Załącznik nr 1
do Zarządzenia nr 20/2019
Wójta Gminy Wydminy
z dnia 20 marca 2019 roku

Polityka ochrony danych w Urzędzie Gminy Wydminy

Wydminy 2019

Definicje

RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000).

Krajowe Ramy Interoperacyjności (KRI) – Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.).

ADO, Administrator Danych Osobowych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Dane szczególne – dane osobowe, o których mowa w art. 9 ust. 2 RODO – ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Jednostka – Urząd Gminy Wydminy,

Podmiot danych – osoba, której dane dotyczą, właściciel danych osobowych, w szczególności klient jednostki, jej pracownik lub współpracownik.

Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Osoba upoważniona – osoba wykonująca zadania polegające na przetwarzaniu, w formie tradycyjnej lub elektronicznej, danych osobowych na wyraźne polecenie ADO, która jest upoważniona do wykonywania tych czynności.

Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (strona trzecia: wszystkie podmioty za wyjątkiem: podmiotu danych, ADO, podmiotu przetwarzającego, osób upoważnionych).

Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, **nie są uznawane za odbiorców**.

Osoba nieuprawniona – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe z naruszeniem przepisów o ochronie danych osobowych, lub poza wyraźnym uprawnionym poleceniem ADO.

Osoba uprawniona – oznacza podmiot danych oraz ADO, podmiot przetwarzający, osoba upoważniona w zakresie, w jakim jest to zgodne z RODO.

Organ nadzorczy – oznacza Prezesa Urzędu Ochrony Danych Osobowych (PUODO).

Państwo trzecie – oznacza państwo nienależące do Unii Europejskiej, a po uwzględnieniu RODO w Porozumieniu o Europejskim Obszarze Gospodarczym, państwo trzecie będzie oznaczało państwo spoza Europejskiego Obszaru Gospodarczego.

Usługi społeczeństwa informacyjnego – każda usługa świadczona za wynagrodzeniem, na odległość, drogą elektroniczną, pozbawioną charakteru materialnego, realizowana na indywidualne żądanie usługobiorcy.

Wyraźne polecenie administratora – oznacza zlecenie zadań wymagających przetwarzania danych osobowych osobie fizycznej, niezależnie od formy prawnej, w szczególności poprzez zawarcie umowy o pracę, określenie zadań w ramach zakresu czynności lub dokumencie równoważnym, powierzenie pełnienia funkcji wraz z określeniem zadań lub zlecenie zadań w formie umowy cywilnoprawnej. W sytuacjach tego wymagających, ADO może wydać polecenie w formie ustnej.

Spis treści

1. Informacje ogólne 5
   1.1. Kontekst funkcjonowania 5
   1.2. Podstawowe cele zapewnienia bezpieczeństwa danych 5
   1.3. Administrator danych osobowych 5
   1.4. Podstawowe zasady przetwarzania danych osobowych 5
   1.5. Obszar przetwarzania danych 6
   1.6. Określenie wartości zasobów danych 6
   1.7. Role w systemie przetwarzania danych osobowych 7
2. Instrukcja gromadzenia i przetwarzania danych osobowych 7
   2.1. Instrukcja ogólna gromadzenia danych osobowych 7
   2.2. Uzyskanie zgody na przetwarzania danych osobowych 8
   2.3. Obowiązek informacyjny 8
   2.4. Publikacja danych osobowych 9
3. Instrukcja wypełniania praw podmiotów danych 10
   3.1. Zasady ogólne 10
4. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych 11
   4.1. Uwzględnianie ochrony danych w fazie projektowania 11
   4.2. Domyślna ochrona danych 12
5. Środki organizacyjne służące bezpieczeństwu danych osobowych 13
   5.1. Rejestr czynności przetwarzania danych osobowych i Rejestr kategorii przetwarzania danych osobowych 13
   5.2. Upoważnienia i uprawnienia do przetwarzania danych osobowych 13
   5.3. Obowiązki osób upoważnionych 15
   5.4. Powierzanie przetwarzania danych osobowych 16
   5.5. Udostępnianie danych osobowych 17
   5.6. Zapewnienie rozliczenia aktywów udostępnionych użytkownikowi 17
   5.7. Szkolenie pracowników 18
6. Środki techniczne służące bezpieczeństwu danych osobowych 18
   6.1. Niszczenie dokumentacji 18
   6.2. Likwidacja i serwis sprzętu komputerowego 18
   6.3. Zabezpieczenie budynku i pomieszczeń 19
   6.4. Monitoring wizyjny 20
   6.5. Zasady korzystania z portali internetowych oraz poczty elektronicznej 21
   6.6. Monitoring poczty elektronicznej oraz innych narzędzi pracy 21
   6.7. Zabezpieczenia przenośnych nośników danych 22

6.8. Zarządzanie oprogramowaniem i sprzętem teleinformatycznym 22
6.9. Tworzenie kopii zapasowych 24
6.10. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem 25
6.11. Bezpieczeństwo infrastruktury teleinformatycznej 25
7. Bezpieczeństwo 26
7.1. Analiza ryzyka 26
7.2. Ocena skutków przetwarzania dla ochrony danych 26
8. Incydenty bezpieczeństwa ochrony danych osobowych 27
8.1. Naruszenia 27
8.2. Postępowanie w przypadku zaistnienia naruszenia 27
8.3. Postępowanie wyjaśniające 28
8.4. Ewidencjonowanie incydentów, informowanie organu nadzorczego i podmiotu danych 28
8.5. Wsparcie podmiotów zewnętrznych 29
9. Inspektor Ochrony Danych 30
9.1. Wyznaczenie i pozycja IOD 30
9.2. Zadania Inspektora Ochrony Danych 31
10. Aktualizacja dokumentacji 31

1. Informacje ogólne

1.1. Kontekst funkcjonowania

Urząd Gminy Wydminy realizuje zadania określone ustawie z dnia 8 marca 1990 r. o samorządzie gminnym oraz innych przepisach szczególnych. Celem działania gminy jest zaspakajanie zbiorowych potrzeb wspólnoty i tworzenie warunków dla pełnego uczestnictwa mieszkańców w jej życiu. Do zakresu działania gminy należą wszystkie sprawy publiczne o znaczeniu lokalnym, niezastrzeżone ustawami na rzecz innych podmiotów. Gmina realizuje zadania własne, zlecone z zakresu administracji rządowej lub powierzone na podstawie innych instrumentów prawnych.

W zakresie realizowanych zadań pracownicy jednostki przetwarzają dane osobowe dla osiągnięcia nałożonych przepisami prawa celów.

1.2. Podstawowe cele zapewnienia bezpieczeństwa danych

Jednostka podejmuje działania mające na celu zapewnienie:

1. poufności danych – oznaczającej, że dane są udostępniane wyłącznie osobom i podmiotom do tego uprawnionym,
2. dostępności danych – oznaczającej, że dane dostępne są do wykorzystania na żądanie osoby uprawnionej w określonym czasie oraz zapewniony jest mechanizm pozwalający na odzyskiwanie danych w sytuacji ich utraty,
3. integralności danych – oznaczającej, że treść, zakres lub wartość danych nie została zmieniona w sposób nieuprawniony.

Omówione w niniejszej dokumentacji zasady dotyczą przetwarzania danych zarówno w formie tradycyjnej – papierowej, jak również przetwarzania danych w formie elektronicznej z użyciem wszelkich zasobów teleinformatycznych jednostki, w tym także służbowych urządzeń mobilnych takich jak tablety lub urządzenia typu smartphone oraz innych urządzeń korzystających z zasobów teleinformatycznych jednostki lub z nimi połączonych (np. urządzenia typu smart TV itp.)

1.3. Administrator danych osobowych

W zakresie przetwarzanych danych osobowych Administratorem danych osobowych jest Wójt Gminy Wydminy, który ustala cele i sposoby przetwarzania danych osobowych.

1.4. Podstawowe zasady przetwarzania danych osobowych

Administrator danych osobowych przetwarza dane osobowe z poszanowaniem następujących zasad:

1. **zgodności z prawem**, która oznacza przetwarzanie danych osobowych w oparciu o podstawę prawną i zgodnie z prawem,
2. **rzetelności i przejrzystości**, która oznacza transparentność procesów przetwarzania, w tym spełnianie praw podmiotów danych i przejrzyste informowanie o przetwarzaniu danych osobowych,
3. **ograniczenia celu przetwarzania**, która oznacza przetwarzanie wyłącznie takiej ilości danych osobowych i takiego rodzaju danych, które są niezbędne do osiągnięcia celu przetwarzania,

4. **ograniczenia przechowywania**, która oznacza przetwarzanie danych osobowych przez okres nie dłuższy niż jest to niezbędne do osiągnięcia celu przetwarzania,
5. **prawidłowości**, która oznacza podejmowanie działań w celu przetwarzania jedynie prawidłowych danych i ich uaktualniania,
6. **integralności i poufności**, która oznacza przyjęcie takich metod przetwarzania i zabezpieczenia, aby zapewnić ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, ujawnieniem osobom nieuprawnionym, oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,
7. **rozliczalności**, która oznacza możliwość wykazania spełnienia przestrzegania wyżej wymienionych zasad.

1.5. Obszar przetwarzania danych

Obszarem przetwarzania danych, w tym danych osobowych są wszystkie budynki i pomieszczenia jednostki, w których realizowana jest podstawowa działalność Administratora Danych Osobowych. Przetwarzanie danych osobowych może być wykonywane także w innych miejscach, w których Administrator Danych Osobowych realizuje swoje zadania.

1.6. Określenie wartości zasobów danych

Administrator Danych Osobowych przetwarza dane osobowe, w tym dane szczególne, w zakresie niezbędnym do realizacji wykonywanych zadań i spełnienia obowiązków nałożonych przepisami prawa.

Uwzględniając treść art. 24 i 32 oraz motywu 75 i 76 RODO Administrator Danych Osobowych określił następujące wartości przetwarzanych zasobów informacyjnych zawierających dane osobowe:

- **zasoby podstawowe** – dla zbiorów i zestawów danych, w których przetwarzane są dane osobowe zawierające podstawowe informacje o podmiotach danych, takie jak imię i nazwisko, dane teleadresowe, oraz informacje dotyczące rodzaju czynności podejmowanych przez ADO na rzecz tych osób,
  których ujawnienie powoduje **ryzyko** związane z dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą, pozbawieniem przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
- **zasoby wrażliwe** – dla zbiorów i zestawów danych, w których przetwarzane są dane osobowe, w tym dane szczególne, dane o wyrokach skazujących, naruszeniach prawa lub powiązanych środkach bezpieczeństwa, lub ilość i rodzaj przetwarzanych danych pozwala na tworzenie profili osobistych (np. dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się),
  których ujawnienie powoduje **wysokie ryzyko** związane z dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą, podmioty danych mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi.

Ponadto jako dane **wrażliwe** traktowane są wszelkie dane zawierające informacje konfiguracyjne systemów informatycznych, metody ich zabezpieczania, a także dane mogące znacznie wpłynąć na poziom bezpieczeństwa danych w jednostce.

1.7. Role w systemie przetwarzania danych osobowych

Administrator Danych Osobowych (ADO) – Wójt Gminy Wydminy,

Osoba upoważniona – osoba posiadająca upoważnienie do przetwarzania danych osobowych na zasadach określonych w pkt. 5.2. niniejszej dokumentacji,

Administrator Systemu Informatycznego (ASI) – osoba wyznaczona przez ADO do zapewnienia sprawnego działania systemów informatycznych. Zadania ADO realizowane są przy pomocy pracowników Urzędu oraz osób, którym ADO zlecił realizację zadań na podstawie umów cywilnoprawnych lub innych instrumentów prawnych.

Użytkownik Systemu Informatycznego (użytkownik) – osoba lub podmiot przetwarzający dane osobowe w systemie informatycznym, na wyraźne polecenie ADO, posiadająca własny, unikalny login do systemu.

Inspektor Ochrony Danych (IOD) – osoba fizyczna wyznaczona przez ADO do realizacji zadań określonych w art. 39 RODO i zgłoszony do organu nadzorczego w trybie ustalonym ustawą.

2. Instrukcja gromadzenia i przetwarzania danych osobowych

2.1. Instrukcja ogólna gromadzenia danych osobowych

1. Niedopuszczalne jest przetwarzanie danych osobowych bez podstawy prawnej wynikającej z art. 6 ust. 1, art. 9 ust. 2 lub art. 10 RODO.
2. W momencie gromadzenia danych osobowych osoba upoważniona, upewnia się, że:
    a. posiada aktualną podstawę prawną do przetwarzania danych osobowych wynikającą z art. 6 ust. 1, art. 9 ust. 2 lub art. 10 RODO,
    b. posiada konkretny cel przetwarzania danych osobowych wynikający z działalności ADO,
    c. zakres gromadzonych danych osobowych jest niezbędny dla celu ich przetwarzania lub wynika z obowiązujących przepisów prawa,
    d. ilość i rodzaj gromadzonych danych osobowych jest stosowny i adekwatny do celu przetwarzania lub jest zgodny z zakresem przewidzianym przepisami prawa,
    e. gromadzi prawidłowe (merytorycznie poprawne) dane osobowe,
    f. dane osobowe będą przetwarzane przez okres niezbędny do osiągnięcia celu przetwarzania lub przez okres wynikający z przepisów prawa, w tym z rozporządzenia Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67).
3. W przypadku, gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów, albo są zbędne do realizacji celu, dla którego zostały zebrane, osoba upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

4. Po osiągnięciu celu przetwarzania dane osobowe powinny być przechowywane w formie zanonimizowanej, tzn. uniemożliwiającej identyfikację podmiotów danych lub usunięte, z zastrzeżeniem przepisów prawa określających okres przechowywania danych kategorii dokumentacji, informacji lub danych osobowych.

2.2. Uzyskanie zgody na przetwarzania danych osobowych

1. Zgoda na przetwarzanie danych osobowych (o której mowa w art. 4 ust. 11 i art. 7 RODO) odbierana jest w szczególności w sytuacjach, w których przetwarzanie danych osobowych nie wynika z przepisów prawa i jest niezbędne dla osiągnięcia celu przetwarzania.
2. Przed rozpoczęciem zbierania zgody na przetwarzanie danych osobowych osoba upoważniona upewnia się, że:
    a. nie ma zastosowania inna przesłanka uprawniająca do przetwarzania danych osobowych, wynikająca z art. 6 ust. 1, art. 9 ust. 2 RODO,
    b. zgoda zbierana jest w konkretnie oznaczonym celu przetwarzania, a zakres gromadzonych danych służy osiągnięciu tego celu,
    c. cel przetwarzania opisany jest w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem i będzie zrozumiały dla osoby, która udziela zgody na przetwarzanie danych osobowych,
    d. udzielenie zgody jest dobrowolne, a jej nieudzielenie nie powoduje żadnych negatywnych konsekwencji wobec osoby udzielającej zgody,
    e. osoba udzielająca zgody jest poinformowana o możliwości jej wycofania w dowolnym momencie,
    f. przewidziano formę wycofania zgody, która nie jest trudniejsza (nie wymaga więcej działań) niż forma jej udzielenia,
    g. spełniony został obowiązek informacyjny zgodnie z pkt. 2.3. niniejszej dokumentacji.

2.3. Obowiązek informacyjny

1. W celu zapewnienia przejrzystości i rzetelności przetwarzania danych osobowych, w momencie zbierania danych osobowych od osób, których dane dotyczą, w tym od swoich pracowników, ADO ma obowiązek podać podmiotowi danych informacje wymagane obowiązującymi przepisami prawa, w szczególności wskazane w art. 13 RODO.
2. Obowiązek informacyjny powinien być realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. ADO spełnia obowiązek informacyjny wobec osób kontaktujących się z jednostką, w szczególności poprzez:
    a. umieszczenie informacji o przetwarzaniu danych osobowych na stronie internetowej jednostki oraz w Biuletynie Informacji Publicznej,
    b. umieszczenie informacji o przetwarzaniu danych osobowych na tablicy ogłoszeń w siedzibie jednostki,
    c. zamieszczanie linku do informacji, o której mowa w pkt. 2.3.3. lit. a, w stopce maili wysyłanych za pośrednictwem służbowej poczty elektronicznej lub w stopce pism przesyłanych innymi formami komunikacji elektronicznej,
    d. załączanie do pism stanowiących pierwszą formę kontaktu treści informacji o przetwarzaniu danych osobowych w formie drukowanej,
    e. podanie informacji o przetwarzaniu danych osobowych w formie drukowanej lub ustnej, w momencie pierwszego osobistego kontaktu.

4. ADO spełnia obowiązek informacyjny dotyczący wykonywania zdjęć lub rejestracji obrazu wideo podczas organizowanych przez siebie wydarzeń o charakterze otwartym (imprez otwartych) oraz publikacji tego materiału w przestrzeni publicznej, poprzez:
    a. umieszczenie informacji o przetwarzaniu danych na tablicy informacyjnej w widocznym miejscu na terenie imprezy lub przy wejściach na imprezę,
    b. odczytanie informacji podczas rozpoczęcia imprezy - o ile jest to możliwe,
    c. umieszczanie informacji o przetwarzaniu danych osobowych w treści regulaminu imprezy, jeżeli został przygotowany.
5. Informacja, o której mowa w pkt. 2.3.4. lit. a powinna zawierać co najmniej wskazanie ADO, podanie celu przetwarzania oraz wskazanie miejsca i podanie linku do strony gdzie można zapoznać się z pełną treścią informacji o przetwarzaniu danych w tym zakresie.
6. ADO spełnia obowiązek informacyjny dotyczący transmitowania i utrwalania za pomocą urządzeń rejestrujących obraz i dźwięk obrad (sesji) rady gminy, poprzez umieszczenie informacji przy wejściach do sali sesyjnej. Informacja powinna zawierać przynajmniej wskazanie ADO, informację o obowiązku prawnym wykonywania transmisji oraz wskazanie miejsca i linku do strony gdzie można zapoznać się z pełną treścią informacji o przetwarzaniu danych osobowych.
7. ADO lub wskazana przez niego osoba, przekazuje osobom wykonującym na jego rzecz zadania na podstawie umów o pracę, umów cywilnoprawnych lub innych instrumentów prawnych, informację o przetwarzaniu danych osobowych w momencie rozpoczęcia współpracy.
8. W przypadku zbierania danych osobowych od osób innych niż podmiot danych, ADO najpóźniej w ciągu miesiąca od dnia zebrania danych lub przy pierwszym kontakcie z podmiotem danych podaje mu informacje wskazane w art. 14 RODO.

Osoby realizujące:

- w zakresie przygotowania treści obowiązku informacyjnego – osoby upoważnione, gromadzące dane osobowe w ramach wykonywanych czynności po konsultacji z IOD,
- w zakresie spełnienia obowiązku informacyjnego podczas kontaktu z podmiotem danych – osoba upoważniona obsługująca podmiot danych, realizujących sprawę,
- w zakresie spełnienia obowiązku informacyjnego podczas gromadzenia danych w systemach informatycznych – ASI.

2.4. Publikacja danych osobowych

1. Dopuszczalne jest podawanie do publicznej wiadomości danych osobowych wyłącznie w sytuacjach oraz w zakresie przewidzianym przepisami obowiązującego prawa.
2. Dopuszczalność upublicznienia danych osobowych jest oceniana w szczególności przez:
    a. osoby upoważnione przygotowujące materiały i dokumenty do publikacji w Biuletynie Informacji Publicznej
    b. osoby upoważnione, w tym członków komisji, odpowiedzialnych za przygotowanie materiałów na sesje rady.
3. W sytuacjach, o których mowa w pkt. 2.4.2. przeprowadzona ocena uwzględnia legalność publikacji danych osobowych. W przypadku braku podstawy prawnej do publikacji danych osobowych lub w przypadku wynikającej z przepisów prawa konieczności zapewnienia prywatności osób fizycznych, osoba upoważniona dokonuje anonimizacji danych osobowych przed publikacją ocenianych dokumentów lub informacji.

3. Instrukcja wypełniania praw podmiotów danych

3.1. Zasady ogólne

1. ADO ułatwia podmiotowi danych wykonanie następujących praw wskazanych w rozdziale III RODO:
    a. prawa dostępu do danych,
    b. prawa do sprostowania danych,
    c. prawa do usunięcia danych,
    d. prawa do ograniczenia przetwarzania danych,
    e. obowiązku poinformowania podmiotu danych o sprostowaniu lub usunięciu danych lub ograniczenia ich przetwarzania,
    f. prawa do przenoszenia danych,
    g. prawa do sprzeciwu,
    h. prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu,
    i. zawiadomieniu podmiotu danych o naruszeniu ochrony danych osobowych.
2. Ułatwienie polega na:
    a. terminowym udzielaniu informacji i odpowiedzi na żądania wykonania przysługujących praw,
    b. komunikowaniu się z podmiotem danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. ADO realizuje prawa osób kierujących żądanie w sytuacji, gdy nie ma wątpliwości, co do tożsamości tej osoby oraz, że osoba ta występuje z żądaniem dotyczącym przetwarzania należących do niej danych osobowych.
4. W przypadku, gdy ADO nie przetwarza danych osobowych podmiotu kierującego żądanie, informuje o tym fakcie podmiot, nie później niż w terminie miesiąca od wpłynięcia żądania.
5. W sytuacji, w której ADO wykaże, że nie jest w stanie zidentyfikować osoby kierującej żądanie w ramach posiadanych możliwości, prosi tą osobę o podanie dodatkowych informacji pozwalających na potwierdzenie jej tożsamości.
6. Jeżeli osoba kierująca żądanie nie udzieli informacji wymaganych dla jej identyfikacji, ADO może odmówić wykonania praw.
7. Komunikacja z podmiotem danych w zakresie wykonania praw wymienionych odbywa się w formie pisemnej lub elektronicznej, zgodnie z żądaniem strony.
8. Na żądanie podmiotu danych, komunikacja w zakresie wykonania praw wymienionych oraz spełnienia obowiązku informacyjnego może być prowadzona ustnie, jeżeli tożsamość osoby będzie skutecznie potwierdzona innymi sposobami.
9. Na żądania osób odpowiedź udzielana jest bez zbędnej zwłoki, jednak nie później niż w terminie jednego miesiąca od dnia otrzymania żądania.
10. Ze względu na charakter żądania lub liczbę żądań, termin ich realizacji można przedłużyć o kolejne 2 miesiące. W terminie miesiąca od otrzymania żądania ADO informuje kierującego żądanie o przedłużeniu terminu i jego przyczynach.
11. Spełnienie obowiązku informacyjnego i innych praw podmiotów danych jest wolne od opłat.
12. Jeżeli żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na ustawiczny charakter, ADO ma prawo:
    a. pobrać opłatę za podjęcie działania,
    b. odmówić podjęcia działania.

13. Opłata za podjęcie działania zgodnego z żądaniem ustalana jest na podstawie administracyjnych kosztów udzielenia informacji, komunikacji lub podjęcia działań. Opłaty nie pobiera się za informowanie osób o naruszeniu danych osobowych.
14. O odmowie podjęcia działań ADO informuje osobę kierującą żądanie nie później niż w terminie miesiąca od otrzymania żądania.

Osoby realizujące:

- w zakresie realizacji praw i wolności podmiotów danych – ADO,
- w zakresie przygotowywania projektów pism i odpowiedzi – osoba upoważniona po konsultacji z IOD.

4. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

4.1. Uwzględnianie ochrony danych w fazie projektowania

1. ADO planując nowe zadania lub usługi zapewnia środki organizacyjne i techniczne służące bezpieczeństwu danych osobowych.
2. W fazie planowania nowych zadań lub usług ADO lub osoba upoważniona realizująca zadanie poddaje analizie:
    a. czy przetwarzanie danych osobowych będzie spełniało wymagania RODO, w szczególności czy zapewnione jest spełnienie podstawowych zasad przetwarzania danych osobowych, o których mowa w art. 5 RODO,
    b. czy możliwa będzie realizacja praw i wolności podmiotów danych, którzy będą korzystali z nowego zadania lub usługi,
    c. czy ADO jest w stanie zapewnić odpowiednie środki organizacyjne i techniczne, w tym pseudonimizację i minimalizację, zapewniające bezpieczeństwo przetwarzanych danych w kontekście zidentyfikowanych ryzyk.
3. Uwzględnienie ochrony danych osobowych w fazie projektowania należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

Osoby realizujące:

- w zakresie zapewnienia ochrony danych w fazie projektowania – ADO,
- w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoby upoważnione odpowiedzialne za przygotowanie zapytania ofertowego lub SIWZ, ASI.

4.2. Domyślna ochrona danych

1. W celu zapewnienia domyślnej ochrony danych osobowych ADO wdraża i stosuje odpowiednie środki techniczne i organizacyjne mające na celu minimalizację przetwarzania danych osobowych.
2. Minimalizacja osiągana jest poprzez przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten oznacza:
    a. minimalizację ilości danych osobowych,
    b. minimalizację zakresu danych osobowych,
    c. określenie niezbędnego czasu przetwarzania danych osobowych,
    d. określenie minimalnej grupy osób, które będą miały dostęp do tych danych,
    e. zapewnienie dostępności do danych w niezbędnym zakresie.
3. ADO stosuje środki organizacyjne i techniczne mające na celu zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych.
4. Uwzględnienie domyślnej ochrony danych osobowych należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

Osoby realizujące:

- w zakresie zapewnienia ochrony przetwarzanych lub planowanych do przetwarzania danych – ADO,
- w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoby upoważnione odpowiedzialne za przygotowanie zapytania ofertowego lub SIWZ, ASI.

5. Środki organizacyjne służące bezpieczeństwu danych osobowych

5.1. Rejestr czynności przetwarzania danych osobowych i Rejestr kategorii przetwarzania danych osobowych

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych (dalej RCP), który stanowi jednocześnie inwentarz wszystkich czynności przetwarzania wykonywanych przez ADO.
2. W RCP umieszczone są wszystkie zadania i usługi, które realizuje ADO.
3. RCP jest na bieżąco aktualizowany, w szczególności w sytuacjach:
    a. identyfikacji czynności, które nie zostały wcześniej wykazane w rejestrze czynności przetwarzania danych osobowych,
    b. wprowadzenia nowych usług,
    c. realizacji nowych zadań,
    d. zmiany przepisów mających wpływ na informacje zawarte w rejestrze,
    e. zmiany stanu faktycznego lub realizacji zaleceń IOD albo PUODO.
4. ADO prowadzi rejestr kategorii przetwarzania danych osobowych (dalej RKP) dla czynności przetwarzania, które zostały mu powierzone na podstawie umów powierzenia przetwarzania.
5. Rejestry prowadzone są w formie elektronicznej.
6. Każda osoba upoważniona ma obowiązek poinformować osobę wyznaczoną do prowadzenia rejestrów o wszystkich czynnościach przetwarzania wynikających z realizowanych zadań oraz o kategoriach czynności przetwarzania wynikających z zawartych umów powierzenia przetwarzania danych osobowych.
7. Osoba prowadząca rejestry, raz do roku dokonuje szczegółowego przeglądu zawartych w nim danych i przekazuje ADO oraz IOD informację o dokonanych zmianach lub o braku takiej konieczności. Informacja przekazywana jest w formie pisemnej, w tym elektronicznej.
8. Wzór RCP stanowi załącznik nr 5.1.1.
9. Wzór RKP stanowi załącznik nr 5.1.2.

Osoby realizujące:

- w zakresie prowadzenia i zapewnienia aktualizowania rejestrów – Sekretarz Gminy,
- w zakresie informowania o wszystkich czynnościach przetwarzania oraz o nowych zadaniach, usługach lub zmianach przepisów – osoby upoważnione.

5.2. Upoważnienia i uprawnienia do przetwarzania danych osobowych

Upoważnienia

1. Upoważnienia do przetwarzania danych osobowych (dalej upoważnienia) wydawane są wszystkim osobom przetwarzającym dane na wyraźne polecenie ADO.
2. Upoważnienie wydawane jest w momencie zlecenia realizacji zadania lub zadań wymagających przetwarzania danych osobowych niezależnie od formy tego zlecenia (zawarcia umowy o pracę, umowy cywilnoprawnej, powołania lub innego umocowania do działania w imieniu ADO).
3. Upoważnienia nie mogą być wydawane w zakresie szerszym niż wynika to z zakresu powierzanych zadań.
4. Inspektor Ochrony Danych przygotowuje treść upoważnienia i przekazuje je ADO do podpisu.

5. Upoważnienia są dokumentem wewnętrznym jednostki i wydawane są w jednym egzemplarzu w formie pisemnej.
6. Wzór upoważnienia stanowi załącznik nr 5.2.1.
7. Inspektor Ochrony Danych prowadzi na bieżąco, w formie elektronicznej, rejestr upoważnień do przetwarzania danych osobowych.
8. Wzór rejestru upoważnień stanowi załącznik nr 5.2.2.

Oświadczenia o zachowaniu poufności

9. Oświadczenia o zachowaniu poufności składane są przez:
    a. osoby upoważnione,
    b. osoby, które nie realizują zadań wymagających przetwarzania danych osobowych, jednak mogą mieć do nich dostęp (np. osoby sprzątające lub dokonujące prac gospodarczych w obszarze przetwarzania, w trakcie i po godzinach pracy jednostki).
10. Wzór oświadczenia stanowi załącznik nr 5.2.3.
11. Oświadczenia o zachowaniu poufności i upoważnienia przechowywane przez Inspektora Ochrony Danych.

Uprawnienia w systemach informatycznych

12. Po wydaniu upoważnienia i odebraniu oświadczenia o zachowaniu poufności, ASI nadaje stosowne uprawnienia do pracy w systemach informatycznych.
13. Uprawnienia do systemów informatycznych nie mogą być nadawane w zakresie szerszym niż zakres powierzonych osobie do realizacji zadań.
14. ASI nadaje osobie upoważnionej:
    a. indywidualny login i hasło,
    b. poziom uprawnień w systemie, zgodny z poleceniem ADO lub przełożonego osoby upoważnionej.
15. Upoważnienia i uprawnienia nadawane są na okres zgodny z umową o pracę, umową cywilnoprawną lub innym instrumentem prawnym, na podstawie którego zlecono realizację zadania.
16. Zablokowanie konta użytkownika lub zmiana uprawnień w systemie informatycznym wykonywane są na polecenie ADO lub bezpośredniego przełożonego osoby upoważnionej niezwłocznie w sytuacji:
    a. wcześniejszego zakończenia obowiązywania umowy lub innego instrumentu prawnego, na podstawie którego zlecono realizację zadań,
    b. zmiany zakresu zadań.
17. ASI zapewnia ewidencję użytkowników i poziomów ich uprawnień w systemach informatycznych. Ewidencja prowadzona jest w każdym z systemów informatycznych, a w przypadku systemów, w których ewidencja użytkowników nie jest możliwa, ASI prowadzi ewidencję w formie elektronicznej.
18. Wzór ewidencji użytkowników i uprawnień stanowi załącznik nr 5.2.4.
19. Nie rzadziej niż raz na rok, ASI dokonuje okresowego przeglądu kont użytkowników w celu weryfikacji prawidłowości i adekwatności nadanych w systemach informatycznych uprawnień oraz w celu dokonania ewentualnych zmian w tym zakresie.
20. Z przeprowadzonych czynności ASI sporządza protokół.
21. Wzór protokołu weryfikacji uprawnień stanowi załącznik nr 5.2.5.

Osoby realizujące:

– w zakresie nadania upoważnienia – ADO,

- w zakresie gromadzenia upoważnień i oświadczeń o zachowaniu poufności, a także prowadzenia ewidencji upoważnień – Inspektor Ochrony Danych,
- w zakresie nadawania uprawnień w systemach informatycznych oraz zapewnienia aktualnej ewidencji uprawnień – ASI.

5.3. Obowiązki osób upoważnionych

1. Zbierając dane osobowe od osób, których dane dotyczą osoba upoważniona spełnia obowiązek informacyjny.
2. W celu ograniczenia dostępu do danych osobowych osób nieuprawnionych, wszystkie osoby przetwarzające dane osobowe na polecenie ADO:
    a. przetwarzają dane w zakresie zadań powierzonych im do realizacji zgodnie z otrzymanymi upoważnieniami,
    b. dbają o zapewnienie poufności rozmów prowadzonych z klientami w ten sposób, żeby treść tych rozmów nie mogła być usłyszana przez osoby nieuprawnione,
    c. nie dopuszczają do dostępu do danych osobowych i metod ich zabezpieczania przez osoby nieuprawnione, w szczególności poprzez:
        - zakrywanie treści dokumentów w taki sposób, aby osoby obsługiwane nie mogły zapoznać się z ich treścią,
        - bieżącą pracę tylko z dokumentami niezbędnymi do wykonania aktualnego zadania oraz odkładania dokumentów do przeznaczonych do tego segregatorów, szaf lub szuflad po zakończeniu pracy (zasada czystego biurka),
        - uniemożliwienie odczytywania przez osoby nieuprawnione treści wyświetlanych na monitorze,
        - niszczenie dokumentów, ich projektów lub kopii w przeznaczonych do tego niszczarkach,
        - nie wynoszenie dokumentów zawierających dane osobowe poza siedzibę jednostki,
        - nieudostępnianie dokumentów zawierających dane osobowe osobom nieuprawnionym (również realizując obowiązek wynikający z ustawy o dostępie do informacji publicznej),
        - niepozostawianie bez nadzoru osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe,
        - zamykanie pomieszczeń i niepozostawianie w drzwiach klucza, w sytuacji, gdy w pomieszczeniu nie ma osoby upoważnionej,
        - niezwłoczne odbieranie dokumentów po ich wydrukowaniu,
    d. zapewniają bezpieczeństwo wykorzystywanych systemów informatycznych w szczególności poprzez:
        - zachowanie w poufności identyfikatorów i haseł dostępowych do systemów informatycznych, w tym nieudostępnianie tych elementów innym osobom upoważnionym i osobom nieuprawnionym, nieprzechowywanie zapisanych identyfikatorów i haseł w obszarze stanowiska pracy (ewentualne przechowywanie zapisanych identyfikatorów i haseł dopuszczalne jest w zabezpieczonych kopertach w szafie pancernej, sejfie lub menadżerze haseł), niedopuszczenie do możliwości odczytania wprowadzanego do systemu hasła przez osoby nieuprawnione,
        - zmianę hasła nadanego przez ASI,

- dokonywanie samodzielnie, bez wezwania, zmian wszystkich wykorzystywanych haseł co 90 dni, hasła powinny być tworzone zgodnie z pkt. 6.10.5 niniejszej dokumentacji,
- niewprowadzanie zmian w udostępnionych systemach informatycznych bez wiedzy osoby odpowiedzialnej za ich funkcjonowanie,
- nieinstalowanie jakichkolwiek programów bez wiedzy osoby odpowiedzialnej za prawidłowe funkcjonowanie systemów informatycznych lub danego urządzenia,
- nieudzielanie zdalnego dostępu do systemów informatycznych osobom nieuprawnionym,
- korzystanie wyłącznie z programów udostępnionych przez ADO w celu realizacji zadań,
- korzystanie wyłącznie z zaufanych serwisów internetowych w celu realizacji zadań,
- niekorzystanie z portali społecznościowych, poczty elektronicznej i innych serwisów internetowych w celach prywatnych,
- korzystanie wyłącznie z zaufanych nośników danych udostępnionych przez ADO,
- dbanie o powierzony do użytkowania sprzęt informatyczny, w tym nieudostępnianie go osobom nieuprawnionym (także osobom znanym i członkom rodzin) oraz niepozostawianie powierzonego sprzętu w miejscach dostępnych osobom nieuprawnionym,
- użytkowanie powierzonego sprzętu komputerowego, urządzeń mobilnych i przenośnych nośników danych poza siedzibą jednostki w sposób zapewniający poufność danych, a także niepozostawianie tych urządzeń bez nadzoru,
- zwrot powierzonego sprzętu na żądanie ADO,
- stosowanie się do zaleceń osoby odpowiedzialnej za prawidłowe funkcjonowanie systemu informatycznego.

3. Za naruszenia w zakresie bezpieczeństwa informacji określone w niniejszym dokumencie pracownicy ponoszą odpowiedzialność dyscyplinarną zgodnie z zasadami przyjętymi w jednostce.

5.4. Powierzanie przetwarzania danych osobowych

1. ADO w sytuacjach, w których powierza przetwarzanie danych osobowych innemu podmiotowi zawiera z nim stosowną umowę powierzenia.
2. Powierzenie następuje, gdy podmiot trzeci będzie przetwarzał dane osobowe w imieniu ADO (np. umowy serwisowe sprzętu zawierającego dane osobowe, dostęp podmiotów zewnętrznych do baz danych ADO w ramach tzw. helpdesk, zlecanie realizacji zadań wymagających przetwarzania danych osobowych podmiotom zewnętrznym).
3. Osoby odpowiedzialne za dokonywanie zakupu dostaw i usług w ramach których będą przetwarzane przez podmiot trzeci dane osobowe (w tym na podstawie regulacji wewnętrznych zakresie zamówień i prawa zamówień publicznych), na etapie wyboru dostawcy zapewniają, że wybrany podmiot będzie zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO.
4. Dopuszczalne jest powierzenie przetwarzania danych osobowych na podstawie innych niż umowa powierzenia instrumentów prawnych (np. porozumienie, akt powołania komisji lub treść statutu, w ramach którego tworzona jest jednostka wykonująca zadania w imieniu ADO).

W tej sytuacji treść innego instrumentu prawnego musi zawierać co najmniej wszystkie elementy wymagane RODO lub zawierać treść zgodną ze wzorem umowy powierzenia.

5. Wzór umowy powierzenia stanowi załącznik nr 5.4.1.

Osoby realizujące:

- w zakresie nadzoru w ramach zawieranych umów – ADO, osoby uprawnione do zawierania umów w imieniu ADO,
- w zakresie zapewnienia bieżącego informowania o konieczności powierzenia przetwarzania danych osobowych – osoby upoważnione przygotowujące treść umowy,
- w zakresie ujęcia treści powierzenia przetwarzania w umowach lub innych instrumentach prawnych – osoby odpowiedzialne za przygotowanie i sprawdzenie umów i innych instrumentów prawnych, w tym radca prawny.

5.5. Udostępnianie danych osobowych

1. ADO i osoby upoważnione w ramach realizowanych przez siebie zadań uprawnieni są do udostępniania danych osobowych.
2. Dane osobowe udostępniane są tylko odbiorcom uprawnionym do ich otrzymania:
    a. na podstawie wyraźnej zgody podmiotu danych,
    b. na podstawie obowiązujących przepisów prawa.
3. Dane osobowe udostępniane są:
    a. na podstawie żądania podmiotu danych,
    b. na podstawie pisemnego wniosku od odbiorcy uprawnionego przepisami prawa do otrzymywania danych osobowych,
    c. na podstawie umowy z odbiorcą, w ramach której istnieje konieczność udostępnienia danych i zapewnione są środki ochrony praw i wolności podmiotów danych.
4. Dane osobowe udostępniane są po potwierdzeniu tożsamości wnioskodawcy i jego uprawnienia do otrzymania żądanych danych.
5. Odmawia się udostępnienia danych osobowych w przypadku, gdy spowodowałoby to naruszenie praw i wolności podmiotu danych lub osób trzecich i prawa te są nadrzędne w stosunku do uprawnień odbiorcy. W tym zakresie ADO podejmuje decyzję na podstawie przeprowadzonej analizy i uzasadnienia odmowy zaproponowanej przez osobę upoważnioną.
6. ADO zapewnia ewidencję udostępnień danych osobowych zgodnie z zasadami ewidencjonowania korespondencji przychodzącej i ewidencji prowadzonych spraw, poprzez wpisanie w treści prowadzonej ewidencji informacji o udostępnianiu.

Osoby realizujące:

- w zakresie weryfikacji prawidłowości wniosku i propozycji odpowiedzi – ADO, osoba upoważniona,
- w zakresie udostępniania danych osobowych – ADO lub inna osoba uprawniona do podpisywania pism w imieniu ADO,
- w zakresie prowadzenia ewidencji – osoby upoważnione w zakresie prowadzonych spraw.

5.6. Zapewnienie rozliczenia aktywów udostępnionych użytkownikowi

1. ADO zapewnia ewidencjonowanie udostępnionych pracownikowi urządzeń, systemów informatycznych i innych zasobów służących realizacji zadań służbowych, w tym poprzez prowadzenie ustalonych niniejszą dokumentacją:

a. ewidencji upoważnień,
b. ewidencji przenośnych nośników danych,
c. ewidencji sprzętu i oprogramowania.

2. W sytuacji zakończenia współpracy z użytkownikiem, ASI dokonuje adnotacji na stosowanej w jednostce karcie obiegowej potwierdzającej zwrot wszystkich udostępnionych użytkownikowi urządzeń oraz cofnięcie uprawnień we wszystkich systemach informatycznych.

Osoby realizujące:

– w zakresie potwierdzenia zwrotu wszystkich udostępnionych użytkownikowi urządzeń oraz cofnięcie uprawnień we wszystkich systemach informatycznych – ASI,

5.7. Szkolenie pracowników

1. ADO zapewnia regularne szkolenie pracowników w zakresie:
   a. zagrożeń związanych z bezpieczeństwem informacji,
   b. skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej z tym związanej,
   c. zapewnienia zgodnego z prawem przetwarzania i ochrony danych osobowych.
2. ADO zapewnia regularne szkolenia ASI i innym pracownikom zaangażowanym w proces zapewnienia bezpieczeństwa informacji, w tym danych osobowych w zakresie stosowanych środków zapewniających bezpieczeństwo informacji, w tym stosowanych urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.
3. Szkolenia, o których mowa w pkt. 1 powinny być prowadzone przez ASI, IOD lub podmiot zewnętrzny nie rzadziej niż raz na rok.
4. Szkolenia, o których mowa w pkt. 2 powinny być prowadzone przez podmioty zewnętrzne zapewniające wysokie standardy wiedzy oraz adekwatne do tematu szkolenia doświadczenie.

6. Środki techniczne służące bezpieczeństwu danych osobowych

6.1. Niszczenie dokumentacji

1. ADO zapewnia osobom upoważnionym odpowiednie urządzenia służące niszczeniu dokumentów.
2. W sytuacji konieczności zniszczenia dużej ilości dokumentacji, czynność ta może zostać zlecona podmiotowi zewnętrznemu z zachowaniem zasad powierzania przetwarzania danych osobowych (pkt. 5.5.).
3. Niedopuszczalne jest wyrzucanie do kosza dokumentów zawierających dane osobowe.

Osoby realizujące:

– W zakresie zapewnienia zasobów – ADO,
– w zakresie niszczenia dokumentów w niszczarkach – osoby upoważnione.

6.2. Likwidacja i serwis sprzętu komputerowego

1. ASI zapewnia konserwację sprzętu zgodnie z zaleceniami producenta.
2. Wszelkie naprawy sprzętu muszą być dokonywane pod nadzorem ASI.

3. W przypadku wykonywania prac serwisowych sprzętu komputerowego i oprogramowania ADO zapewnia zawarcie stosownej umowy zawierającej niezbędne wymagania dla bezpieczeństwa powierzanych danych, w tym danych osobowych, w szczególności uwzględniając:
    a. zobowiązanie wykonawcy do zachowania w poufności wszelkich danych i metod ich zabezpieczania,
    b. zobowiązania do wykorzystania przekazanych danych i metod ich zabezpieczania wyłącznie dla celów związanych z realizacją umowy serwisowej,
    c. zakazie lub warunkach przekazania lub ujawnienia podmiotom trzecim przekazanych danych i metod ich zabezpieczania,
    d. zobowiązanie wykonawcy do niekopiowania, niepowielania i nierozpowszechniania przekazanych danych i metod ich zabezpieczania, za wyjątkiem przypadków, gdy jest to potrzebne w celu realizacji umowy,
    e. określenie zasad przekazania ADO wszelkich kopii danych wykonanych przez wykonawcę, które były niezbędne w celu wykonania umowy.
4. Serwis sprzętu i oprogramowania może być wykonywany wyłącznie przez podmioty gwarantujące zastosowanie odpowiednich środków technicznych i organizacyjnych w celu ochrony danych w tym danych osobowych.
5. ASI zapewnia niszczenie sprzętu komputerowego w sposób uniemożliwiający odczytanie danych osobowych.
6. Przed oddaniem sprzętu do zniszczenia wyspecjalizowanym podmiotom, ASI zapewnia usunięcie wszelkich danych z pamięci tych urządzeń.
7. W sytuacji sprzedaży sprzętu komputerowego wycofywanego z użytku, ASI zapewnia usunięcie wszelkich danych z pamięci tych urządzeń.
8. Do usunięcia danych należy wykorzystać przeznaczone do tego programy zapewniające wysoki poziom skuteczności, które w szczególności wykorzystują wielokrotne nadpisywanie danych wartościami losowymi i wartościami zerowymi.

Osoby realizujące:

- w zakresie zawarcia umowy z podmiotami serwisującymi sprzęt komputerowy – ASI, osoby odpowiedzialne za przygotowanie treści umów,
- w zakresie zapewnienia usunięcia danych z likwidowanego sprzętu – ASI.

6.3. Zabezpieczenie budynku i pomieszczeń

1. ADO zapewnia możliwość zamykania i zabezpieczania obszarów przetwarzania w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych.
2. ADO wyznacza osoby odpowiedzialne za otworzenie i zamknięcie swojej siedziby oraz mieszczących się poza siedzibą pomieszczeń i budynków, w których realizowane są zadania ADO.
3. Wzór wyznaczenia osób odpowiedzialnych za otworzenie i zamknięcie budynków ADO stanowi zał. nr 6.3.1.
4. W przypadku korzystania z systemu alarmowego ADO wyznacza osoby które mają dostęp do kodów aktywujących i dezaktywujących system alarmowy na podstawie umowy zawartej z agencją ochrony mienia. Zawarta umowa zapewnia odrębne kody dla każdej z wyznaczonych osób.
5. Osoby wyznaczone odpowiedzialne są za:

a. wykorzystywanie udostępnionych kluczy zgodnie z przeznaczeniem w godzinach wyznaczonych przez ADO,
b. staranne zamknięcie wejścia do budynku,
c. sprawdzenia czy nie doszło do próby włamania i niezwłoczne poinformowanie o takim zdarzeniu,
d. aktywację i dezaktywację kodu do systemu alarmowego.

6. ADO wyznacza miejsce, w którym przechowywane są klucze do pomieszczeń i zapewnia ich należyte zabezpieczenie przed dostępem osób nieuprawnionych.
7. Niedopuszczalne jest posiadanie przez osoby inne niż wyznaczone zgodnie z pkt. 6.2.2 kopii kluczy do budynku ADO i pomieszczeń, w których przetwarzane są dane osobowe, poza osobami do tego wyznaczonymi.
8. Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających w szczególności na:
   a. zabezpieczeniu dokumentacji,
   b. zabezpieczeniu pieczęci,
   c. wylogowania się ze wszystkich systemów informatycznych,
   d. zabezpieczeniu komputerów,
   e. zabezpieczeniu nośników informacji,
   f. wyłączeniu urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp,
   g. zamknięciu okien i drzwi,
   h. pozostawieniu kluczy od pomieszczeń biurowych w wyznaczonym pomieszczeniu/miejscu.
9. Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu osób upoważnionych, które ponoszą pełną odpowiedzialność za ich zabezpieczenie przed dostępem osób nieuprawnionych.

osoby realizujące:

- w zakresie dbałości o udostępnione zasoby i uporządkowanie stanowiska pracy – osoby upoważnione,
- w zakresie zachowania poufności w zakresie kodów dostępowych – osoby którym przydzielono kody,
- w zakresie dbałości o klucze do budynku – osoby wyznaczone do tego zadania.

6.4. Monitoring wizyjny

1. ADO może prowadzić monitoring wizyjny terenu swojej siedziby i terenu wokół niej w celu zapewnienia bezpieczeństwa pracowników i osób przebywających na terenie ADO oraz w celu zapewnienia ochrony mienia. Cele, zakres oraz sposób zastosowania monitoringu wizyjnego ustala się w obowiązującym ADO regulaminie pracy.
2. ADO może prowadzić monitoring wizyjny na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy i na terenie wokół takich nieruchomości i obiektów budowalnych w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej.
3. Dane zapisu z monitoringu wizyjnego przechowywane są nie dłużej niż 3 miesiące lub do czasu zakończenia prawomocnego postepowania, w którym nagrania te stanowią lub mogą stanowić dowód.

4. W celu zapewnienia przejrzystości i rzetelności przetwarzania danych osobowych umieszcza przy każdym wejściu do monitorowanego obszaru lub budynku tabliczkę informującą o tym fakcie. Tabliczka powinna zawierać co najmniej oznaczenie ADO i cel przetwarzania danych. Obowiązek informacyjny w zakresie monitoringu umieszczany jest na tablicy ogłoszeń ADO.
5. Przetwarzanie danych osobowych w systemie monitoringu wizyjnego podlega wszystkim zasadom opisanym w niniejszym dokumencie.

6.5. Zasady korzystania z portali internetowych oraz poczty elektronicznej

1. Na służbowych komputerach, a także na innych urządzeniach dopuszczonych do pracy w sieci teleinformatycznej ADO, zabrania się korzystania ze stron internetowych do celów prywatnych, w tym do korzystania z portali społecznościowych i rozrywkowych.
2. ADO zapewnia dostęp do kont poczty elektronicznej w domenie, którą zarządza lub u dostawcy usług, który zapewnia możliwość zawarcia umowy powierzenia przetwarzania danych.
3. Niedopuszczalne jest rejestrowanie kont służących realizacji zadań w publicznie dostępnych domenach.
4. Niedopuszczalne jest wykorzystywanie do celów służbowych prywatnych kont poczty elektronicznej osób upoważnionych.
5. Niedopuszczalne jest wykorzystywanie do celów prywatnych służbowych kont poczty elektronicznej osób upoważnionych.
6. ADO zapewnia osobom upoważnionym możliwość oznaczania niechcianej poczty jako spam.
7. Osoba upoważniona odpowiedzialna jest za korzystanie z poczty elektronicznej, w tym każdorazowe weryfikowanie nadawcy i nieotwieranie załączników pochodzących z nieznanego źródła.
8. W przypadku przesyłania drogą mailową, pomiędzy osobami upoważnionymi lub przesyłanie odbiorcom danych, danych osobowych o wartości średniej lub wysokiej konieczne jest ich skompresowanie i zaszyfrowanie zaufanym oprogramowaniem i nadanie skompresowanemu plikowi bezpiecznego hasła (zgodnie z pkt. 6.10.5). Hasło powinno zostać przekazane adresatowi innym środkiem komunikacji niż droga mailowa.

Osoby realizujące:
- w zakresie zapewnienia niezbędnych zasobów – ADO,
- w zakresie realizacji obowiązków – osoby upoważnione,
- w zakresie utworzenia kont pocztowych – ASI.

6.6. Monitoring poczty elektronicznej oraz innych narzędzi pracy

1. ADO może monitorować pocztę elektroniczną oraz inne narzędzia udostępnione pracownikom do realizacji zadań w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych narzędzi pracy.
2. Okres przechowywania danych zgromadzonych za pomocą monitoringu nie może być dłuższy niż okres przedawnienia wyrządzenia szkody przez pracownika wynikający z przepisów prawa.
3. W przypadku prowadzenia monitoringu ruchu sieciowego oraz pracy na komputerach, ADO informuje o tym fakcie wszystkie osoby, których to dotyczy.

4. Prowadzenie monitoringu nie może naruszać tajemnicy korespondencji oraz innych praw osób.
5. Korzystanie ze zgromadzonych danych dopuszczalne jest wyłącznie za zgodą ADO.
6. Cele, zakres oraz sposób zastosowania monitoringu poczty elektronicznej oraz innych narzędzi udostępnianych pracownikom do realizacji zadań ustala się w obowiązującym ADO regulaminie pracy.

Osoby realizujące:
- w zakresie zapewnienia niezbędnych zasobów – ADO,
- w zakresie zapewnienia tajemnicy korespondencji oraz nieudostępniania informacji z systemu monitorującego bez wyraźnego polecenia ADO – ASI.

6.7. Zabezpieczenia przenośnych nośników danych

1. W celu zabezpieczenia zasobów dozwolone jest używanie wyłącznie nośników danych udostępnionych przez ADO, które są zabezpieczone oprogramowaniem szyfrującym lub szyfrowaniem sprzętowym.
2. ASI prowadzi ewidencję przenośnych nośników danych dopuszczonych do użytku w jednostce.
3. Wzór ewidencji przenośnych nośników danych stanowi załącznik nr 6.7.1.
4. W przypadku, gdy na nośniku danych przechowywane są dane wrażliwe określone w pkt. 1.6 nośnik danych oznaczany jest kolorem czerwonym.
5. Wszystkie nośniki oznaczone jako wrażliwe powinny być zabezpieczane przed dostępem osób nieuprawnionych i przechowywane ze szczególną starannością.

Osoby realizujące:
- w zakresie zapewnienia niezbędnych zasobów – ADO,
- w zakresie instalacji oprogramowania szyfrującego – ASI,
- w zakresie korzystania wyłącznie z udostępnionych przez ADO nośników danych – osoby upoważnione.

6.8. Zarządzanie oprogramowaniem i sprzętem teleinformatycznym

1. ADO wyznacza osobę odpowiedzialną za instalację i aktualizację oprogramowania oraz za zapewnienie sprawnego funkcjonowania systemu informatycznego (ASI).
2. Do zadań ASI należy w szczególności:
    a. monitorowanie oraz zapewnianie ciągłości działania systemów informatycznych,
    b. monitorowanie ruchu sieciowego poprzez wykorzystanie stosowanych urządzeń lub oprogramowania,
    c. zapewnienie monitorowania dostępu do informacji, poprzez gromadzenie logów systemowych i ich okresowa weryfikacja pod kątem rozliczalności pracy w systemach pracowników zgodnie z wymaganiami KRI,
    d. utrzymywanie, konfigurowanie i monitorowanie wydajności systemów informatycznych,
    e. instalacja i konfiguracja sprzętu i aplikacji,
    f. administracja, w tym aktualizacja oprogramowania systemowego w celu zachowania bezpieczeństwa i integralności systemów informatycznych oraz zabezpieczenia

danych, w szczególności danych osobowych przed bezprawnym dostępem osób trzecich,
   g. konserwacja oprogramowania i systemów informatycznych,
   h. współpraca z licencjodawcami i innymi dostawcami oprogramowania,
   i. zapewnienie tworzenia kopii zapasowych danych, w tym danych osobowych oraz zarządzanie nimi zgodnie z ustalonym harmonogramem,
   j. dbanie o aktualność oprogramowania antywirusowego,
   k. zapewnienie mechanizmów zdalnego blokowania urządzeń mobilnych i komputerów przenośnych lub usuwania danych z tych urządzeń,
   l. zapewnienie utylizacji sprzętu komputerowego w sposób uniemożliwiający odzyskanie danych z pamięci tych urządzeń.
3. W przypadku wyznaczenia osoby odpowiedzialnej za ww. czynności niebędącej pracownikiem ADO należy zapewnić spełnienie zasad powierzania przetwarzania danych osobowych.
4. Powierzenie zadań związanych z instalacją i aktualizacją oprogramowania oraz zapewnieniem sprawnego funkcjonowania systemu informatycznego odbywa się poprzez dokonanie odpowiedniego zapisu w zakresie czynności pracownika ADO lub zapisu w zawartej umowie cywilnoprawnej.
5. Do użytkowania może być dopuszczone tylko oprogramowanie, które posiada licencję lub dokument równoważny upoważniający do zainstalowania i użytkowania.
6. Dopuszczalne jest instalowanie i/lub użytkowanie oprogramowania:
   a. dla którego jednostka posiada aktualną licencję lub inne prawa użytkowania,
   b. wyłącznie służącego realizacji celów służbowych.
7. Osoby upoważnione mogą korzystać wyłącznie z kont z uprawnieniami użytkownika.
8. ASI korzysta z konta o uprawnieniach administracyjnych tylko w sytuacji wykonywania zadań związanych z instalacją i aktualizacją oprogramowania oraz zapewnieniem sprawnego funkcjonowania systemu informatycznego. W przypadku wykonywania innych zadań zobowiązany jest korzystać z konta o uprawnieniach użytkownika.
9. Dopuszczalne jest stosowanie zdalnego dostępu do komputerów będących w zasobach ADO w ramach pomocy technicznej pod warunkiem zapewnienia szyfrowanego połączenia i innych mechanizmów zapewniających nienaruszalność praw i wolności podmiotów danych oraz zawarcia zapisów o szczegółowej realizacji tego wymogu w umowie powierzenia przetwarzania danych osobowych lub umowy realizacji usługi.
10. ASI w miarę możliwości technicznych:
    a. stosuje mechanizmy zapewniające możliwość podłączenia do infrastruktury informatycznej jednostki wyłącznie zaufane urządzenia,
    b. blokuje możliwość podłączania do infrastruktury informatycznej jednostki urządzeń niezaufanych lub niemożliwych do zidentyfikowania.
11. Osoba odpowiedzialna za zapewnienie sprawnego działania systemów informatycznych prowadzi ewidencję wykorzystywanego u ADO sprzętu i oprogramowania. Ewidencja prowadzona jest na bieżąco niezależnie od prowadzonej ewidencji księgowej środków trwałych, pozostałych środków trwałych oraz wartości niematerialnych i prawnych.
12. Ewidencja prowadzona jest w formie elektronicznej. Dopuszczalne jest prowadzenie ewidencji sprzętu i oprogramowania poprzez wykorzystanie zaufanego oprogramowania audytowego.
13. Wzór ewidencji sprzętu komputerowego i oprogramowania stanowi załącznik nr 6.8.1.

14. Osoba odpowiedzialna za zapewnienie sprawnego działania systemów informatycznych prowadzi ewidencję wykorzystywanych mechanizmów bezpieczeństwa systemów teleinformatycznych.
15. Wzór ewidencji wykorzystywanych mechanizmów bezpieczeństwa systemów teleinformatycznych stanowi załącznik nr 6.8.2.

6.9. Tworzenie kopii zapasowych

1. Kopie zapasowe, o których mowa w pkt. 6.8.2.i wykonywane są zgodnie z przygotowanym przez ASI harmonogramem.
2. Harmonogram, zgodnie z potrzebami jednostki, uwzględnia tworzenie kopii zapasowych w szczególności:
    a. danych roboczych użytkowników,
    b. baz danych zlokalizowanych na serwerach, na jednostkach roboczych oraz w chmurach obliczeniowych jeżeli są wykorzystywane,
    c. systemów operacyjnych serwerów,
    d. danych przechowywanych na urządzeniach mobilnych,
    e. dzienników zdarzeń (logów systemowych) wszystkich istotnych systemów bazodanowych,
    f. bieżące potrzeby jednostki z uwzględnieniem wyników przeprowadzonych analiz ryzyka.
3. Kopie zapasowe wykonywane są także dla danych przetwarzanych na urządzeniach mobilnych będących w zasobach jednostki.
4. Poza harmonogramem kopie zapasowe wykonywane są w szczególności przed przeprowadzeniem istotnej zmiany konfiguracyjnej systemu lub po jej przeprowadzeniu w przypadkach aktualizacji oprogramowania, zmian praw dostępu, zmian konfiguracji.
5. Wzór harmonogramu tworzenia kopii zapasowych stanowi załącznik nr 6.9.1.
6. Zaleca się przechowywanie nośników danych, na których zapisane są kopie zapasowe w innym pomieszczeniu lub budynku niż źródło danych.
7. W zakresie spełnienia wymagań KRI należy zapewnić możliwość przechowywania przez okres dwóch lat zapisów dzienników systemów obejmujących działania użytkowników lub obiektów systemowych polegające na dostępie do:
    a. systemu z uprawnieniami administracyjnymi,
    b. konfiguracji systemu, w tym konfiguracji zabezpieczeń,
    c. przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Osoby realizujące:

- w zakresie zapewnienia niezbędnych zasobów – ADO,
- w zakresie tworzenia harmonogramu tworzenia kopii zapasowych, prowadzenia ewidencji wykorzystywanego oprogramowania oraz wykorzystywanych mechanizmów bezpieczeństwa systemów teleinformatycznych, zapewnienia zgodnej z wymaganiami niniejszej dokumentacji pracy i konfiguracji systemów informatycznych, w tym zgłaszania ADO niezbędnych potrzeb – ASI.

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

1. Podstawową metodą uwierzytelniania użytkowników w systemie informatycznym są identyfikator użytkownika i hasło.
2. Identyfikator użytkownika nadawany jest przez ASI zgodnie z wymogami systemu.
3. Hasło początkowe nadaje ASI, a następnie przekazuje je użytkownikowi po zweryfikowaniu jego tożsamości. Niedopuszczalne jest w szczególności:
    a. przekazywanie hasła za pośrednictwem osób trzecich,
    b. przekazywanie hasła telefonicznie lub za pomocą poczty elektronicznej.
4. Osoba upoważniona zmienia hasło otrzymane od ASI po pierwszym zalogowaniu.
5. Niezależnie od wartości zasobu danych osobowych przetwarzanych w danym systemie, stosowane hasła powinny zawierać co najmniej 8 znaków, w tym duże i małe litery, znaki interpunkcyjne, cyfry i znaki specjalne. Hasła powinny być łatwe do zapamiętania, jednakże nie powinny być oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby lub osób bliskich (np. imiona, numery telefonów, daty urodzenia itp.).
6. ASI zapewnia możliwość zmiany hasła w systemach informatycznych.
7. Na stanowiskach pracy dopuszczalne jest korzystanie wyłącznie z zaufanych menadżerów haseł dostępnych z licencjami umożliwiającymi dochodzenie roszczeń w przypadku ich nieprawidłowego działania. W takim przypadku hasło główne powinno mieć co najmniej 10 znaków, w tym duże i małe litery, znaki interpunkcyjne, cyfry i znaki specjalne.
8. Osoba upoważniona jest zobowiązana do zachowania haseł w poufności i nieudostępniania ich nikomu.
9. Środki uwierzytelniania stosowane są w szczególności:
    a. do uruchomienia wszystkich stacji roboczych, komputerów przenośnych oraz urządzeń mobilnych będących w zasobach jednostki, w tym także na poziomie BIOS urządzenia,
    b. do uruchomienia innych urządzeń infrastruktury IT, o ile mechanizm uwierzytelniania został przewidziany dla tych urządzeń,
    c. do uruchomienia systemów operacyjnych lub oprogramowania sterującego zainstalowanego na urządzeniach infrastruktury IT jednostki,
    d. do zalogowania użytkownika do systemów informatycznych służących realizacji zadań.

Osoby realizujące:

- w zakresie zapewnienia zgodnej z wymaganiami niniejszego punktu pracy i konfiguracji systemów informatycznych – ASI,
- w zakresie stosowania haseł zapewnienia zgodnych z ww. wymaganiami – użytkownicy systemu informatycznego.

6.11. Bezpieczeństwo infrastruktury teleinformatycznej

1. ASI zapewnia:
    a. stały dostęp do zapasowego źródła dostępu do usług sieciowych,
    b. odłączenie/dezaktywację niewykorzystywanych punktów dostępowych i gniazd przyłączeniowych,

c. bezpieczne rozmieszczenie sprzętu komputerowego w taki sposób aby zminimalizować ryzyko dostępu osób nieuprawnionych,
d. w miarę możliwości technicznych mechanizmy ochrony przed szkodliwym oprogramowaniem na poziomie:
   – sieciowym,
   – serwerów,
   – stacji roboczych,
   – zdalnego dostępu do systemów,
   – urządzeń mobilnych.

2. ADO zapewnia zasoby niezbędne do realizacji ww. zadań.

7. Bezpieczeństwo

7.1. Analiza ryzyka

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych, a także możliwość utraty integralności, dostępności lub poufności informacji.
2. W ramach analizy ryzyka ADO zapewnia identyfikację i ocenę stosowanych mechanizmów kontroli ryzyka, dla poszczególnych zagrożeń, a w przypadku stwierdzenia takiej potrzeby planuje i wdraża uwzględniając koszty i aktualny stan wiedzy nowe metody kontroli ryzyka zapewniające zadowalający poziom bezpieczeństwa.
3. Analiza ryzyka przeprowadzana jest nie rzadziej niż raz na rok.
4. Analizy ryzyka prowadzona jest z udziałem:
   a. ADO,
   b. IOD,
   c. zespołu ds. kontroli zarządczej,
   d. ASI,
   e. innych osób wyznaczonych przez ADO.
5. Stosowany arkusz analizy ryzyka stanowi załącznik nr 7.1.1.
6. Metodologia przeprowadzania analizy ryzyka stanowi załącznik nr 7.1.2.
7. ADO może zdecydować o stosowaniu innej metodyki analizy ryzyka.

Osoby realizujące:
– w zakresie planowania analizy ryzyka i wskazania osób biorących udział w tym procesie – ADO,
– w zakresie przeprowadzenia analizy ryzyka – ADO, ASI, IOD, zespół ds. kontroli zarządczej, inne osoby wyznaczone przez ADO.

7.2. Ocena skutków przetwarzania dla ochrony danych

1. Przed rozpoczęciem przetwarzania danych osobowych, które ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO dokonuje oceny skutków planowanych czynności przetwarzania dla ochrony danych.
2. Dokonując oceny skutków dla ochrony danych ADO konsultuje się z IOD.

3. Ocena ryzyka nie jest przeprowadzana dla przetwarzania danych osobowych wynikających z zadań, których wykonanie jest obowiązkiem nałożonym na ADO obowiązującymi przepisami prawa.
4. ADO przeprowadza ocenę skutków przetwarzania danych osobowych jeżeli samodzielnie dokonuje doboru narzędzia do realizacji zadania o którym mowa w pkt 7.2.3.

Osoby realizujące:

- w zakresie weryfikacji konieczności przeprowadzenia oceny skutków dla ochrony danych i wskazania osób biorących udział w tym procesie – ADO, IOD,
- w zakresie przeprowadzenia oceny skutków dla ochrony danych – ADO, inne osoby wyznaczone przez ADO.

8. Incydenty bezpieczeństwa ochrony danych osobowych

8.1. Naruszenia

1. Do typowych naruszeń (incydentów) zagrażających ochronie danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (np. utrata zasilania, utrata łączności, zalanie, pożar),
    b. zdarzenia losowe wewnętrzne (np. awarie serwera, urządzeń sieciowych, komputerów, dysków, oprogramowania, pomyłki użytkowników, utrata danych),
    c. zdarzenia zewnętrzne umyślne (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub informacji, kradzież lub zagubienie sprzętu, ujawnienie danych osobom nieuprawnionym, świadome zniszczenie dokumentów/danych dokonane przez osoby nierealizujące zadań na rzecz ADO lub działanie wirusów i innego szkodliwego oprogramowania),
    d. zdarzenia wewnętrzne umyślne (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub informacji, kradzież lub zagubienie sprzętu, ujawnienie danych osobom nieuprawnionym, świadome zniszczenie dokumentów/danych, dokonane przez osoby realizujące zadania na rzecz ADO lub działanie wirusów i innego szkodliwego oprogramowania, niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów zawierających dane),
    e. nieprzestrzeganie przez pracowników zasad ochrony danych (np. niestosowanie ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, stosowanie kluczy do pomieszczeń służbowych innych niż wydane przez ADO),
    f. zdarzenia nieumyślne będące skutkiem nieszczęśliwych wypadków.
2. Naruszenia mogą występować pojedynczo, na jednym stanowisku lub na wielu stanowiskach jednocześnie.

8.2. Postępowanie w przypadku zaistnienia naruszenia

1. W sytuacji podejrzenia zaistnienia naruszenia każdy pracownik:
    a. w pierwszej kolejności powinien zadbać o własne bezpieczeństwo,
    b. w miarę swoich możliwości powinien zminimalizować skutki naruszenia, w tym celu może także poprosić o pomoc współpracowników, bezpośrednich przełożonych, IOD lub osoby odpowiedzialne za ochronę budynku,
    c. informuje bezpośredniego przełożonego lub ADO.
2. ADO podejmuje wszelkie możliwe działania mające na celu minimalizację skutków naruszeń.

3. ADO, zależnie od charakteru zdarzenia, wskazuje osoby, które zajmą się obsługą naruszenia, identyfikacją jego przyczyn i skutków dla ochrony danych.

Osoby realizujące:

- w zakresie zgłaszania podejrzeń incydentów i minimalizacji skutków – osoby upoważnione, ASI,
- w zakresie wskazania osoby prowadzącej postępowanie – ADO.

8.3. Postępowanie wyjaśniające

1. Postępowanie wyjaśniające prowadzi osoba lub osoby wskazane przez ADO.
2. ADO prowadzi postępowanie wyjaśniające także w przypadku naruszeń zgłaszanych anonimowo.
3. Osoba prowadząca postępowanie:
    a. ustala charakter i lokalizację zaistnienia naruszenia,
    b. ustala rodzaj naruszenia, w tym ilość i zakres danych osobowych, które zostały zagrożone w wyniku naruszenia,
    c. ustala okoliczności towarzyszące naruszeniu,
    d. wskazuje podjęte lub konieczne do podjęcia działania w celu minimalizacji skutków naruszenia,
    e. ustala przyczyny wystąpienia naruszenia i dokonuje ich oceny,
    f. proponuje środki naprawcze w celu odwrócenia skutków naruszenia i zapobieżenia jego ponownemu wystąpieniu.
4. Wszystkie osoby upoważnione udzielają niezbędnych informacji, przygotowują oświadczenia i zabezpieczają niezbędne dokumenty na żądanie osoby prowadzącej postępowanie wyjaśniające.
5. Z prowadzonego postępowania sporządzany jest raport.
6. Wzór raportu stanowi załącznik nr 8.3.1.
7. ADO podejmuje decyzje o stosowanych środkach naprawczych.

Osoby realizujące:

- w zakresie prowadzenia postępowania i sporządzenia raportu z prowadzonego postępowania – osoba wskazana przez ADO,
- w zakresie pomocy osobie prowadzącej postępowanie wyjaśniające oraz zgłoszenie propozycji środków naprawczych – osoby upoważnione, ASI, IOD,
- w zakresie zatwierdzenia raportu z postępowania wyjaśniającego i decyzji o środkach naprawczych – ADO.

8.4. Ewidencjonowanie incydentów, informowanie organu nadzorczego i podmiotu danych

1. W sytuacji gdy incydent powoduje małe prawdopodobieństwo naruszenia praw i wolności podmiotów danych, odnotowywany jest w rejestrze incydentów.
2. Ewidencja naruszeń stanowi załącznik nr 8.4.1.
3. W sytuacji, gdy naruszenie powoduje większe niż małe prawdopodobieństwo naruszenia praw i wolności podmiotów danych, ADO informuje organ nadzorczy w ciągu 72 godzin od stwierdzenia naruszenia. W tym celu ADO przygotowuje we współpracy z IOD zgłoszenie

i przesyła je organowi nadzorczemu w formie elektronicznej, zgodnie z udostępnionym przez UODO mechanizmem.

4. W zakresie w jakim nie da się udzielić organowi nadzorczemu pełnej informacji w terminie wskazanym w powyższym punkcie, można je udzielać sukcesywnie bez zbędnej zwłoki.
5. W sytuacji, gdy naruszenie powoduje wysokie prawdopodobieństwo naruszenia praw i wolności podmiotów danych, ADO informuje podmioty danych bez zbędnej zwłoki.
6. Zawiadomienie sporządzone jest jasnym i prostym językiem, opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej:
    a. dane kontaktowe IOD,
    b. opis możliwych konsekwencji naruszenia ochrony danych osobowych,
    c. opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych,
    d. opis środków zastosowanych w celu zminimalizowania jego ewentualnych negatywnych skutków – jeżeli ma to zastosowanie.
7. ADO może odstąpić od poinformowania podmiotów danych o naruszeniu w sytuacji, gdy:
    a. naruszenie dotyczyło danych osobowych, które zostały zanonimizowane, zaszyfrowane lub zabezpieczone środkami technicznymi i organizacyjnymi uniemożliwiającymi odczyt tych danych przez osoby nieuprawnione,
    b. ADO zastosował, po zaistnieniu naruszenia, środki eliminujące wysokie ryzyko naruszenia praw lub wolności podmiotu danych,
    c. wymagałoby ono niewspółmiernie dużego wysiłku – w takim przypadku ADO wydaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą zostają poinformowane w równie skuteczny sposób.

Osoby realizujące:

- w zakresie prowadzenia rejestru incydentów – ASI,
- w zakresie uzupełniania informacji w ewidencji naruszeń – osoba prowadząca postępowanie,
- w zakresie przygotowania treści zgłoszenia – osoba prowadząca postępowanie we współpracy z IOD,
- w zakresie dokonania zgłoszenia do organu nadzorczego – ADO,
- w zakresie podjęcia decyzji o odstąpieniu od zgłoszenia naruszenia organowi nadzorczemu lub o nieinformowaniu podmiotów danych – ADO,
- w zakresie informowania podmiotów danych o incydencie – osoby wskazane przez ADO, we współpracy z IOD.

8.5. Wsparcie podmiotów zewnętrznych

1. W sytuacjach, w których zasoby sprzętowe i kadrowe nie pozwalają na adekwatną reakcję jednostki na incydenty bezpieczeństwa, ADO może podjąć decyzję o skorzystaniu z pomocy innych podmiotów.
2. W celu zapewnienia wyższego poziomu bezpieczeństwa ADO, w miarę możliwości, zawiera z tymi podmiotami stosowane porozumienia o współpracy w zakresie udzielania pomocy w przypadku incydentów informacji.
3. Porozumienie powinno zawierać co najmniej:
    a. zakres udzielanej pomocy,
    b. ewentualne formy rozliczenia,
    c. zasady zapewnienia poufności danych,

d. zapisy dotyczące powierzenia przetwarzania danych osobowych zgodnie z pkt. 5.5 niniejszej dokumentacji, w przypadku gdy takie powierzenie będzie elementem udzielanej pomocy.

4. Podmioty te powinny zapewniać doświadczenie i wiedzę niezbędną do udzielenia pomocy w reagowaniu na dany incydent, a także poufność informacji do których miały dostęp w trakcie udzielania pomocy.
5. ADO może korzystać z usług towarzystw ubezpieczeniowych, miedzy innymi w zakresie odpowiedzialności finansowej wynikającej z tytułu incydentów bezpieczeństwa informacji w tym cyberataków.

9. Inspektor Ochrony Danych

9.1. Wyznaczenie i pozycja IOD

1. ADO wyznacza inspektora ochrony danych w formie pisemnej w sposób ogólnie przyjęty przez ADO.
2. Wyznaczeniem może być także odpowiedni zapis w umowie cywilnoprawnej lub innym instrumencie prawnym.
3. ADO zapewnia niezależność IOD poprzez:
    a. zapewnienie organizacyjnej podległości bezpośrednio najwyższemu kierownictwu ADO lub bezpośrednio ADO,
    b. unikanie wydawania poleceń dotyczących sposobu realizacji zadań IOD – ograniczenie to obowiązuje zarówno ADO jak i osoby przez niego upoważnione,
    c. zakaz karania w żadnej formie (pośredniej lub bezpośredniej) lub odwoływania IOD za wykonywane czynności związane z ochroną danych osobowych,
    d. taką organizację pracy i zlecanie IOD innych zadań, które nie powodują konfliktu interesów.
4. ADO informuje IOD o wszystkich sprawach związanych z ochroną danych osobowych i stosuje się do jego zaleceń w tym zakresie.
5. ADO zapewnia wszelkie niezbędne zasoby IOD, które umożliwią mu wykonywanie zadań, w tym poprzez:
    a. wspieranie IOD w realizacji zadań przez kadrę kierowniczą,
    b. zapewnienie dostępu do zasobów ADO umożliwiających realizację zadań,
    c. umożliwienie dostępu do wszystkich działów i stanowisk pracy ADO w celu wykonywania zadań związanych z ochroną danych osobowych,
    d. zapewnienie szkoleń lub środków finansowych na szkolenie IOD,
    e. jeżeli to niezbędne – powołanie zespołu wspierającego działania IOD.
6. ADO konsultuje z IOD:
    a. konieczność przeprowadzenia oceny skutków dla ochrony danych oraz ewentualną konieczność zlecenia tej oceny podmiotowi zewnętrznemu,
    b. dobór metodologii przeprowadzenia oceny skutków dla ochrony danych,
    c. prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z wymogami ochrony danych,
    d. stosowane zabezpieczenia, w tym środki techniczne i organizacyjne stosowane do minimalizowania wszelkich zagrożeń praw i interesów podmiotów danych.
7. ADO podejmuje wszelkie ostateczne decyzje w zakresie ochrony danych osobowych.

Osoby realizujące:

- w zakresie zapewnienia niezależności, wsparcia i niezbędnych zasobów IOD – ADO,
- w zakresie bieżącego kontaktu z IOD w sytuacjach związanych z ochroną danych osobowych – osoby upoważnione.

9.2. Zadania Inspektora Ochrony Danych

1. IOD monitoruje działania ADO, wspiera go w przestrzeganiu przepisów prawa w zakresie ochrony danych osobowych i wspomaga w podejmowaniu decyzji w tym zakresie. W tym celu IOD:
    a. zbiera informacje w celu identyfikacji czynności przetwarzania,
    b. analizuje i sprawdza zgodność tego przetwarzania,
    c. informuje, doradza i rekomenduje określone działania.
2. IOD współpracuje z organem nadzorczym i stanowi punkt kontaktowy dla tego organu, w szczególności w zakresie:
    a. związanym z przetwarzaniem danych osobowych,
    b. uprzednich konsultacji, jeżeli jest to wymagane przepisami,
    c. wszelkich innych spraw, jeżeli jest to wymagane przepisami.
3. IOD wykonuje swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
4. IOD wspiera i doradza ADO w zakresie prowadzenia rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania.
5. IOD może wykonywać inne czynności niezwiązane z ochroną danych osobowych, jeżeli nie będą one powodowały konfliktu interesów z podstawową działalnością IOD.
6. IOD prowadzi w formie elektronicznej rejestr podjętych czynności, w którym ewidencjonuje wszystkie podjęte działania związane z ochroną danych osobowych. Rejestr, na koniec każdego roku lub na żądanie, przekazywany jest ADO.
7. IOD bierze udział w aktualizacji Polityki ochrony danych w miarę występujących potrzeb i zmian przepisów.
8. Inspektor Ochrony Danych dokumentuje w postaci protokołów podejmowane przez siebie działania monitorujące.

10. Aktualizacja dokumentacji

1. Niniejsza dokumentacja podlega przeglądowi nie rzadziej niż raz na rok.
2. Przeglądu dokumentacji dokonują w szczególności:
    a. IOD,
    b. ASI,
    c. inne osoby wskazane przez ADO.
3. Przeglądu dokonuje się z uwzględnieniem w szczególności:
    a. przepisów dotyczących ochrony danych osobowych, w tym:
        – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

– Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000),
– innych przepisów określających zasady przetwarzania danych osobowych,

b. przepisów dotyczących informatyzacji, w tym:
– ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 ze zm.),
– Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.),
– innych przepisów określających realizację zadań publicznych z wykorzystaniem usług społeczeństwa informacyjnego.

4. Przegląd uwzględnia wymagania realizacji zadań związane ze zmieniającymi się warunkami i możliwościami świadczenia usług publicznych w formie elektronicznej.
5. O wszelkich zmianach dokumentacji informuje się pracowników w zwyczajowo przyjętej w jednostce formie.

Wójt Gminy Wydminy

/-/ mgr inż. Radosław Król

Załącznik nr 5.1.1.

Administrator Danych Osobowych: Wójt Gminy Wydminy, pl. Rynek 1/1, 11-510 Wydminy

Inspektor Ochrony Danych: Bolesław Idek, iod@wydminy.pl

	1	2	3	4	5	6	7	8	9	10	11	12	13
												Transfer do kraju trzeciego lub org. międzynarodowej	
LP.	**Nazwa czynności przetwarzania**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontaktowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1**	**Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)**	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
1.													
2.													
3.													
4.													
5.													
6.													
7.													
8.													

Nazwa podmiotu przetwarzającego: Wójt Gminy Wydminy, pl. Rynek 1/1, 11-510 Wydminy
IOD: iod@wydminy.pl

Załącznik nr 5.1.2.

Rejestr kategorii przetwarzania

Bezpieczeństwo danych osobowych zapewnione jest zgodnie z przyjętą Polityką ochrony danych.

Lp.	Nazwa i dane ADO	Podstawa powierzenia (umowa lub instrument prawny nr … itp.)	Kategorie przetwarzania	Czy dane przekazywane są do państwa trzeciego lub organizacji międzynarodowej	Okres powierzenia
1					
2					
3					

Zał. nr 5.2.1.

Upoważnienie nr ……..

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

Pana/Panią **……**

(Imię i nazwisko)

……

(stanowisko lub funkcja)

do przetwarzania danych osobowych w zakresie powierzonych do realizacji zadań na podstawie: …… (tu wpisać odpowiednio: umowy o pracę z dnia …. / zakresu czynności z dnia …../ umowy zlecenia nr …. z dnia ……/ powołania z dnia ……, itp.)

Upoważnienie jest ważne od dnia …… do dnia ……..(uzupełnić wyłącznie w sytuacji jeżeli wynika zawartej umowy)

Jednocześnie informuję, że:

1. jest Pan/Pani zobowiązany do przetwarzania danych osobowych wyłącznie na polecenie administratora zgodnie z celami wynikającymi z powierzonych przez administratora danych osobowych zadań oraz zasadami zawartymi w Polityce ochrony danych,
2. udostępnianie danych osobowych lub umożliwianie dostępu do danych osobowych osobom nieuprawnionym podlega odpowiedzialności dyscyplinarnej na zasadach prawa pracy oraz cywilnej wobec podmiotu danych, karze grzywny oraz karze ograniczenia wolności,
3. niniejsze upoważnienie nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania stosunku pracy, zakończenia realizacji umowy cywilnoprawnej, odwołania z pełnionej funkcji lub zakończenia kadencji, a ponadto może być w każdym czasie zmienione lub odwołane.

……

(*podpis ADO)*

Zapoznałem się

……

(data i podpis upoważnionego)

Zał. nr 5.2.2.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię	Nazwisko	Nr upoważnienia	Stanowisko	Data nadania	Data ustania	Uwagi
1							
2							
3							

Zał. nr 5.2.3.

.....
Imię i nazwisko

.....
miejscowość, data

.....
STANOWISKO ALBO PESEL

OŚWIADCZENIE

Niniejszym oświadczam, że:

1. Zapoznałam/em się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z treścią rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) oraz ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. poz. 1000).
2. Zapoznałam/em się z Polityką ochrony danych w Urzędzie Gminy Wydminy.
3. Zostałam/em poinformowany o prawie do ochrony dobra osobistego, jakim jest tajemnica korespondencji.
4. Zostałam/em poinformowany o możliwości monitorowania poczty elektronicznej oraz innych urządzeń udostępnionych do realizacji zadań służbowych.
5. Zapoznałam/em się i rozumiem zasady dotyczące przestrzegania i ochrony danych, w szczególności ochrony danych osobowych opisane w powyższych dokumentach i zobowiązuję się do ich przestrzegania pod rygorem odpowiedzialności dyscyplinarnej oraz przewidzianej przepisami prawa.
6. Zobowiązuję się do zgłaszania wszelkich podejrzeń o naruszeniu bezpieczeństwa danych osobowych przełożonemu, ASI, Inspektorowi Ochrony Danych lub innej wyznaczonej do tego osobie.
7. Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych oraz środków organizacyjnych i technicznych służących ich zabezpieczeniu, także po zaprzestaniu przetwarzania danych lub zakończeniu współpracy, zatrudnienia, stażu, praktyki, wolontariatu, wykonaniu zlecenia, ustaniu członkostwa, po ustaniu pełnienia powierzonej funkcji.
8. Zobowiązuję się do poszanowania praw i wolności innych osób, w tym poszanowania ich życia prywatnego oraz dobrego imienia.

.....
data i podpis oświadczającego

Zał. nr 5.2.5.

Protokół weryfikacji uprawnień z dnia ……

L.p.	Imię i nazwisko użytkownika	Login	Nazwa systemu	Podjęte działania w ramach uprawnień
1				
2				
3				

Sporządzający:

……..

Zatwierdzam:

……..

Podpis ADO

Umowa powierzenia przetwarzania danych osobowych nr ……

zawarta w dniu …….. (zwana dalej „Umową") pomiędzy:

Wójtem Gminy Wydminy, pl. Rynek 1/1, 11-510 Wydminy powierzającym przetwarzanie danych osobowych (zwanym dalej **Administratorem**)

a

…….. (zwanym dalej Podmiotem przetwarzającym)

§ 1 Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanym dalej Rozporządzeniem).
2. Administrator oświadcza, że jest Administratorem powierzanych danych osobowych w rozumieniu przepisów Rozporządzenia oraz, że powierzane dane zgromadził zgodnie z obowiązującymi przepisami prawa z uwzględnieniem obowiązku informacyjnego o którym mowa w art. 13 i 14 Rozporządzenia.
3. Zasady i cele przetwarzania określa niniejsza Umowa, która nie narusza obowiązków wynikających z Rozporządzenia.
4. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa właścicieli powierzanych danych.
5. Podmiot przetwarzający oświadcza, iż stosuje środki organizacyjne i techniczne spełniające wymogi Rozporządzenia oraz chroniące prawa osób, których dane są powierzane do przetwarzania.

§2 Zakres i cel przetwarzania danych

1. Administrator powierza Podmiotowi przetwarzającemu dane osobowe określone w załącznikach nr 1 - ??? do niniejszej umowy.
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie (**WERSJA 1**) w celu realizacji umowy nr …… z dnia …….. (*należy wskazać umowę główną o świadczenie usług zawartą z podmiotem przetwarzającym*). (**WERSJA 2**) w niżej wymienionych celach:
    a. *wskazać czynności związane z przetwarzaniem*
    b. …

§3 Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się zgodnie z wymaganiami Rozporządzenia:
    a. do stosowania środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa powierzanych danych osobowych odpowiadający ryzyku związanemu z ich przetwarzaniem (art. 32 w związku z art. 28 ust. 3 lit. c RODO),
    b. dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych,

c. do poinformowania Administratora przed rozpoczęciem przetwarzania danych o realizacji ewentualnego obowiązku prawnego polegającego na przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 28 ust. 3. lit. a RODO),
d. do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy,
e. do odebrania od osób upoważnionych stosownych oświadczeń o zobowiązaniu do zachowania w tajemnicy treści przetwarzanych danych, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu (art. 28 ust. 3. lit. b RODO).

2. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, lub po rozwiązaniu umowy, zwraca Administratorowi wszystkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że przepisy powszechnie obowiązującego prawa Unii lub prawa krajowego nakazują przechowywanie tych danych osobowych.
3. Podmiot przetwarzający, w miarę możliwości i w niezbędnym zakresie, pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.
4. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia.
5. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych:
   a. niezwłocznie, jednak nie później niż w ciągu 24 h od stwierdzenia naruszenia, informuje Administratora o tym fakcie i podaje wszelkie znane informacje dotyczące naruszenia,
   b. ustala przyczynę naruszenia lub wskazuje czynności podjęte w celu ustalenia tej przyczyny,
   c. podejmuje wszelkie czynności mające na celu ograniczenie skutków naruszenia, usuniecie naruszenia oraz zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami,
   d. zbiera wszelkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości,
   e. udziela Administratorowi wszelkiej pomocy w identyfikacji i zawiadomieniu osób, których praw dotyczyło naruszenie oraz w obsłudze ich roszczeń.
6. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o:
   a. wszelkich postępowaniach, w szczególności administracyjnych lub sądowych, dotyczących przetwarzania przez Podmiot przetwarzający powierzonych danych,
   b. wszelkich decyzjach administracyjnych lub orzeczeniach dotyczących przetwarzania tych danych skierowanych do Podmiotu przetwarzającego,
   c. wszelkich planowanych lub realizowanych w Podmiocie przetwarzającym kontrolach i inspekcjach dotyczących przetwarzania powierzonych na podstawie niniejszej umowy danych, w szczególności prowadzonych przez przedstawicieli Generalnego Inspektora Ochrony Danych Osobowych lub powołanego po wejściu w życie Rozporządzenia organu nadzorczego.

§4 Prawo kontroli

1. Na pisemny wniosek Administratora, Podmiot przetwarzający udziela informacji na temat przetwarzania powierzonych danych osobowych, w tym na temat zastosowanych przy

przetwarzaniu danych osobowych środków technicznych i organizacyjnych, w ustalonym przez Administratora terminie nie krótszym niż 3 dni robocze od dnia otrzymania wniosku.

2. Administrator ma prawo do przeprowadzenia audytów, realizowanych przez siebie lub upoważnionego audytora, oraz inspekcji spełnienia obowiązków określonych w niniejszej umowie w zakresie określonym w art. 28 ust. 3 lit. h RODO.
3. Podmiot przetwarzający umożliwia i przyczynia się do realizacji audytów i inspekcji.
4. O planowanym audycie lub inspekcji Administrator informuje Podmiot przetwarzający nie później niż na 7 dni przed ich planowanym terminem w formie pisemnej w tym elektronicznej.
5. Administrator ma prawo do przeprowadzania audytów i inspekcji także u podwykonawców przetwarzania w trybie i zakresie określonym w niniejszej umowie. Podmiot przetwarzający zobowiązuje się zapewnić możliwość przeprowadzenia audytów i inspekcji u podmiotów, którym podpowierzył, w trybie §5 niniejszej umowy, przetwarzanie danych osobowych powierzonych przez Administratora.
6. O wynikach audytów i inspekcji Administrator informuje pisemnie Podmiot przetwarzający. Informacja pisemna zawiera opis podjętych czynności, opis ustalonego stanu faktycznego, wnioski ustalone na podstawie zgromadzonych informacji i jasno sformułowane zalecenia.
7. Podmiot przetwarzający podejmuje działania naprawcze w zakresie stwierdzonych uchybień lub przekazuje wyjaśnienia o przyczynach niepodjęcia takich działań w terminie wskazanym przez Administratora.

§5 Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na dalsze powierzenie powierzanie przetwarzania danych osobowych przez podmiot przetwarzający.
2. Podmiot przetwarzający informuje Administratora o zamiarze dalszego powierzenia przetwarzania danych osobowych.
3. Podmiot przetwarzający może przekazać powierzone dane osobowe do państwa trzeciego wyłącznie w przypadku:
    a. pisemnego polecenia Administratora,
    b. konieczności spełnienia obowiązku jaki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podmiot, któremu podpowierzane jest przetwarzanie, w tym podmiot w państwie trzecim, winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
5. Odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych ponosi Podmiot przetwarzający.

§ 6 Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za:
    a. szkody wyrządzone wskutek niewykonania lub nienależytego wykonania obowiązków wynikających z niniejszej umowy,
    b. udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym,
    c. przetwarzanie z naruszeniem obowiązujących przepisów,

d. nieuprawnioną zmianę danych, uszkodzenie lub zniszczenie, które nastąpiły z winy Podmiotu przetwarzającego.

2. Odpowiedzialność ograniczona jest do szkody rzeczywistej.

§7 Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony, czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Administrator zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów, do których miał dostęp w wyniku realizacji swoich uprawnień wynikających z niniejszej umowy, w szczególności dotyczących stosowanych przez Podmiot przetwarzający środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa powierzanych danych. Zachowanie tajemnicy obowiązuje Administratora w trakcie realizacji niniejszej umowy i po zakończeniu jej obowiązywania

§8 Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony ALBO określony od …….. do ……. .
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… okresu wypowiedzenia.

§9 Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.

Administrator danych

Podmiot przetwarzający

Załącznik nr 1
do umowy nr ..... z dnia .....

Kategoria osób których dane dotyczą: .....

1. Zakres powierzanych do przetwarzania danych osobowych (art. 6 ust. 1 RODO)

1. nazwiska i imiona
2. imiona i nazwiska rodziców
3. data urodzenia
4. miejsce urodzenia
5. adres zamieszkania lub pobytu
6. adres korespondencyjny
7. numer ewidencyjny PESEL
8. NIP
9. miejsce pracy
10. zawód
11. wykształcenie
12. seria i nr dowodu
13. nr telefonu
14. adres e-mail
15. wizerunek
16. nr rachunku bankowego
17. stanowisko
18. .....
19. .....
20. .....
21. .....
22. .....

2. Zakres powierzanych do przetwarzania szczególnych danych osobowych (art. 9 ust. 1 RODO)

1. pochodzenie rasowe lub etniczne
2. poglądy polityczne
3. przekonania religijne lub światopoglądowe
4. przynależność do związków zawodowych
5. dane genetyczne
6. dane biometryczne
7. dane dotyczące zdrowia
8. dane dotyczące seksualności lub orientacji seksualnej
9. .....
10. .....
11. .....
12. .....
13. .....
14. .....

Zał. nr 6.3.1.

Wyznaczenie

Na podstawie Polityki Ochrony Danych wprowadzonej uchwałą/zarządzeniem ……..

wyznaczam

1. Panią/Pana: …….. stanowisko:……..
2. Panią/Pana: …….. stanowisko:……..

jako osobę odpowiedzialną za otworzenie i zamknięcie budynku mieszczącego się …….. oraz za aktywację i dezaktywację systemu alarmowego w wyznaczonych godzinach pracy.

Jednocześnie zobowiązuję Pana/Panią do:

a. wykorzystywania udostępnionych kluczy zgodnie z przeznaczeniem,
b. niewykonywania kopii udostępnionych kluczy,
c. starannego zamknięcie wejścia do budynku,
d. aktywacji i dezaktywacji systemu alarmowego,
e. w momencie otwierania budynku sprawdzania czy nie doszło do próby włamania i niezwłoczne poinformowanie mnie o takim zdarzeniu.

……..
data, podpis ADO

Zał. nr 6.7.1

Ewidencja przenośnych nośników danych

L.p.	Nazwa nośnika	Nr seryjny	Imię i nazwisko pracownika, któremu wydano nośnik	Data wydania	Data zwrotu	Uwagi
1						
2						
3						

Zał. nr 6.8.1.

Karta sprzętu komputerowego i oprogramowania

Nr ewidencyjny urządzenia:	Osoba odpowiedzialna:

Konfiguracja sprzętowa:	
1. *nazwa i rodzaj podzespołu* 2. *nazwa i rodzaj podzespołu* 3. *nazwa i rodzaj podzespołu* 4. *nazwa i rodzaj podzespołu*	5. *nazwa i rodzaj podzespołu* 6. *…*

Lp.	Nazwa programu	Licencja (płatna/open source)	Cel wykorzystania
1			
2			
3			

Zał. nr 6.8.2.

Ewidencja wykorzystywanych mechanizmów bezpieczeństwa systemów teleinformatycznych

Lp.	Nazwa stosowanego zabezpieczenia	Rodzaj urządzenia lub programu	Zastosowanie
1			
2			
3			

Zał. nr 6.9.1

Ewidencja przenośnych nośników danych

L.p.	Nazwa urządzenia tworzącego kopie zapasowe	Nośnik danych	Metoda (np. automatyczna/manualna; przyrostowa itp.)	Częstotliwość wykonywania kopii zapasowych	Zasoby objęte kopią zapasową (wymienić SI, bazy danych, urządzenia)	Okres przechowywania kopii zapasowej
1						
2						
3						

Kategoria ryzyka:	Zagrożenia:	Stosowane zabezpieczenia i procedury bezpieczeństwa:	Ocena skuteczności zabezpieczeń w stosunku do zagrożeń:	Wykryte podatności:	Poziom ryzyka z uwzględnieniem zabezpieczeń:	Decyzja dotycząca ryzyka lub proponowane działania:	Planowany termin realizacji
PRZETWARZANIE PAPIEROWE							
	należy wymienić zidentyfikowane (możliwe) zagrożenia	należy wymienić wszystkie zabezpieczenia przewidziane dla danej kategorii ryzyka	tu należy ocenić jak skuteczne są zastosowane zabezpieczenia dla poszczególnych zagrożeń: niska/średnia/wysoka	należy wypisać podatności (słabe punkty zabezpieczeń) dla poszczególnych kategorii zagrożeń	dla poszczególnych zagrożeń należy ocenić jaki jest realny poziom ryzyka z uwzględnieniem zagrożeń: niskie/średnie/wysokie	w kolejnych wierszach należy wpisać czy ryzyko jest akceptowane lub jakie działania należy podjąć, żeby je zminimalizować	w kolejnych wierszach należy wpisać do kiedy należy podjąć działania minimalizujące ryzyko
nieuprawnione zniszczenie lub utracenie danych osobowych (dostępność)							
nieuprawnione zmodyfikowanie danych osobowych (integralność)							
nieuprawnione ujawnienie lub dostęp do danych osobowych (poufność)							
PRZETWARZANIE W SYSTEMACH IT							
	należy wymienić zidentyfikowane (możliwe) zagrożenia	należy wymienić wszystkie zabezpieczenia przewidziane dla danej kategorii ryzyka (uwzględniając zabezpieczenia stacji roboczych; urządzeń brzegowych; monitorowania ruchu sieciowego)	tu należy ocenić jak skuteczne są zastosowane zabezpieczenia dla poszczególnych zagrożeń: niska/średnia/wysoka	należy wypisać podatności (słabe punkty zabezpieczeń) dla poszczególnych kategorii zagrożeń	dla poszczególnych zagrożeń należy ocenić jaki jest realny poziom ryzyka z uwzględnieniem zagrożeń: niskie/średnie/wysokie	w kolejnych wierszach należy wpisać czy ryzyko jest akceptowane lub jakie działania należy podjąć, żeby je zminimalizować	w kolejnych wierszach należy wpisać do kiedy należy podjąć działania minimalizujące ryzyko
nieuprawnione zniszczenie lub utracenie danych osobowych (dostępność)							
nieuprawnione zmodyfikowanie danych osobowych (integralność)							
nieuprawnione ujawnienie lub dostęp do danych osobowych (poufność)							
wspólne dla: poufności integralności dostępności							

Metodologia przeprowadzania analizy ryzyka

Analiza ryzyka powinna być dokonana dla każdego z atrybutu bezpieczeństwa danych osobowych: należy rozważyć wpływ, jaki na prawa i wolności osób, których dane są przetwarzane może mieć nieuprawnione ujawnienie (**utrata poufności**) danych, w tym danych osobowych, nieuprawniona zmiana (**utrata integralności**) danych, w tym danych osobowych, zniszczenie lub utrata (**utrata dostępności**) danych, w tym danych osobowych. Podobnie należy ocenić jakie konsekwencje będzie miała utrata poufności, integralności i dostępności danych dla Administratora oraz osób których dane te dotyczą.

Przyjmuje się następujące szczegółowe etapy procesu szacowania ryzyka:

1. Określenie kontekstu przetwarzania danych
   – Zidentyfikowanie aktywów / obszarów przetwarzania danych

2. Wykonanie szacowania ryzyka
   a) określenie możliwych zagrożeń i ocena ich prawdopodobieństwa
      – Zidentyfikowanie zagrożeń dla aktywów
      – Zidentyfikowanie istniejących zabezpieczeń
      – Ocena skuteczności zidentyfikowanych zagrożeń
      – Zidentyfikowanie podatności
   b) Wskazanie poziomu ryzyka dla aktywów z uwzględnieniem zabezpieczeń
   c) Podjęcie decyzji co do postępowania z ryzykiem, zaproponowanie działania
   d) Określenie terminu wdrożenia ewentualnych działań o ile są potrzebne

1. Określenie kontekstu przetwarzania danych - uwarunkowań związanych z działaniem organizacji

a) zidentyfikowanie aktywów - szczegółowy opis przetwarzanych danych i ich klasyfikacja

Przetwarzane dane osobowe zostały opisane i zestawione w Rejestrze czynności przetwarzania, który jest prowadzony na podstawie Art. 30 RODO.

Każde istotne aktywo / obszar przetwarzania opisywane będą w odrębnej zakładce Arkusza Analizy Ryzyka.

2. Wykonanie szacowania ryzyka

a) określenie możliwych zagrożeń i ocena ich prawdopodobieństwa – kol. 2

Na tym etapie należy przeanalizować zagrożenia, które mogą wpłynąć na bezpieczeństwo informacji.

Wykaz zagrożeń, które mogą wpłynąć na bezpieczeństwo przetwarzanych informacji został zamieszczony w Tabeli nr 1.

b) określenie zastosowanych zabezpieczeń – kol. 3

Opis przykładowych zabezpieczeń, które mają zmniejszyć podatność aktywów na zagrożenia lub ograniczyć skutki zmaterializowania się zagrożeń, został zamieszczony w Tabeli nr 2.

c) ocena skuteczności zabezpieczeń – kol. 4

Przyjmuje się trzy poziomy skuteczności zabezpieczeń: mała, średnia i duża

Skuteczność mała oznacza, iż zabezpieczenie nie jest adekwatne do zagrożenia, nie jest kompletne lub w inny sposób nie odpowiada wymogom. Właściciel aktywa nie może uznać go za wystarczającą zabezpieczone. Właściciel aktywa powinien podjąć pilne działania zmierzające do wzmocnienia zabezpieczeń.

Skuteczność średnia oznacza, iż zabezpieczenie nie jest w pełni adekwatne do zagrożenia, nie jest kompletne lub w inny sposób nie w pełni odpowiada wymogom. Właściciel aktywa powinien podjąć działania zmierzające do wzmocnienia zabezpieczeń.

Skuteczność duża oznacza, iż zabezpieczenie jest generalnie adekwatne do zagrożenia, jest kompletne oraz odpowiada wymogom. Właściciel aktywa powinien monitorować jego skuteczność.

d) Identyfikacja podatności – kol. 5

Przykładowy wykaz podatności został umieszczony w opisującym zagrożenia Tabeli nr 3 do Polityki. Przed szacowaniem ryzyka należy przejrzeć wykaz podatności. Podatność jeszcze nie powoduje szkody, ale zostanie wykorzystana, gdy zagrożenie zmaterializuje się.

e) ocena ryzyka z uwzględnieniem zabezpieczeń oraz podatności – kol. 6

Ustaliwszy charakter, zakres i cele i kontekst przetwarzania danych należy ocenić wpływ przetwarzania danych na podstawowe prawa i wolności osób, wynikający z możliwej utraty bezpieczeństwa danych osobowych.

Przy szacowaniu ryzyka należy uwzględnić następujące czynniki:

- statystyki dotyczące podobnych zdarzeń,
- atrakcyjność aktywa,
- rodzaje podatności,
- istniejące zabezpieczenia

Przyjmuje się trzy poziomy ryzyka: **małe, średnie i duże**

Poziom ryzyka	Opis działania
niski	Poziom ryzyka **akceptowany** - działania podejmowane w zależności od wymaganych nakładów i dostępnych środków
średni	Poziom ryzyka **nieakceptowany** - działanie może zostać przesunięte w czasie, ale ryzyko wymaga monitorowania
wysoki	Poziom ryzyka **nietolerowany** - wymaga natychmiastowego działania

e) Wskazanie działań jakie należy podjąć w związku z oszacowanym ryzykiem – kol. 7

Dla ryzyka zaklasyfikowanego jako „średnie" właściciel aktywa (Procesu przetwarzania danych) wraz osobami wskazanymi przez administratora danych osobowych opracowują plan postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu „niskiego".

Dla ryzyka „wysokiego" trzeba podjąć działania zmierzające do natychmiastowego jego obniżenia, a gdy te działania nie zmniejszają ryzyka należy zrezygnować z przetwarzania danych osobowych lub zgodnie z Art. 36 ust. RODO przed rozpoczęciem przetwarzania skonsultować się z organem nadzorczym.

f) Wskazanie terminów realizacji zaplanowanych działań naprawczych – kol. 8

Dla każdego działania naprawczego należy wskazać datę jego realizacji. Plan jest zatwierdzany przez administratora danych osobowych.

Tabela nr 1 - Lista potencjalnych zagrożeń

Nazwa zagrożenia
Zniszczenia fizyczne
Pożar
Zalanie
Zanieczyszczenie
Zniszczenie urządzeń lub nośników
Pył, korozja, wychłodzenie
Utrata podstawowych usług
Awaria systemu klimatyzacji
Utrata dostaw prądu
Brak dostępu do usług zewnętrznych
Brak dostępu do Internetu
Brak dostępu do poczty elektronicznej
Brak dostępu do aplikacji internetowych
Zakłócenia spowodowane promieniowaniem
Promieniowanie elektromagnetyczne
Promieniowanie cieplne
Naruszenie bezpieczeństwa informacji
Szpiegostwo
Przechwycenie sygnałów na skutek zjawiska interferencji
Szpiegostwo zdalne
Podsłuch
Kradzież
Kradzież nośników lub dokumentów
Kradzież urządzenia
Odtworzenie z wyrzuconych nośników
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie
Pozostawienie wydruków na ogólnodostępne drukarce
Wyrzucenie nośników elektronicznych (CD, pendrive)
Oddanie do likwidacji dysków nie pozbawionych zapisów
Ujawnienie
Ujawnienie sposobu działania aplikacji i systemu jej zabezpieczeń
Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.
Dopuszczenie, aby ktokolwiek mógł pozyskać informację o infrastrukturze IT
Dopuszczenie do użytkowania sprzętu lub oprogramowania przez osoby nie uprawnione
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji z dostępem do danych osobowych

Pozostawienie w miejscu niezabezpieczonym zapisanego hasła dostępu
Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora
Pozostawienie otwartych okien, drzwi po zakończeniu pracy
Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu
Utrata kontroli nad kopią danych osobowych
Pozostawienie w pomieszczeniu bez nadzoru osób postronnych, w tym pracowników nieuprawnionych
Dane z niewiarygodnych źródeł
Wykorzystanie ogólnodostępnych serwisów pocztowych w celach służbowych
Manipulowanie urządzeniem
Zmiana konfiguracji sprzętowej lub programowej systemów oraz stacji roboczych przez niepowołane osoby
Sfałszowanie oprogramowania
Awarie techniczne
Awaria urządzenia
Niewłaściwe funkcjonowanie urządzeń
Przeciążenie systemu informacyjnego
Niewłaściwe funkcjonowanie oprogramowania
Nieautoryzowane działania
Nieautoryzowane użycie urządzeń
Dopuszczenie, aby osoby inne niż informatyk podłączały jakiejkolwiek urządzenia do sieci
Dopuszczenie, aby osoby inne niż informatyk dokonywały zmian w okablowaniu
Dopuszczenie, aby osoby inne niż informatyk zmieniały konfigurację sprzętu
Dopuszczenie do serwerów lub znalezienia się w serwerowni osób spoza służb informatycznych
Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych
Wyniesienie kluczy od pomieszczeń biurowych po zakończonej pracy
Nieuprawnione używanie oprogramowani
Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania
Użycie narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych
Sporządzanie kopii danych na nośnikach danych w sytuacji nie przewidzianych procedurą
Wykorzystanie służbowej poczty elektronicznej do celów prywatnych
Użycie fałszywego lub skopiowanego oprogramowania
Zniekształcenie danych
Celowe działanie użytkowników lub osób trzecich prowadzące do zafałszowania danych lub utraty integralności
Nielegalne przetwarzanie danych
Przetwarzanie danych bez upoważnienia lub niezgodnie z zakresem obowiązków
Przetwarzanie danych bez uzasadnionej podstawy prawnej
Przetwarzanie danych niezgodnie z zasadami opisanymi w Art. 5 RODO

Używanie nieautoryzowanych (prywatnych) nośników
Naruszenie bezpieczeństwa funkcji
Błąd użytkowania/administratora
Zaniedbania użytkowników i administratorów
Niewykonanie kopii danych
Niesprawdzenie integralności kopii (możliwości odtworzenia)
Przekroczenie uprawnień
Uzyskanie hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.
Nieuzasadnione przeglądanie (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą identyfikatora i hasła użytkownika.
Sporządzanie kopii danych w sytuacji nie przewidzianej procedurą
Niedostępność pracowników
Choroba ważnych osób
Niedobór pracowników

Tabela nr 2 – Przykłady zabezpieczeń

Zabezpieczenia
Organizacja bezpieczeństwa informacji
Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana właścicielom aktywów.
Rozdzielanie obowiązków i odpowiedzialności pozostających w konflikcie ze sobą.
Wprowadzenie polityki oraz wspierających ją zabezpieczeń w celu zarządzania ryzykami wynikającymi z użytkowania urządzeń mobilnych, oraz informacji pobieranych, przetwarzanych lub przechowywanych w miejscach wykonywania telepracy.
Bezpieczeństwo zasobów ludzkich
Zapewnienie, aby umowy z pracownikami i kontrahentami określały odpowiedzialność stron w obszarze bezpieczeństwa informacji.
Szkolenie pracowników i innych zainteresowanych podmiotów w zakresie bezpieczeństwa informacji i stosowanych i wymaganych zabezpieczeń
Stosowanie odpowiedzialności dyscyplinarnej w zakresie bezpieczeństwa informacji
Zobowiązanie do stosowania zasad poufności po zakończeniu lub zmianie zatrudnienia, a następnie ich egzekwowanie.
Zarządzanie aktywami
Zidentyfikowanie aktywów, związanych z informacjami i środkami przetwarzania informacji oraz sporządzenie i utrzymywanie ewidencji tych aktywów.
Zidentyfikowanie, udokumentowanie i wdrożenie zasad akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji.
Zapewnienie, aby w momencie zakończenia zatrudnienia, umowy lub porozumienia wszyscy pracownicy i użytkownicy podmiotów zewnętrznych zwracali wszystkie posiadane aktywa organizacji.
Zapewnienie, aby informacje były klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.
Bezpieczne wycofywanie nośników, które nie będą już dłużej wykorzystywane
Kontrola dostępu
Zapewnienie użytkownikom dostępu wyłącznie do tych sieci, usług sieciowych i systemów, do których otrzymali wyraźne uprawnienia.
Rejestrowanie i wyrejestrowywanie użytkowników.
Zapewnienie, aby po zakończeniu zatrudnienia, umowy lub porozumienia przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji były odbierane, lub dostosowywane do zaistniałych zmian.
Kontrolowanie dostępu do systemów i aplikacji przez procedurę bezpiecznego logowania.
Ograniczenie dostępu do kodu źródłowego programu.
Kryptografia
Stosowanie zabezpieczeń kryptograficznych do ochrony informacji.

Bezpieczeństwo fizyczne i środowiskowe
Zabezpieczenie obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.
Zabezpieczenia wejść zapewniające dostęp wyłącznie osobom uprawnionym.
Stosowanie fizycznego zabezpieczenia biur, pomieszczeń i obiektów.
Umieszczenie i ochrona sprzętu w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.
Ochronę sprzętu przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.
Zapewnienie, aby okablowanie zasilające i telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne, było chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem.
W celu zapewnienia dostępności i integralności sprzętu zaleca się jego prawidłową konserwację.
Zapewnienie, aby sprzęt, informacje lub oprogramowanie nie były wynoszone poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.
Zabezpieczenie aktywów wynoszonych poza siedzibę organizacji przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.
Przed zbyciem lub przekazaniem sprzętu do ponownego użycia Skuteczne usunięcie danych lub ich bezpiecznie nadpisane.
Wprowadzenie polityki czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz polityki czystego ekranu dla środków przetwarzania informacji.
Stosowanie systemów i urządzeń monitorujących wykorzystanie zasobów sieciowych.
Bezpieczna eksploatacja
Nadzorowanie zmian w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji.
Stosowanie oprogramowania minimalizującego ryzyko naruszenia bezpieczeństwa sieci i stosowanych systemów informatycznych
Monitorowanie i dostosowanie wykorzystania zasobów oraz przewidywanie wymaganej pojemności w przyszłości, dla zapewnienia właściwej wydajności systemu.
Oddzielanie środowisk rozwojowych, testowych i produkcyjnych celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.
Wdrożenie zabezpieczeń wykrywających, zapobiegających i odtwarzających, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.
Tworzenie, przechowywanie i systematyczne przeglądanie dzienników zdarzeń rejestrujących działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.
Ochronę środków służących rejestrowaniu zdarzeń oraz informacji w dziennikach zdarzeń przed manipulacją i nieuprawnionym dostępem.

Rejestrowanie działań administratorów i operatorów systemów, a dzienniki chronić i systematycznie przeglądać.

Tabela nr 3 – Przykłady typowych podatności

Rodzaj	Przykład podatności	Przykłady zagrożeń
Sprzęt	Niezabezpieczone urządzenie do przechowywania danych	Kradzież danych lub dokumentów
	Brak staranności przy pozbywaniu się nośników	Kradzież nośników lub danych
	Niekontrolowane kopiowanie	Kradzież danych
	Wrażliwość na wilgoć, pył, zanieczyszczenie	Pył, korozja, wychłodzenie
	Wrażliwość na zmiany temperatury	Zjawiska pogodowe lub aspekty produkcyjne
	Wrażliwość na zmiany napięcia zasilania	Utrata zasilania
	Brak planów okresowej wymiany sprzętu	Zniszczenie lub awaria urządzenia lub nośników
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej	Nadużycie praw
	Błędne przypisanie praw dostępu	Nadużycie praw
	Brak mechanizmów identyfikacji i uwierzytelnienia użytkownika	Fałszowanie praw
	Złe zarządzanie hasłami	Fałszowanie praw
	Brak fizycznej kontroli budynków, drzwi i okien	Kradzież nośników lub danych
	Brak skutecznej kontroli zmian	Zakłócenie procesu
Sieć	Niezabezpieczone linie telefoniczne	Podsłuch
	Złe łączenie kabli	Awaria urządzenia telekomunikacyjnego
	Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy	Fałszowanie praw
	Niezabezpieczone połączenie z siecią publiczną	Nieautoryzowane użycie urządzeń
	Uszkodzenie fizyczne sieci lub kabli	Zatrzymanie procesu
Personel	Nieobecność personelu	Naruszenie danych, brak dostępności
	Niewystarczające szkolenie z bezpieczeństwa, użycia oprogramowania lub sprzętu	Błąd użytkowania

	Brak mechanizmów monitorowania	Nielegalnie przetwarzanie danych
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	Nieautoryzowane użycie urządzeń
Siedziba	Lokalizacja na obszarach zagrożonych powodzią	Powódź
	Brak fizycznej ochrony budynków, drzwi i okien	Kradzież, zniszczenie
Organizacja	Brak procedur regulujących bezpieczeństwo aktywów	Utrata danych, Niezgodność z przepisami prawa, Nieautoryzowany dostęp
	Brak regularnego nadzoru	Nadużycie praw
	Brak zdefiniowanego postępowania dyscyplinarnego	Kradzież urządzenia

Raport nr …. z naruszenia ochrony danych

1. Data i godzina stwierdzenia naruszenia:
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane w związku z naruszeniem ochrony danych (*imię, nazwisko, stanowisko służbowe lub funkcja*):
    a.
    b.
3. Określenie miejsca zdarzenia i zasobu, którego dotyczył incydent:

4. Rodzaj naruszenia:
    a. opis naruszenia:
    b. ilość naruszonych danych osobowych:
    c. zakres naruszonych danych osobowych:
    d. kategoria podmiotów danych lub kategoria czynności przetwarzania:
5. Opis okoliczności towarzyszących naruszeniu:
6. Opis przyczyny wystąpienia naruszenia
7. Podjęte działania w celu minimalizacji skutków:
8. Podjęte działania w celu uniknięcia naruszenia w przyszłości:

Podpisy osoby sporządzającej / osób sporządzających:

Ewidencja naruszeń

Lp.	Data i godzina naruszenia	Osoba zgłaszająca	Syntetyczny opis incydentu	Ocena czy skutki powodują: małe ryzyko/ryzyko/wysokie ryzyko naruszenia ochrony danych osobowych	Data poinformowania Prezesa Urzędu Ochrony Danych Osobowych	Podjęte działania
1						
2						
3						