wdrożenia i utrzymywania przez cały czas obowiązywania niniejszej umowy Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zgodnie z wymaganiami Rozporządzenia.
11. Procesor nie może powierzyć wykonania wszystkich lub choćby części czynności przetwarzania danych osobowych, o których mowa w punkcie 2 Umowy, innemu podmiotowi (Podprocesorowi) bez uprzedniej pisemnej zgody Zleceniodawcy.
12. W przypadku, o którym mowa powyżej, Procesor ma obowiązek zweryfikować, czy Podprocesor opracował i wdrożył Politykę bezpieczeństwa danych osobowych oraz Instrukcję zarządzania systemem informatycznym służącymi do przetwarzania danych osobowych przed przystąpieniem do przetwarzania.
13. Po rozwiązaniu lub wygaśnięciu Umowy Procesor zobowiązuje się niezwłocznie zwrócić Zleceniodawcy powierzone dane osobowe i trwale usunąć je z wszystkich nośników, zarówno w wersji elektronicznej, jaki i papierowej. Zobowiązanie, o którym mowa w niniejszym ustępie obejmuje również te podmioty, które przetwarzają dane na zlecenie Procesora jako Podprocesorzy.
14. Procesor zobowiązuje się w ciągu 7 dni od daty usunięcia danych przekazać Zleceniodawcy protokoły zniszczenia zbiorów danych osobowych.

§ 4 Uprawnienia Administratora

1. Zleceniodawca zastrzega możliwość przeprowadzenia kontroli Procesora w zakresie przestrzegania wymagań art. 36-39a Ustawy. Kontrola taka może się odbywać wyłącznie po uprzednim powiadomieniu Procesora.
2. Po kontroli Zleceniodawca może przekazać Procesorowi pisemne zalecenia pokontrolne wraz z terminem ich realizacji.
3. Procesor zobowiązuje się do niezwłocznego poinformowania Zleceniodawcy o jakimkolwiek postępowaniu administracyjnym lub sądowym, decyzji administracyjnej, orzeczeniu, zapowiedzianych kontrolach i inspekcjach, jeśli dotyczą one danych osobowych powierzonych przez Zleceniodawcę.

§ 5 Odpowiedzialności i kary

1. Procesor przyjmuje do wiadomości, iż podczas realizacji Umowy w zakresie przestrzegania przepisów art. 36-39a Ustawy, ponosi odpowiedzialność jak Zleceniodawca.
2. Procesor przyjmuje do wiadomości, iż w związku z realizacją Umowy może być poddany kontroli zgodności przetwarzania danych przez GIODO, z zastosowaniem odpowiednio przepisów art. 14 – 19b Ustawy.
3. Procesor odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez niego powierzonych danych osobowych.
4. W przypadku naruszenia przepisów Ustawy w ramach realizacji Umowy z przyczyn leżących po stronie Procesora, w następstwie którego Zleceniodawca zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Procesor zobowiązuje się do zwrócenia równowartości odszkodowania lub grzywny poniesionych przez Zleceniodawcę.
5. W przypadku naruszenia postanowień paragrafów 3-5 Umowy, Zleceniodawca może obciążyć Procesora karą umowną w wysokości .....zł (słownie: .....złotych) za każde naruszenie.

§ 6 Obowiązywanie umowy

1. Umowa zostaje zawarta na czas obowiązywania umowy, o której mowa w § 2 ust. 2.
2. Zleceniodawca może wypowiedzieć Umowę a także umowę, o której mowa w § 2 ust. 2 w przypadku:
    a) rażącego naruszenia przez Procesora postanowień Umowy,
    b) wyrządzenia przez Procesora przy wykonaniu Umowy szkody Zleceniodawcy lub osobie, której dane Procesor przetwarza na mocy umowy powierzenia,
    c) wszczęcia przez GIODO postępowania przeciw Procesorowi w związku z naruszeniem ochrony danych osobowych.

§ 7 Postanowienia końcowe

1. Wszelkie zmiany Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową, zastosowanie znajdują przepisy polskiego prawa, w tym Ustawy oraz Kodeksu Cywilnego.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Zleceniodawca ..... *Zleceniobiorca* .....

Załącznik nr 1.12	Ewidencja podmiotów, którym powierzono przetwarzanie danych	Wersja 2

L.P.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Nazwa procesora	Podstawa prawna powierzenia przetwarzania	Zakres powierzenia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					

Załącznik nr 1.13	Rejestr udostępnień danych osobowych	Wersja 2

L.P.	Nazwa zbioru danych, z którego następuje udostępnienie danych osobowych	Nazwa podzbioru, z którego następuje udostępnienie danych osobowych	Imię i nazwisko, stanowisko służbowe pracownika dokonującego udostępnienia	Zakres udostępnienia	Nazwa podmiotu któremu udostępniono dane	Podstawa udostępnienia danych	Data udostępnienia	Uwagi
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								
16.								
17.								
18.								
19.								
20.								

Załącznik nr 1.13	Rejestr udostępnień danych osobowych	Wersja 2

Załącznik nr 1.14	Wzór raportu z naruszenia bezpieczeństwa przetwarzania danych osobowych	Wersja 2

W dniu ..... doszło do naruszenia bezpieczeństwa danych osobowych przetwarzanych w .....

Nazwa zbioru danych, w którym doszło do naruszenia: .....

Osoba odpowiedzialna za bezpieczeństwo danych osobowych w kontrolowanej jednostce:

.....

Opis stanu faktycznego i wykonanych czynności:

.....
.....

Stwierdzone nieprawidłowości:

.....
.....

Lp.	Data naruszenia	Nazwa Zbioru Danych Osobowych	System przetwarzania/nazwa systemu	Zakres naruszenia danych
1				
2				
3				

Zalecenia naprawcze:

.....
.....

Termin odzyskania danych z kopii zapasowych: .....

Termin wznowienia przetwarzania danych: .....

.....

data i podpis osoby odpowiedzialnej

.....

data i podpis Administratora Bezpieczeństwa Informacji

Rozdzielnik:

1 x Administrator Danych

Załącznik nr 1.15	Wniosek o planowanym utworzeniu zbioru danych osobowych	Wersja 1

Olszówka, dnia .....

Informacja o planowanym utworzeniu zbioru danych w Urzędzie Gminy w Olszówce	
Proponowana nazwa zbioru danych (nazwa zbioru danych powinna odpowiadać celowi przetwarzania danych oraz ich zakresowi, a także odpowiadać nazewnictwu stosowanemu w przepisach prawa)	
Podstawa prawna przetwarzania danych osobowych w zbiorze danych (należy wskazać przepis prawa lub określić przesłankę dopuszczalności przetwarzania danych określoną w art. 23 ust. lub w art. 27 ust. 2 Ustawy o ochronie danych osobowych)	
Komórka organizacyjna prowadząca zbiór danych	
Sposób przetwarzania danych w zbiorze (system informatyczny, forma papierowa)	
Zakres przetwarzania danych (należy wskazać kategorie danych osobowych przetwarzanych w zbiorze danych)	
Cel przetwarzania danych osobowych w zbiorze danych	
Kategorie odbiorców w rozumieniu art. 7 pkt 6 Ustawy o ochronie danych osobowych, którym dane mogą być udostępnianie	
Informacje o sposobie udostępniania danych	
Informacje, czy zbiór podlega obowiązkowi rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych, a w przypadku zwolnienia z obowiązku rejestracji wskazanie podstawy prawnej tego zwolnienia zgodnie z art. 43 ust.1 Ustawy o ochronie danych osobowych	
Uzasadnienie potrzeby utworzenia zbioru danych	

.....
podpis kierownika komórki organizacyjnej
lub upoważnionego pracownika

.....

(miejscowość i data)

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH

Niniejszym oświadczam, że dane osobowe, które zostały przekazane do ..... w dniu ..... w związku z realizacją Umowy z dnia ..... zawartej pomiędzy ....., a ..... zostały dnia ..... usunięte z wszelkich nośników wraz z informacjami mogącymi posłużyć do odtworzenia, w całości lub części, zawartości

Oświadczam, że nie zostały wykonane kopie powyżej wymienionej danych osobowych.

.....

(podpis Administratora Danych)

.....

(podpis Administratora Bezpieczeństwa Informacji)

.....
miejscowość, data

PROTOKÓŁ
Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*
w zakresie ochrony danych osobowych

1.	Nazwa kontrolowanej komórki organizacyjnej:	
2.	Przedmiot kontroli:	
3.	Data wykonania czynności kontrolnych:	
4.	Imię i nazwisko osoby wykonującej czynności kontrolne:	
5.	Imiona i nazwiska osób udzielających informacji dotyczących przedmiotu kontroli:	
6.	Ustalenia dokonane w trakcie czynności kontrolnych:	
7.	Pozyskane dowody / próbki:	
8.	Wnioski i zalecenia pokontrolne:	

.....
(data i podpis osoby wykonującej czynności kontrolne)

.....
(podpis kierownika kontrolowanej komórki organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Administrator Bezpieczeństwa Informacji

*niepotrzebne skreślić

Załącznik nr 1.18	Wzór sprawozdania dla AD	Wersja 1

.....

miejscowość, data

SPRAWOZDANIE
ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Oznaczenie Administratora Danych i adres jego siedziby
Imię i nazwisko Administratora Bezpieczeństwa Informacji
Wykaz czynności podjętych przez Administratora Bezpieczeństwa Informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach
Data rozpoczęcia i zakończenia sprawdzenia
Przedmiot i zakres sprawdzenia
Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych
Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem
Spis załączników stanowiących składową część sprawozdania

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Link do informacji znajdujących się w rejestrze	Nazwa Zbioru Danych Osobowych
ZDO 1	
ZDO 2	
ZDO 3	

POWRÓT DO PIERWSZEJ STRONY

LP.	INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE	
1	Nazwa zbioru danych;	
2	Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;	
3	Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 3la ustawy i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;	
4	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy i adres jego siedziby lub miejsca zamieszkania w przypadku powierzenia przetwarzania danych temu podmiotowi;	
5	Podstawa prawna upoważniająca do prowadzenia zbioru danych;	
6	Cel przetwarzania danych w zbiorze;	
7	Opis kategorii osób, których dane są przetwarzane w zbiorze;	
8	Zakres danych przetwarzanych w zbiorze;	
9	Sposób zbierania danych do zbioru w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;	
10	Sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane podmiotom innym niż upoważnione na podstawie przepisów prawa;	
11	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	
12	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego;	
13	Data wpisania zbioru do rejestru;	
14	Data dokonania ostatniej aktualizacji;	

POWRÓT DO PIERWSZEJ STRONY

LP.	INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE	
1	Nazwa zbioru danych;	
2	Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;	
3	Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 3la ustawy i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;	
4	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy i adres jego siedziby lub miejsca zamieszkania w przypadku powierzenia przetwarzania danych temu podmiotowi;	
5	Podstawa prawna upoważniająca do prowadzenia zbioru danych;	
6	Cel przetwarzania danych w zbiorze;	
7	Opis kategorii osób, których dane są przetwarzane w zbiorze;	
8	Zakres danych przetwarzanych w zbiorze;	
9	Sposób zbierania danych do zbioru w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;	
10	Sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane podmiotom innym niż upoważnione na podstawie przepisów prawa;	
11	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	
12	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego;	
13	Data wpisania zbioru do rejestru;	
14	Data dokonania ostatniej aktualizacji;	

POWRÓT DO PIERWSZEJ STRONY

LP.	INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE	
1	Nazwa zbioru danych;	
2	Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;	
3	Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 3la ustawy i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;	
4	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy i adres jego siedziby lub miejsca zamieszkania w przypadku powierzenia przetwarzania danych temu podmiotowi;	
5	Podstawa prawna upoważniająca do prowadzenia zbioru danych;	
6	Cel przetwarzania danych w zbiorze;	
7	Opis kategorii osób, których dane są przetwarzane w zbiorze;	
8	Zakres danych przetwarzanych w zbiorze;	
9	Sposób zbierania danych do zbioru w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;	
10	Sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane podmiotom innym niż upoważnione na podstawie przepisów prawa;	
11	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	
12	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego;	
13	Data wpisania zbioru do rejestru;	
14	Data dokonania ostatniej aktualizacji;	

Historia zmian

Data	Autor	Zmiany	Uwagi

Załącznik nr 2
do zarządzenia nr 5/2017
z dnia 01.03.2017 r.
Wójta Urzędu Gminy w Olszówce

Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Urząd Gminy w Olszówce

Wersja nr 3		**Pieczęć:** URZĄD GMINY w OLSZÓWCE OLSZÓWKA 15 62-641 Olszówka NIP 666-14-02-313, R.000549329 tel. 63 273 90 10, fax 63 273 90 30	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Administrator Systemów Informatycznych	01.03.2017 r.	Administrator Danych	01.03.2017 r.
Ilość stron: 22 (+ 3 załączniki)			

Spis treści

1. Historia zmian

Data	Autor	Zmiany	Uwagi

2. Postanowienia ogólne

Instrukcja określająca sposób zarządzania systemem informatycznym zwaną dalej Instrukcją jest dokumentem, który określa zasady i sposób postępowania pracowników Urzędu Gminy w Olszówce, w związku z przetwarzaniem danych osobowych w systemach informatycznych.

Celem Instrukcji jest określenie zasad zarządzania systemami informatycznymi służącymi w Urzędzie Gminy do przetwarzania danych osobowych oraz zapewnienie odpowiedniego poziomu bezpieczeństwa i ochrony przed przetwarzaniem danych osobowych w zbiorach w sposób sprzeczny z postanowieniami Ustawy, Rozporządzenia, Polityki i stosownych umów powierzenia przetwarzania danych osobowych.

3. Podstawy prawne

1. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922) zwana dalej Ustawą.
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakie powinny posiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024) zwane dalej Rozporządzeniem.

Instrukcja jest dokumentem uzupełniającym Politykę bezpieczeństwa danych osobowych w Urzędzie Gminy w Olszówce. Niewymienione w Instrukcji wymagania, procedury i sposoby postępowania zostały określone w Polityce bezpieczeństwa danych osobowych.

Do stosowania zapisów instrukcji zobowiązani są:

1. Administrator Danych (AD),
2. Administrator Bezpieczeństwa Informacji (ABI),
3. Administrator Systemu Informatycznego (ASI),
4. Osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym.

4. Definicje

1.1 **Instrukcja** – rozumie się przez to Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązującą w Urzędzie Gminy w Olszówce;

1.2 **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych, która została przyjęta jako obowiązujący dokument w Urzędzie Gminy w Olszówce;

1.3 **Administrator Danych (AD)** – Urząd Gminy w Olszówce reprezentowany przez Wójta - decyduje o celach i środkach przetwarzania danych osobowych;

1.4 **Administrator Bezpieczeństwa Informacji (ABI)** – osoba, wyznaczona przez Urząd Gminy w Olszówce odpowiedzialna za organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych;

1.5 **Administrator systemu informatycznego (ASI)** – osoba lub zewnętrzny podmiot nadzorujący pracę systemu informatycznego oraz wykonujący w nim czynności wymagające specjalnych uprawnień;

1.6 **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

1.7 **Dane wrażliwe** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

1.8 **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

1.9 **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący użytkownika;

1.10 **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

1.11 **Integralność systemu** – właściwość zapewniająca nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

1.12 **Nośnik danych** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;

1.13 **Odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu przetwarzającego dane osobowe mającego siedzibę lub miejsce zamieszkania w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

1.14 **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która została upoważniona na piśmie przez Administratora Danych do przetwarzania danych osobowych w Urzędzie Gminy w Olszówce;

1.15 **Pracownicy** - osoby zatrudnione w Urzędzie Gminy w Olszówce na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy

wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u administratora danych osobowych;

1.16 **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

1.17 **Przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

1.18 **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

1.19 **Sieć publiczna** – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 Ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489 z późniejszymi zmianami;

1.20 **Sieć telekomunikacyjna** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 Ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016, 1489 z późniejszymi zmianami;

1.21 **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

1.22 **Teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

1.23 **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

1.24 **Uwierzytelniane** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu;

1.25 **Użytkownik** – osoba należąca do pracowników posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych, w szczególności do przetwarzania danych osobowych w systemie informatycznym;

1.26 **Zbiór danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

1.27 **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;

1.28 **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

1.29 **Wykaz skrótów**:

- **AD** – Administrator Danych,
- **Urząd** – Urząd Gminy w Olszówce,

- **ABI** – Administrator Bezpieczeństwa Informacji,
- **ASI** – osoba odpowiedzialna za systemy informatyczne służące do przetwarzania danych osobowych,
- **GIODO** – Generalny Inspektor Ochrony Danych Osobowych – organ do sprawy ochrony danych osobowych,
- **Ustawa** – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922 z późn. zm.),
- **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakie powinny posiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024).

5. Poziom bezpieczeństwa przetwarzania danych osobowych

1. Zgodnie z §6 Rozporządzenia u AD zastosowano poziom bezpieczeństwa przetwarzania danych osobowych **„Wysoki"** ze względu na połączenie urządzeń z siecią publiczną.

5.1. Środki ochrony fizycznej

1. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
2. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej u AD z ważnym upoważnieniem do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych osobowych;
3. Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);
4. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;
5. Zbiory danych są przetwarzane i przechowywane w pomieszczeniach, w których okna są zabezpieczone za pomocą krat, rolet lub folii antywłamaniowej;
6. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych niemetalowych i metalowych szafach;
7. Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojących gaśnic;
8. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;
9. Kopie zapasowe zbiorów danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajdują się serwery, na którym dane osobowe przetwarzane są na bieżąco.

5.2. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych.
2. Wszystkie urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną.
3. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
4. Zastosowano urządzenia typu UPS dla maszyn serwerowych oraz stacji roboczych, chroniących system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
5. Użytkownicy systemu informatycznego zobowiązani są do okresowej zmiany haseł.
6. Zmiana hasła następuje nie rzadziej, niż co 30 dni.
7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest przydzielony innej osobie.

8. Dostęp do systemów operacyjnych, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
9. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
10. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.
11. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
12. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
13. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
14. Zastosowano środki adekwatne do możliwości technicznych i organizacyjnych AD, uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
15. Sprzęt komputerowy służący do przetwarzania danych osobowych połączony jest z siecią publiczną Internet za pośrednictwem urządzeń brzegowych pełniących rolę bramy zabezpieczającej przed niepowołanym dostępem.
16. Urządzenia, dyski lub inne nośniki informacji zawierające dane osobowe pozbawia się zapisu tych danych przed: likwidacją, przekazaniem podmiotowi nieuprawnionemu, naprawą chyba, że naprawa odbywa się pod nadzorem osoby upoważnionej do przetwarzania danych osobowych.
17. Urządzenia i nośniki informacji zawierające dane osobowe przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

5.3. Środki ochrony w ramach narzędzi programowych

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Zastosowano działający w tle program antywirusowy na komputerach użytkowników.
4. Skonfigurowano i zapewniono automatyczne pobieranie aktualizacji do systemów operacyjnych.
5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
6. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
7. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

9. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
10. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

6. Procedura nadawania, aktualizacji i wycofania uprawnień do przetwarzania danych osobowych w systemach informatycznych i rejestrowanie tych uprawnień

1. Dla wszystkich użytkowników stosowane są uprawnienia do zasobów i zbiorów wedle zasady niezbędnego minimum potrzebnego do pracy.
2. W przypadku, w którym AD zatrudnia nowego pracownika lub nawiązuje współpracę na podstawie umowy zlecenia, umowy o dzieło lub umowy o świadczenie usług z podmiotem, który wykonywać będzie przedmiot umowy w siedzibie AD, ASI niezwłocznie po powzięciu informacji o tym fakcie nadaje pracownikowi odpowiednie uprawnienia dostępu do systemów informatycznych, w którym przetwarzane są dane osobowe.
3. ASI odpowiedzialny jest również za aktualizację i wycofanie uprawnień dostępu do systemu informatycznego.
4. Określenie dostępu, o którym mowa w punktach 2 i 3 powyżej następuje w porozumieniu z AD i ABI.
5. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez AD.
6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania danych i środków zabezpieczenia w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia/zaprzestaniu wykonywania prac. Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe stanowi część składową upoważnienia do przetwarzania danych osobowych.
7. ASI informuje użytkownika o przydzielonych uprawnieniach, koncie i haśle początkowym.
8. Użytkownicy powinni pracować na kontach zwykłych użytkowników. Praca na kontach administracyjnych jest dopuszczalna tylko dla ASI oraz upoważnionych przez niego lub AD osób.
9. Po nadaniu, aktualizacji lub wycofaniu uprawnień, stosownych zmian w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w Polityce dokonuje ABI.
10. O fakcie zrealizowania dyspozycji wycofania uprawnień użytkownika do systemu informatycznego, w którym przetwarzane są dane osobowe, ASI niezwłocznie blokuje konto użytkownika i informuje o tym fakcie ABI.
11. Identyfikator nowego konta w systemie informatycznym nadany przez ASI musi być unikalny w obrębie systemu i organizacji.

12. ABI prowadzi raz na 6 miesięcy przegląd aktualności kont użytkowników wraz z uprawnieniami im nadanymi przez ASI.
13. Osobą zastępującą ASI w sytuacjach awaryjnych jest pani Elwira Nita.

7. Metody i środki uwierzytelniania użytkowników w systemach informatycznych

1. ASI nadaje użytkownikowi unikalny identyfikator oraz hasło początkowe.
2. Do uwierzytelnienia użytkownika w systemie na wszystkich poziomach stosuje się identyfikatory oraz hasła a także odpowiedni poziom uprawnień zarządzane przez ASI.
3. Identyfikator użytkownika w systemie operacyjnym składa się z pierwszej litery imienia i pełnego nazwiska użytkownika zapisywanych bez polskich znaków diakrytycznych. W przypadku zbieżności loginów ASI nadaje inny identyfikator.
4. Identyfikator i hasło początkowe przekazywane jest przez ASI użytkownikowi osobiście, w miejscu pracy użytkownika.
5. Identyfikator użytkownika, nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
6. Hasła użytkowników podlegają okresowej zmianie nie rzadziej niż co 30 dni. System informatyczny wymusza zmianę przez użytkownika hasła automatycznie.
7. Hasła powinny być różne od dwunastu (12) ostatnio używanych.
8. Hasło użytkownika umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie jego ważności.
9. Minimalna długość hasła przydzielonego użytkownikowi wynosi 8 znaków alfanumerycznych (małe i wielkie litery oraz cyfry) i znaków specjalnych.
10. W przypadku wprowadzenia pięciokrotnie (5) błędnego hasła dostęp do systemu jest blokowany na trzydzieści minut.
11. ASI uwierzytelnia się w systemie informatycznym służącym do przetwarzania danych osobowych przy pomocy hasła o minimalnej długości wynoszącej 10 znaków alfanumerycznych (małe i wielkie litery oraz cyfry) i znaków specjalnych.
12. Zabrania się używania identyfikatora lub hasła drugiej osoby.
13. Identyfikator (hasło) osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostanie niezwłocznie zablokowany w systemie informatycznym, w którym są przetwarzane, hasło zostanie unieważnione oraz zostaną podjęte stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
14. Użytkownik jest zobowiązany po pierwszym zalogowaniu do systemu do zmiany hasła początkowego na indywidulne.
15. Hasło indywidulne musi być tworzone przez użytkownika zgodnie z zasadami bezpieczeństwa opisanymi w Instrukcji oraz polityką haseł ustawioną w Active Directory.
16. Użytkownik bezwzględnie nie może ujawnić osobom trzecim środków uwierzytelniania w tym identyfikatora oraz jakichkolwiek – aktualnych, poprzednich, tymczasowych haseł mu powierzonych.
17. Użytkownik zobowiązany jest do przechowywania środków uwierzytelniania (identyfikatora i hasła) w sposób uniemożliwiający dostęp osobom trzecim.
18. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym system zapewnia odnotowanie:

a. daty pierwszego wprowadzenia danych do systemu,
b. identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
c. informacji o odbiorcach, którym dane osobowe zostały udostępnione.

19. W przypadku braku funkcjonalności o której mowa w pkt. 18 rejestr informacji jest prowadzony w formie papierowej przez ABI po otrzymaniu informacji od ASI.

8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników systemu

1. Rejestrowanie użytkownika odbywa się z chwilą rozpoczęcia przez niego pracy w systemie. Procedura ta rozpoczyna się od wprowadzenia identyfikatora oraz hasła. Na tej podstawie system stwierdza tożsamość i przydzielone uprawnienia użytkownika. Po poprawnym wykonaniu tej czynności użytkownik może wykonywać wszystkie czynności w ramach przyznanych uprawnień.
2. Czynności związane z rozpoczęciem i zakończeniem pracy w systemie wymagają następujących działań:
   2.1. Użytkownik włącza komputer.
   2.2. Użytkownik wprowadza identyfikator i hasło do programu szyfrującego powierzchnie dysków (w przypadku używania laptopów) w celu otrzymania dostępu do zasobów komputera.
   2.3. Użytkownik wprowadza identyfikator i hasło i loguje się do systemu operacyjnego.
   2.4. Użytkownik uzyskuje dostęp do przetwarzania danych osobowych za pośrednictwem oprogramowania systemu operacyjnego.
   2.5. W przypadku, kiedy użytkownik korzysta z komputera przenośnego, poza wewnętrzną (korporacyjną) siecią teleinformatyczną, korzystanie z jej zasobów wymaga:
      - zachowania zgodnie z pkt. 2.1 do 2.4,
      - połączenia za pomocą modułu wi-fi lub modemu 3G/LTE z siecią publiczną,
      - uwierzytelnienia certyfikatu dostępu przez VPN.
   2.6. Po zakończeniu pracy użytkownik powinien rozłączyć wszelkie połączenia VPN z siecią firmową a następnie wylogowuje się z systemu za pomocą polecenia „wyloguj".
   2.7. Użytkownik wyłącza komputer.
3. Zawieszenie pracy w systemie wymaga od użytkownika wylogowania się i zakończenia pracy w systemie. Każda następna operacja w systemie musi być ponownie oparta na wykonaniu procedury uwierzytelniania użytkownika.
4. Użytkownik zobowiązany jest do ochrony identyfikatora i hasła w trakcie wprowadzania ich do systemu.
5. Procedura uwierzytelniania powinna być wykonana przez użytkownika w sposób uniemożliwiający zapoznanie się z hasłem i identyfikatorem osobom postronnym, tzn. nikt poza użytkownikiem nie powinien widzieć ekranu monitora oraz klawiatury w trakcie wprowadzania danych uwierzytelniających.

6. W przypadku używania laptopów zaleca się stosowanie filtrów prywatyzujących w celu ochrony wprowadzanego identyfikatora i hasła użytkownika przed osobami niepowołanymi.
7. W przypadku braku możliwości bezpiecznego zalogowania się lub problemów z funkcjonowaniem systemu, użytkownik zobowiązany jest do przerwania czynności i powrócenia do niej w warunkach bezpiecznych.
8. Stanowisko komputerowe powinno być ustawione w takim miejscu aby zapobiec nieupoważnionym osobom wgląd lub dostęp do danych zawierających dane osobowe.
9. Należy zwrócić szczególną uwagę na otoczenie, w jakim znajduje się stanowisko komputerowe. Niedopuszczalne jest umieszczanie przedmiotów które mogłyby uszkodzić sprzęt komputerowy.
10. Należy dbać o to aby stanowisko komputerowe było zadbane i utrzymane w czystości. Zabrania się spożywania pokarmów i płynów w bezpośrednim otoczeniu stanowiska komputerowego, które skutkowałoby jego uszkodzeniem np. zalaniem klawiatury.
11. Jeżeli użytkownik stwierdzi naruszenie lub zagrożenie naruszeniem bezpieczeństwa przetwarzanych danych osobowych (zniszczenie, uszkodzenie, modyfikację, nieuprawniony wgląd), niezwłocznie zgłasza incydent ASI oraz bezpośredniemu przełożonemu, który powiadamia o zdarzeniu ABI. Powyższe powiadomienia powinny nastąpić za pośrednictwem dostępnego kanału komunikacji szczegółowo opisując zdarzenie.

9. Procedury korzystania z oprogramowania

1. Zabronione jest użytkowanie oprogramowania niezwiązanego z zakresem wykonywanych obowiązków służbowych pracownika.
2. Można korzystać wyłącznie z oprogramowania i systemów dopuszczonych przez ASI do eksploatacji.
3. W szczególnych sytuacjach dopuszczone jest stosowanie lub wprowadzanie do systemu informatycznego aplikacji pod warunkiem przestrzegania warunków umowy licencyjnej oraz uzyskania pisemnej lub mailowej zgody od ASI.
4. Zabrania się korzystania z programów i systemów niebędących własnością AD lub niedopuszczonych przez ASI do użytkowania. Dotyczy to w szczególności:
    a. nielegalnego oprogramowania naruszającego prawa autorskie,
    b. legalnego oprogramowania ale bez ważnej licencji,
    c. programów załączonych do gazet, czasopism itp. oraz innych instalowanych bez konsultacji z ASI.
5. Instalacji bądź deinstalacji oprogramowania może dokonać tylko ASI bądź wyznaczona przez niego osoba.
6. Każda instalacja bądź uruchomienie nowego oprogramowania musi być poprzedzone kontrolą antywirusową pakietu instalacyjnego.
7. ASI zobowiązany jest do nadzorowania zgodności instalowanego oprogramowania z posiadanymi licencjami.
8. ASI prowadzi audyt oraz wykaz oprogramowania dopuszczonego do użytkowania w Urzędzie.
9. Zakupy oprogramowania muszą być zaakceptowane przez ABI i przez ASI.
10. Dopuszcza się możliwość monitorowania jednostek komputerowych pod kątem zainstalowanego oprogramowania oraz przechowywanych lokalnie plików.
11. Każdy z pracowników musi posiadać podpisane oświadczenie o znajomości treści Instrukcji Zarządzania Systemem Informatycznym oraz o ponoszeniu odpowiedzialności za instalację bądź deinstalację oprogramowania we własnym zakresie. Wzór oświadczenia stanowi załącznik nr 1 do niniejszej Instrukcji.

10. Procedury korzystania z Internetu i poczty elektronicznej

Celem procedury jest uregulowanie zasad korzystania z Internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych przez te media.

1. Użytkownicy zobowiązani są do przestrzegania następujących zasad:
   a. zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych niezwiązanych w wykonywaniem obowiązków pracowniczych bądź świadczeniem usług przez współpracowników AD.
   b. użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane,
   c. do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez ASI formy dostępu.
   d. ASI może stosować mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
      - blokowanie stron internetowych określonego typu,
      - blokowanie określonych stron internetowych,
      - analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

2. Użytkownicy poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:
   a. do wymiany korespondencji w czasie korzystania z systemu informatycznego jest wykorzystywana tylko służbowa poczta elektroniczna,
   b. przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych,
   c. w przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z ASI,
   d. użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu,
   e. w przypadku przesyłania danych wrażliwych lub informacji stanowiących tajemnicę służbową należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie).
   f. jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją.
   g. użytkownicy nie mogą uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu ASI, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.

h. użytkownicy nie mogą rozsyłać za pośrednictwem poczty elektronicznej informacji, które mogą mieć wpływ na bezpieczeństwa i stabilność systemu informatycznego,
i. użytkownicy nie mogą rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów – określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej.

11. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Odpowiedzialnym za tworzenie kopii zapasowych danych osobowych oraz narzędzi programowych służących do przetwarzania danych jest ASI.
2. Poza standardowym wyposażeniem serwerów w macierz sprzętową RAID, skonfigurowaną w sposób pozwalający na nieprzerwaną pracę serwera w przypadku awarii jednego z dysków, najważniejsze dane Urzędu są zabezpieczane w sposób cykliczny i zautomatyzowany. Poniżej zostały opisane zasady oraz mechanizmy wspierające ten proces.
3. Kopie zapasowe wykonywane są zgodnie z poniższym harmonogramem:

Nazwa serwera źródłowego	Nazwa/rodzaj zasobu	Rodzaj kopii	Częstotliwość	Rotacja
39-UG	całość	pełna	raz dziennie (weekend)	8 tygodni
39-UG	całość	różnicowa	raz dziennie (weekdays)	8 tygodni

4. Rotacja oznacza okres po jakim wykonana kopia jest usuwana.
5. ASI powinien mieć zapewnioną możliwość wykonania raz w miesiącu testów odtworzenia kopii zapasowych w środowisku testowym oddzielonym od produkcyjnego (np. poprzez wirtualizację).
6. Jeżeli ASI przewiduje konieczność tworzenia innych niż zapasowych całościowych lub częściowych kopii danych, należy je wykonywać wyłącznie na ewidencjonowanych nośnikach elektronicznych. Rejestr nośników elektronicznych prowadzi ASI.

12. Zasady bezpiecznego przechowywania, transportu i niszczenia urządzeń oraz innych elektronicznych nośników informacji zawierających dane osobowe

1. Dyski zewnętrzne lub inne nośnikach informacji, na których wykonano kopie zapasową należy przechowywać w wyznaczonym obszarze przetwarzania danych w meblach biurowych zamykanych na klucz zabezpieczając je przed dostępem do nich osób nieupoważnionych, przed zniszczeniem oraz kradzieżą.
2. Dane osobowe znajdujące się na komputerach przenośnych powinny zostać zabezpieczone poprzez szyfrowanie całej powierzchni dysków twardych.
3. Dane osobowe zapisane na dyskach zewnętrznych lub innych nośnikach informacji, po ustaniu potrzeby ich przechowywania, należy niezwłocznie usunąć z urządzenia oraz wykonać formatowanie nośnika. W przypadku, kiedy nośnik pozwala jedynie na jednokrotny zapis należy go zniszczyć.
4. Zniszczenie nośnika informacji, który zawierał kiedykolwiek dane osobowe odbywa się pod nadzorem ASI, z wykorzystaniem urządzeń przystosowanych do tego rodzaju czynności oraz zostaje odnotowane w rejestrze utylizacji, który prowadzi ASI.
5. Transport urządzeń, dysków i innych nośników informacji poza obszar przetwarzania danych jest dozwolony jedynie za zgodą ASI.
6. Osoba wynosząca urządzenie, dysk lub inny nośnik informacji poza obszar przetwarzania danych, zobowiązana jest do zachowania szczególnych środków bezpieczeństwa w celu zapobieżenia dostępowi do nośnika osobom nieupoważnionym. W szczególności niedozwolone jest pozostawianie nośnika poza obszarem przetwarzania danych bez nadzoru.
7. ASI jest zobowiązany prowadzić ewidencję urządzeń mobilnych, na których są przetwarzane dane osobowe, według załącznika nr 2.

13. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest naruszenie bezpieczeństwa systemu informatycznego w tym uzyskanie do niego nieuprawnionego dostępu.

1. Ze względu na podłączenie systemu informatycznego AD do sieci publicznej wszystkie jego elementy są narażone na ingerencję szkodliwego oprogramowania.
2. Źródłami zagrożeń dla systemu informatycznego są zewnętrzne działania osób trzecich, które po przez sieć publiczną próbują uzyskać nieuprawniony dostęp do zasobów informatycznych AD lub działania mające na celu zainfekowanie systemu wirusem komputerowym oraz wewnętrzne działania pracowników AD, w tym próby instalacji nielicencjonowanego oprogramowania lub użycie zainfekowanych wirusem nośników informacji w komputerach służbowych.
3. Zabezpieczeniem przeciwdziałającym zainstalowaniu szkodliwego oprogramowania jest blokada takiej możliwości przez system. Aby móc zainstalować oprogramowanie użytkownik musi mieć status „administratora", który nadawany jest przez ASI na określony czas. System zapewnia codzienny przegląd i weryfikację nadanych uprawnień.
4. W przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego przez szkodliwe oprogramowanie, każdy pracownik AD ma obowiązek zgłosić niezwłocznie zaistniały fakt do ASI.
5. Programem służącym do wykrywania wirusów komputerowych jest Kaspersky Endpoint Security 10, który został zainstalowany na stacjach roboczych oraz serwerach.
6. Oprogramowanie, o którym mowa w punkcie powyżej jest ustandaryzowane (wersja) oraz centralnie zarządzane przez ASI.
7. Oprogramowanie wykonuje raz w miesiącu pełne skanowanie zawartości jednostek komputerowych oraz serwerów pod kątem ewentualnych zagrożeń.
8. ASI jest odpowiedzialny za konfigurację oraz nadzór oprogramowania w taki sposób aby zapewnić regularne skanowanie komputerów pod kątem ewentualnych zagrożeń (np. poprzez cykliczne zadanie zgodne z ustalonym harmonogramem).
9. Aktualizacja bazy wirusów na stanowiskach lub komputerach przenośnych posiadających dostęp do Internetu odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
10. Przyłączając do komputerów zewnętrzne nośniki (np. pendrive, zewnętrzny dysk itp.) są one każdorazowo automatycznie skanowane pod kątem ewentualnych zagrożeń.
11. W przypadku wykrycia wirusa należy:
    a. uruchomić program antywirusowy i skontrolować użytkowany system, usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego, jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
        - zakończyć pracę w systemie komputerowym,
        - odłączyć komputer zainfekowany od sieci.

12. Komputer służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej (Internet) poprzez fizyczne i/lub logiczne zabezpieczenia chroniące przed nieuprawnionym dostępem.
13. Na stanowisku komputerowym, na którym przetwarzane są dane osobowe przed podłączeniem do Internetu należy:
    a. zainstalować program antywirusowy i ustanowić opcję codziennego uaktualniania bazy wirusów,
    b. zainstalować zaporę ogniową (firewall).
14. Zabrania się wykorzystywania Internetu do celów prywatnych a w szczególności do przeglądania stron zawierających treści erotyczne, rasistowskie itp.
15. Zabrania się używania programów typu Kazaa, Torrent do ściągania plików z Internetu (udostępnionych w sieci publicznej) w tym w szczególności do ściągania muzyki, filmów, nielegalnego oprogramowania i innych działań „pirackich".
16. ASI jest zobowiązany do przeglądu logów lub zapisów w dzienniku systemu antywirusowego.

14. Sposób realizacji wymogów określonych w § 7 Rozporządzenia

1. Systemy informatyczne służące do przetwarzania danych osobowych u AD zgodnie z Rozporządzeniem spełniają poniższe wymagania i zapewniają odnotowywanie:

    1.1. Daty pierwszego wprowadzenia danych do systemu.
    1.2. Identyfikatora użytkownika wprowadzającego dane do systemu informatycznego.
    1.3. Źródła danych osobowych.
    1.4. Informacji o odbiorcach danych osobowych oraz dacie i zakresie udostępnienia danych.
    1.5. Sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 Ustawy.
    1.6. Możliwości sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w pkt 1.1 – 1.5

W przypadku braku funkcjonalności o której mowa powyżej rejestr informacji jest prowadzony w formie papierowej przez ABI po otrzymaniu informacji od ASI.

15. Procedury wykonywania napraw, przeglądów i konserwacji systemu informatycznego oraz elektronicznych nośników informacji służących do przetwarzania danych

1. Bieżące przeglądy i konserwacje sprzętu komputerowego, w tym przeglądy i aktualizacje oprogramowania wchodzącego w skład systemu informatycznego, dokonywane są przez ASI, bądź wyznaczoną przez AD osobę.
2. W przypadku, gdy przeglądy i konserwacje systemu informatycznego dokonywane są przez osoby lub podmioty nieposiadające upoważnień do przetwarzania danych osobowych, muszą one odbywać się pod bezpośrednim nadzorem ASI. Przeglądy i konserwacje powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
3. Celem wykonywania okresowych przeglądów systemu informatycznego jest określenie wymaganego przepisami prawa poziomu zabezpieczeń przetwarzania danych osobowych.
4. Przeglądy zgodności z zasadami bezpieczeństwa zasobów teleinformatycznych oraz urządzeń infrastruktury teleinformatycznej należy przeprowadzać co najmniej raz na rok.
5. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa teleinformatycznego powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem, a ich użycie kontrolowane przez ASI.
6. W przypadku likwidacji sprzętu informatycznego lub nośników danych należy każdorazowo sporządzić protokół z czynności na podstawie załącznika nr 3 do niniejszej Instrukcji.
7. W przypadku powierzenia naprawy lub likwidacji dysków lub innych nośników informacji zawierających dane osobowe podmiotowi nieposiadającemu upoważnienia do przetwarzania danych osobowych zgodnie z Rozporządzeniem należy:
   7.1. W przypadku likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe uszkadza się nośnik w sposób uniemożliwiający ich odczytanie i odzyskanie.
   7.2. W przypadku naprawy – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

16. Postępowanie w przypadku stwierdzania naruszenia ochrony danych osobowych

1. Na naruszenie bezpieczeństwa danych osobowych lub możliwość wystąpienia takiego zagrożenia może wskazywać na przykład:
   1.1. Nietypowy stan pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych np. otwarte drzwi, okna, drzwi do szaf i biurek, włączone urządzenia.
   1.2. Zaginięcie sprzętu lub nośników informacji.
   1.3. Nieuzasadnione modyfikacje lub usunięcie danych.
   1.4. Nieprawidłowe lub nietypowe działanie systemu informatycznego.
   1.5. Infekcja wirusa w systemie informatycznym.
   1.6. Uruchomienie przez użytkownika podejrzanych załączników w poczcie elektronicznej.
   1.7. Nietypowe komunikaty wyświetlane na monitorze.
   1.8. Ujawnienie przetwarzanych danych osobowych lub procedur ochrony przetwarzania danych osobom nieupoważnionym.
   1.9. Ujawnienie istnienia nieautoryzowanych kont dostępu do danych osobowych.
   1.10. Przesłanie danych do niewłaściwego adresata.
   1.11. Znalezienie poza obszarem przetwarzania danych osobowych dokumentów papierowych lub nośników informacji zawierających takie dane.
   1.12. Niekontrolowany lub niezgodny z Polityką i Instrukcją pobyt w obszarze przetwarzania danych osoby nieupoważnionej.
2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych lub zaistnienia sytuacji wskazującej na naruszenie, każdy pracownik, a w szczególności osoba upoważniona do przetwarzania danych osobowych, ma obowiązek niezwłocznego powiadomienia o tym fakcie ASI oraz bezpośredniego przełożonego, który zobowiązany jest do pisemnego bądź e-mailowego poinformowania o zgłoszeniu AD oraz ABI.
3. Zadaniem osoby, która zgłosiła naruszenie zasad bezpieczeństwa danych osobowych przed przybyciem ASI lub innej upoważnionej osoby jest:
   3.1. Podjęcie czynności niezbędnych dla powstrzymania dalszych niepożądanych skutków zaistniałego naruszenia o ile istnieje taka możliwość.
   3.2. Wstrzymanie pracy przy komputerze i zabezpieczenie miejsca zdarzenia.
   3.3. Nieopuszczanie bez istotnej uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ASI.
   3.4. Dokonywanie przez pracowników zmian w miejscu naruszenia bez uzyskania zgody ASI, jeżeli jest to uzasadnione koniecznością ratowania osób lub mienia, albo zapobieżenia grożącemu niebezpieczeństwu.
4. Zadaniem ASI po przybyciu na miejsce naruszenia jest:
   4.1. Zapoznanie z zaistniałą sytuacją i wybór metody dalszego postępowania.
   4.2. Zebranie relacji dotyczącej zaistniałego naruszenia od osoby powiadamiającej i ewentualnie od innych świadków naruszenia.
   4.3. Zawiadomienie AD oraz ABI o zaistniałym naruszeniu.

4.4. Sporządzenie pisemnego raportu zgodnie ze wzorem stanowiącym załącznik nr 14 do Polityki Bezpieczeństwa.

5. ASI przekazuje raport ABI, w którym proponuje postępowanie naprawcze mające na celu zapobieżenie podobnym naruszeniom w przyszłości oraz, jeżeli jest to konieczne, określa termin odtworzenia danych z kopii zapasowych i wznowienia przetwarzania danych.
6. Każde naruszenie zasad ochrony bezpieczeństwa danych osobowych w systemie informatycznym musi zostać odnotowane w rejestrze, który prowadzi ASI.
7. Odpowiedzialnym za prowadzenie i okresowe przeglądy rejestru jest ASI.

17. Obowiązki użytkownika związane z obowiązywaniem Instrukcji

Użytkownik systemu informatycznego wykorzystywanego u AD jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i stosować się do jej treści. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu użytkownik będący pracownikiem ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy.

W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszyscy użytkownicy upoważnieni do przetwarzania danych osobowych mogą ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie. Treść niniejszej Instrukcji jest objęta ochroną jako tajemnica przedsiębiorstwa.

18. Spis załączników

Załącznik nr	Opis
Załącznik 1	Porozumienie z pracownikiem lub współpracownikiem w zakresie oprogramowania
Załącznik 2	Ewidencja urządzeń mobilnych
Załącznik 3	Wzór protokołu likwidacji sprzętu informatycznego

Załącznik nr 1	Wzór porozumienia z pracownikiem w zakresie oprogramowania	Wersja 1

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu ..... r. w ..... pomiędzy:
.....z siedzibą w .....,
reprezentowaną/ego przez..... ....., (zwaną/ego dalej „Pracodawcą");
oraz
Panią/Panem ..... zamieszkałą/ym w .....przy

ul. ..... (zwaną/ym dalej „Pracownikiem");

Wstęp:

(A) Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę zawartej w .....r.

(B) Pracodawca wyposażył stanowisko pracy Pracownika w legalne oprogramowanie komputerowe określone w metryce komputera, która stanowi załącznik do niniejszego porozumienia. Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania. Pracodawca zastrzega sobie możliwość stosowania oprogramowania do monitorowania i pobierania statystyk aktywności użytkownika z komputera służbowego, na którym pracuje zatrudniony. Pracodawca zastrzega sobie możliwość kontrolowania służbowej skrzynki pocztowej użytkownika, również w przypadku jego nieobecności.

(C) Pracownik korzysta z Oprogramowania oraz z zasobów informatycznych tylko i wyłącznie w związku z wykonywaniem obowiązków pracowniczych.

(D) Pracownik zobowiązuje się do nie ingerowania w system informatyczny bez wiedzy i pisemnej zgody Pracodawcy. Ingerencja w system informatyczny bez pisemnej zgody Pracodawcy będzie traktowana jako poważne naruszenie obowiązków pracowniczych wraz z konsekwencjami prawnymi z tego wynikającymi.

1) Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
2) Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny (tekst jednolity: Dz. U. z 2016, poz. 1137) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity: Dz. U. z 2016, poz. 666, z późn. zm.) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.
3) Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę łączącej Pracodawcę z Pracownikiem lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jednolity: Dz. U. z 2016 r. poz. 1666).
4) Niniejsze Porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron.
5) Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.

.....
podpis Pracownika

.....
podpis osoby upoważnionej do reprezentowania Pracodawcy

Użytkownik (właściciel)	Typ urządzenia	Nazwa producenta	Model	Numer seryjny	Kod PIN	Kod blokady	AV	Szyfrowanie	Zdalne wymazanie	Centralne zarządzanie

PROTOKÓŁ ZNISZCZENIA

sporządzony w dniu .....

przez komisję w składzie

1. ..... 3. .....

2. ..... 4. .....

w obecności: .....

Komisja stwierdziła że niżej wyszczególnione zostały komisyjnie zniszczone:

Lp.	Nazwa i opis przedmiotu	Nr seryjny	Ilość
1.			
2.			
3.			

a) inne uwagi i wnioski komisji:

.....

.....

.....

Podpisy komisji:

1. .....

2. .....

3. .....

4. .....

.....

podpis osoby odpowiedzialnej