**ZARZĄDZENIE Nr 20/2023**

**Wójta Gminy Kiernozia**

**z dnia 27 kwietnia 2023r.**

**w sprawie ustalenia i wdrożenia „Polityki bezpieczeństwa danych osobowych” w Urzędzie Gminy w Kiernozi.**

Na podstawie art. 30 ust.1 i art. 31 w zw. z art. 41 ust 2 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40 z późn. zm.). oraz art. 37 ust.1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, s.1 - **zarządzam, co następuje:**

**§ 1.** Traci moc Zarządzenie Nr 85 Wójta Gminy Kiernozia z dnia 31.12.2020 r. w sprawie aktualizacji procedur w zakresie ochrony danych osobowych i wdrożenia Polityki Bezpieczeństwa Ochrony Danych.

**§ 2.** Wprowadza się do użytku służbowego „Politykę bezpieczeństwa danych osobowych” stanowiącą Załącznik Nr 1 do niniejszego zarządzenia.

**§ 3.** Zobowiązuję wszystkich pracowników Urzędu Gminy w Kiernozi do zapoznania się z Polityką bezpieczeństwa danych osobowych oraz jej przestrzegania w bieżącej pracy.

**§ 4.** Zarządzenie wchodzi w życie z dniem podjęcia.

# POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

# W GMINIE KIERNOZIA

**Instytut Szkoleniowo – Doradczy J. Kuszmider**
90-520 Łódź, Gdańska 116/7
Tel. 782-447-178; 607-770-718 email: kontakt@iszd.pl www.iszd.pl

**Administrator Danych Osobowych:**

| | |
|---|---|
| Adres | **Urząd Gminy w Kiernozi, ul. Sobocka 1A, 99-412 Kiernozia** |
| Adres e-mail | e-mail: gmina@kiernozia.gmina.pl |
| Nr telefonu | **tel. 24 2779080** |

……

(data/podpis)

**Inspektor Ochrony Danych:**

| | |
|---|---|
| Imię i nazwisko | **Magdalena Kuszmider** |
| Adres e-mail | **magdalena@kuszmider.com.pl** |
| Nr. telefonu | **607770718** |

……

(data/podpis)

# Spis treści

# 1. WSTĘP

***Polityka Bezpieczeństwa Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym jest dokumentem przeznaczonym do użytku wewnętrznego w jednostce. Dokumenty związane z bezpieczeństwem danych osobowych nie podlegają udostępnieniu w trybie ustawy o dostępie do informacji publicznej.***

Niniejsza Polityka Bezpieczeństwa Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym została opracowana z uwzględnieniem wytycznych oraz na podstawie 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1), ustawy o ochronie danych osobowych z dnia 10 maja 2018r. (Dz.U.2019.1781 t.j.), 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.2017.2247 t.j.) , a także ustaw kompetencyjnych dotyczących zadań własnych i zleconych jednostki w oparciu o zmiany przepisów krajowych oraz przy zachowaniu zasad wynikających z dobrych praktyk. Ochrona danych osobowych jest realizowana poprzez zastosowanie środków bezpieczeństwa fizycznego, informatycznego i procedury organizacyjne.

## 2. ZAKRES STOSOWANIA

Polityka Bezpieczeństwa Danych Osobowych obowiązuje wszystkich pracowników, praktykantów, wolontariuszy i stażystów jednostki oraz podmioty realizujące zadania na podstawie podpisanej z jednostką umowy cywilnoprawnej, a także pracownicy i współpracownicy podmiotów trzecich, z którymi została zawarta umowa, na mocy której ww. osoby mają dostęp do informacji chronionych, w tym do danych osobowych.

Polityka ma zastosowanie do wszystkich danych osobowych oraz innych informacji podlegających ochronie, przetwarzanych w pomieszczeniach jednostki niezależnie od formy ich przetwarzania. Instrukcja Zarządzania Systemem Informatycznym obowiązuje wszystkie osoby mające dostęp do danych osobowych w systemach informatycznych zgodnie z upoważnieniem udzielonym przez administratora.

## 3. CELE POLITYKI

Do podstawowych celów stosowania Polityki Bezpieczeństwa Danych Osobowych należy zaliczyć:

- określenie reguł postępowania oraz dostępu do danych osobowych przez osoby biorące udział w procesach przetwarzania,
- określenie obowiązków osób biorących udział w procesach przetwarzania danych osobowych,
- określenie sposobów zabezpieczenia danych poprzez czynności organizacyjne czy środki techniczne,
- określenie zasad oraz sposobów reagowania na zagrożenia występujące w procesach przetwarzania danych osobowych,
- zapewnienie odpowiedniej wiedzy w odniesieniu do ochrony danych osobowych,
- zapewnienia bezpieczeństwa danych osobowych podczas ich przetwarzania w postaci tradycyjnej poprzez zastosowanie procedur postępowania z danymi osobowymi,

Celem stosowania Instrukcji Zarządzania Systemem Informatycznym jest:

- określenie zasad oraz reguł postępowania z danymi osobowymi przetwarzanymi w formie elektronicznej,
- określenie zasad dostępu do danych osobowych przetwarzanych w systemach teleinformatycznych,
- opis technicznego sposobu zabezpieczenia sprzętu umożliwiającego przetwarzanie danych osobowych w systemach teleinformatycznych.

## 4. AKTY PRAWNE

- 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L Nr 119),
- Konstytucja RP z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.),
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U.2019.1781),
- 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 (t.j. Dz.U.2017.2247 ),
- Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40 z późn. zm.);
- Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2022 r. poz. 1634 z późn. zm.);
- Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 z późn. zm.);
- Ustawa z dnia 24 września 2010 r. o ewidencji ludności (t.j. Dz. U. z 2022 r. poz. 1191 z późn. zm.).
- Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (t.j. Dz. U. z 2021 r. poz. 2268 z późn. zm.).
- Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe (t.j. Dz. U. z 2021 r. poz. 1082 z późn. zm.);
- Ustawa z dnia 27 października 2017 r. o finansowaniu zadań oświatowych (t.j. Dz. U. z 2022 r. poz. 2082 z późn. zm.);
- Ustawa z dnia 7 września 1991 r. o systemie oświaty (t.j. Dz.U. z 2022 r. poz. 2230);
- Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz.U. z 2022 r. poz. 1009 z późn. zm.)

- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2022 r. poz. 2000 z późn. zm.)
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2022 r. poz. 1360 z późn. zm.);
- Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (t.j. Dz. U. z 2023 r. poz. 344);
- Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (t.j. Dz. U. z 2022 r. poz. 503 z późn. zm.);
- Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2022 r. poz. 2519 z późn. zm.);
- Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (t.j. Dz. U. z 2023 r. poz. 537);
- Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (t.j. Dz. U. z 2022 r. poz. 530); Rozporządzenie Rady Ministrów z dnia 25 października 2021 r. w sprawie wynagradzania pracowników samorządowych (t.j. Dz.U. z 2021 poz. 1960);
- ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (t.j. Dz. U. z 2022 r. poz. 2240);
- ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (t.j. Dz. U. z 2023 r. poz. 46);
- ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach (t.j. Dz. U. z 2023 r. poz. 519 z późn. zm.);
- ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz. U. z 2022 r. poz.479 z późn. zm.);
- Ustawa z dnia 21 marca 1985 r. o drogach publicznych (t.j. Dz. U. z 2023 r. poz. 645);
- Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców (t.j. Dz. U. z 2023 r. poz. 221);
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2022 r. poz. 2000 z późn. zm.);
- Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2020 r. poz. 164 z późn. zm.);
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2019 r. poz. 742 z późn. zm.);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902);
- Statut Gminy
- inne ustawy i przepisy wykonawcze nakładające na gminy zadania o charakterze publicznym mające na celu zaspokojenie zbiorowych potrzeb mieszkańców oraz załatwienie indywidualnych spraw jego mieszkańców.

## 5. DEFINICJE

**Administrator Danych Osobowych (ADO)** – to osoba fizyczna lub prawna, organ publiczny, jednostka 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;

**Inspektor Ochrony Danych (IOD)** – osoba fizyczna powołana do wsparcia ADO w realizacji obowiązków dotyczących ochrony danych osobowych i wpisana do prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych rejestru.

**Polityka** – Polityka Bezpieczeństwa Danych Osobowych

**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);

**UoODO -** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

**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;

**Szczególna kategoria danych osobowych -** dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia;

**Dane biometryczne -** dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO);

**Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (art. 4 pkt 15 RODO);

**Zbiór danych -** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

**Upoważnienie-** dokumenty wydany przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, może również określać identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;

**Osoba upoważniona do przetwarzania danych osobowych** - osoba, która otrzymała odpowiednie imienne upoważnienie od ADO i złożyła oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych;

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

**Odbiorca danych -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

**Organizacja międzynarodowa -** oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

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

**Strona trzecia -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

**Użytkownik/pracownik (w tym podmiotu trzeciego) -** osoba przetwarzająca dane na podstawie upoważnienia ADO w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w jednostce lub formy prawnej wiążącej z tą

osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

**Naruszenie ochrony danych osobowych -** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

**Przetwarzanie –** oznacza każda 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;

**Profilowanie –** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

**Pseudonimizacja -** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

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

**Nośnik komputerowy (wymienny)** - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dysku flash, pendrive;

**Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

**Identyfikator / login** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

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

**Uwierzytelnianie –** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

**Sieci telekomunikacyjnej –** rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 32 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne;

**Sieci publicznej –** rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne;

**Teletransmisji –** rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

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

**Zasada integralności i poufności -** oznacza przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

**Zasada merytorycznej poprawności** - oznacza, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

**Zasada minimalizacji danych -** oznacza, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

**Zasada ograniczenia celu** - oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

**Zasada ograniczenia przetwarzania** - oznacza, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów

archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;

**Zasada rozliczalności -** ADO jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie;

**Zasada zgodności z prawem, rzetelności i przejrzystości** - oznacza przetwarzanie danych wyłącznie w przypadku spełnienia jednego ze wskazanych w RODO warunków (art. 6 i 9) oraz przekazanie osobie, której dane są pozyskiwane informacji określonych w art. 13 i 14.

# 6. PRZETWARZANIA DANYCH OSOBOWYCH ORAZ PODSTAWY PRZETWARZANIA

***Definicja przetwarzania danych osobowych***

***Zgodnie z art. 4 pkt 2 rozporządzenia RODO „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 przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie***

**Podstawy prawne przetwarzania danych osobowych definiuje Artykuł 6 RODO**

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
   - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych w jednym lub większej liczbie określonych celów;
   - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

2. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c) i e); w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX
3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:
   - w prawie Unii; lub
   - w prawie państwa członkowskiego, któremu podlega administrator.
     - Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można

ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

- wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
- kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
- charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;
- ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
- istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania (Procedura nr 2) lub pseudonimizacji.

# 7. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

**Poniżej przedstawiono ogólne zasady dotyczące przetwarzania danych osobowych zdefiniowane przez Artykuł 5 RODO**

Dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
- prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

# 8. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

***Art. 4 pkt 12 RODO naruszenie ochrony danych osobowych jest naruszeniem bezpieczeństwa prowadzącym do niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.***

***Administrator powinien zgłaszać organowi nadzorczemu każdy przypadek naruszenia ochrony danych osobowych zgodnie z procedurą* „Procedura nr. 1.”*, chyba że „jest mało prawdopodobne, by incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych”.***

***Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono.***

**Szczególne obowiązki administratora związane z naruszeniem ochrony danych osobowych**

- wprowadzenie procedury określającej sposób postępowania z naruszeniem **„Procedura nr 1”,**
- prowadzenie rejestru naruszeń; „**Załącznik nr 2**”
- zgłaszanie naruszeń organowi nadzorczemu (dokonuje również pełnomocnik administratora);
- powiadamianie osoby, której dane dotyczą, o naruszeniu; „**Załącznik nr 3**”
- podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.

**Identyfikacja zdarzenia jako naruszenie ochrony danych**

Aby zdarzenie można było zidentyfikować jako naruszenie, muszą być spełnione łącznie następujące przesłanki:

- naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie;
- skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
- naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

**Termin zgłoszenia naruszenia**

Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator **bez zbędnej zwłoki** – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO.

**Organ właściwy do zgłaszania naruszeń ochrony danych osobowych**

Organem tym jest Prezes Urzędu Ochrony Danych Osobowych. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl

**Zawiadomienie osoby, której dane dotyczą o naruszeniu „Załącznik nr 3"**

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi bez zbędnej zwłoki zawiadomić osobę której dane dotyczą, o takim naruszeniu

**Procedura nr 1**

***Procedura określająca sposób postępowania z naruszeniem ochrony danych osobowych***

*Zgodnie z art. 33 i 34 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1)*

**§1 Cel procedury**

Celem procedury jest określenie sposobu postępowania w przypadku uzasadnionego podejrzenia naruszenia danych osobowych lub naruszenia ochrony danych.

## §2 Zakres stosowania

Procedurę należy stosować w każdym przypadku, kiedy pracownik jednostki ma uzasadnione podejrzenie, iż mogło dojść do naruszenia ochronę danych osobowych. Procedura dotyczy wszystkich pracowników administratora.

## §3 Identyfikacja zdarzenia

Naruszenie bezpieczeństwa przetwarzanych danych osobowych, określone jest jako przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

## §4 Obowiązki osoby identyfikującej naruszenie

W każdym przypadku, kiedy pracownik jednostki ma uzasadnione podejrzenie, iż mogło dojść do naruszenia ochronę danych osobowych lub doszło do naruszenia ochrony danych zobowiązany jest niezwłocznie, najpóźniej w ciągu 24 godzin po stwierdzeniu naruszenia lub uzasadnionego podejrzenia, iż doszło do naruszenia ochrony danych osobowych zawiadomić Inspektora Ochrony Danych lub Administratora Danych Osobowych. Jeżeli mimo uzasadnionego podejrzenia, iż mogło dojść do naruszenia ochrony danych osobowych lub naruszenia ochrony danych osobowych, pracownik jednostki nie zgłosi Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych tego faktu, to zobowiązany jest do wyjaśnienia przyczyny opóźnienia na piśmie w ciągu 24 godzin. Wyjaśnienie na piśmie przedkłada Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych. Niewywiązanie się ze zobowiązań w zakresie ochrony danych osobowych skutkuje nałożeniem na pracownika odpowiedzialności zgodnie z obowiązującymi przepisami prawa w szczególności Kodeksem Pracy

## §5 Wyłączenia zgłoszenia

Zgłoszenia o uzasadnionym podejrzeniu naruszenia ochrony danych, naruszeniu ochrony danych nie dokonuje się jeśli jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, jednak decyzję o tym podejmuje Administrator Danych Osobowych w porozumieniu z Inspektorem Ochrony Danych.

## §6 Sposób reagowania na naruszenie

Sposób reagowania na naruszenia przez pracowników, którzy je ujawnili;

- należy niezwłocznie poinformować o zdarzeniu osobę nadzorującą, Administratora Danych Osobowych, Inspektora Ochrony Danych;
- miejsce zdarzenia powinno się pozostawić w stanie nienaruszonym do czasu przybycia inspektora ochrony danych lub innej osoby nadzorującej;
- zebrane materiały powinno się przedstawić administratorowi danych, który z pomocą inspektora ochrony danych, w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych powinien ocenić, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą;

## §7 Termin zgłoszenia

W przypadku naruszenia ochrony danych osobowych w organizacji, Administrator Danych lub Inspektor Ochrony Danych bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, jest zobowiązany zgłosić takie naruszenie organowi nadzorczemu – Prezesa Urzędu Ochrony Danych Osobowych.

## §7 Poinformowanie osób, których naruszenie dotyczy

W przypadku, gdy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych należy również poinformować osobę, której dane dotyczą „**Załącznik nr 3**”

## §8 Zgłoszenie naruszenia

Zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych powinno odbyć się zgodnie z art. 33 ust. 3 RODO.

## §9 Rejestr naruszeń

W rejestrze naruszeń ochrony danych osobowych powinny znaleźć się wszystkie zdarzenia zidentyfikowane jako naruszenia bez względu na to czy podlegają one zgłoszeniu czy nie. „**Załącznik nr 2**”

# 9. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

***Administrator Danych Osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia:***

- wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem i aby móc to wykazać;
- odpowiada za stworzenie i funkcjonowanie systemu ochrony danych , w tym: stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną a w szczególności zabezpiecza dane przed:
  - udostępnieniem osobom nieupoważnionym;
  - zabraniem przez osobę nieuprawnioną;
  - zmianą, utratą, uszkodzeniem lub zniszczeniem.
- zapewnia by przetwarzanie danych osobowych było zgodne z prawem, w oparciu o obowiązujące przepisy prawa regulujących realizację zadań własnych i zleconych, również w obszarze przetwarzania i bezpieczeństwa danych osobowych;
- prowadzi oraz wdraża dokumentację dotyczącą przetwarzania danych osobowych, w szczególności:
  - politykę Bezpieczeństwa Danych Osobowych oraz Instrukcję Zarządzania Systemem Informatycznym;
  - rejestr czynności przetwarzania;
  - retencję danych (chyba, że okresy przechowywania danych zostały oznaczone w Rejestrze Czynności Przetwarzania);
  - wykaz osób upoważnionych do przetwarzania;
  - rejestr naruszeń;
  - inne procedury regulujące kwestie bezpieczeństwa danych osobowych.
- wyznacza Inspektora Ochrony Danych;
- odpowiada za bezpieczeństwo systemów informatycznych służących do przetwarzania danych osobowych;

- nadaje upoważnia pracownikom do przetwarzania danych osobowych w systemach informatycznych zgodnie z zakresem obowiązków użytkowników systemu;
- organizuje i zapewnia:
  - szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony **„Załącznik nr 1”,**
  - okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,
  - okresową ocenę skutków dla ochrony danych osobowych **„Procedura nr 5”**
  - kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,
  - monitorowanie zastosowanych środków ochrony,
  - możliwość realizacji wytycznych, jeśli zostaną wskazane przez UoODO.
  - wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi, jeśli jest to niezbędne w wybranych przypadkach:
  - pseudonimizację i szyfrowanie danych osobowych;
  - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
  - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
  - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

**Procedura nr 5**

***Procedura oceny skutków dla ochrony danych***

## §1 Cel procedury

Celem procedury jest zidentyfikowanie zagrożeń oraz określenie poziomu ryzyka występującego przy przetwarzaniu danych osobowych i oszacowanie jego skutków

## §2 Zakres stosowania

Procedura ma zastosowanie we wszystkich komórkach organizacyjnych jednostki, w których dochodzi do przetwarzania danych osobowych.

## §3 Odpowiedzialność

Administrator jest odpowiedzialny za akceptację poziomu ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Dokonując oceny skutków administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

## §4 Rodzaje przetwarzania kwalifikujące się do oceny skutków

Ocenę skutków ryzyka dla ochrony danych osobowych stosuje się w szczególności w przypadku

- Ewaluacja lub ocena, w tym profilowanie i przewidywanie w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych,
- Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki,
- Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa,
- Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych,
- Przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu,
- Przetwarzanie danych genetycznych,
- Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy:
  • liczby osób, których dane są przetwarzane,
  • zakresu przetwarzania,
  • okresu przechowywania danych,
  • geograficznego zakresu przetwarzania,
- Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł,
- Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi,
- Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych,
- Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy,
- Przetwarzanie danych lokalizacyjnych.

Powyższy wykaz nie zwalnia administratora z obowiązku przeanalizowania wszelkich operacji przetwarzania danych w oparciu o pełną ocenę skutków dla ochrony danych. Przykłady powyższych operacji przetwarzania, w których może wystąpić wysokie ryzyko naruszenia nie mają charakteru wyczerpującego.

## §5 Analiza ryzyka

a. Opis planowanych operacji przetwarzania (w jakim celu, zakresie i czasie będą przetwarzane dane osobowe)
   ……
   ……

b. Ocena konieczności i proporcjonalności (czy zakres przetwarzanych danych, zakres osób, których dane przetwarzamy, a także zakres odbiorców którym te dane udostępniamy, jest niezbędny z punktu widzenia celów i podstaw prawnych przetwarzania)

……
……

c. Środki planowane w celu wykazania zgodności (opisujemy przez wskazanie zabezpieczeń organizacyjnych i technicznych, a także rekomendacji dotyczących usunięcia wykrytych niezgodności)

……
……

d. Ocena ryzyka naruszenia praw lub wolności

**Określenie poziomu ryzyka**

| **Waga naruszenia** | **Opis** |
|---|---|
| Niska | Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności |
| Średnia | Osoby mogą dotknąć niedogodności, które są możliwe do pokonania |
| Wysoka | Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami |
| Bardzo wysoka | Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje |

| **Prawdopodobieństwo** | **Opis** |
|---|---|
| Niskie | Zdarzenie prawie nieprawdopodobne |
| Średnie | Zdarzenie mało prawdopodobne |
| Wysokie | Zdarzenie wysoce prawdopodobne |

Bardzo wysokie Zdarzenie niemal pewne

Poziom ryzyka stanowi iloczyn wagi zagrożenia oraz prawdopodobieństwa jego wystąpienia dla danego obszaru operacji przetwarzania danych jaką jest nauczanie zdalne.

| | | | | | |
|---|---|---|---|---|---|
| **WAGA** | Bardzo wysoka (4) | 4 | 8 | 12 | 16 |
| | Wysoka (3) | 3 | 6 | 9 | 12 |
| | Średnia (2) | 2 | 4 | 6 | 8 |
| | Niska (1) | 1 | 2 | 3 | 4 |
| | | Niskie (1) | Średnie (2) | Wysokie (3) | Bardzo wysokie (4) |
| | **Prawdopodobieństwo** | | | | |

**Skala dopuszczalności ryzyka**

| Ocena ryzyka | Dopuszczalność ryzyka | Działania |
|---|---|---|
| Ryzyko bardzo wysokie<br>poziom: 12-16 | Nieakceptowalne | Przetwarzanie danych osobowych nie może być podjęte ani kontynuowane do czasu obniżenia poziomu ryzyka do dopuszczalnego. |
| Ryzyko wysokie<br>poziom: 8-11 | Dopuszczalne | Przetwarzanie danych osobowych jest dopuszczalne, ale konieczna jest ocena skutków dla ochrony danych osobowych oraz podjęcie działań zmierzających do obniżenia poziomu ryzyka do akceptowalnego. |
| Ryzyko średnie - akceptowalne | Akceptowalne | Przetwarzanie danych osobowych jest dopuszczalne, konieczne jest podejmowanie |

| | | |
|---|---|---|
| poziom: 4-7 | | działań mających na celu obniżanie poziomu ryzyka i niedopuszczenie do wzrostu jego poziomu. |
| Ryzyko nieznaczne lub pomijalne<br>poziom: 1-3 | Niskie | Przetwarzanie danych osobowych jest dopuszczalne, konieczne jest podejmowanie działań mających na celu obniżanie poziomu ryzyka i niedopuszczenie do wzrostu jego poziomu. |

Poziom ryzyka dla czynności przetwarzania…….. wynosi……

e. Środki planowane w celu wyeliminowania ryzyka (ustala się na podstawie rekomendacji wydanych w poprzednim kroku. Realizując je, najczęściej niwelujemy podatności, z których wynika możliwość wystąpienia zagrożenia)

……
……

Po wdrożeniu środków należy sprawdzić ponownie poziom ryzyka tak aby był on na poziomie akceptowalnym.

Poziom ryzyka dla czynności przetwarzania po wdrożeniu środków…….. wynosi……

f. Decyzja administratora

Jeśli ryzyko jest wysokie, a nie planujemy go zminimalizować, to musimy skonsultować się z Prezesem UODO (art. 36 RODO).

……

Administrator Danych Osobowych

# 10. KWALIFIKCJE, UPRAWNIENIA I OBOWIĄZKI INSPEKTORA OCHRONY DANYCH

***W przypadku kiedy Administrator Danych Osobowych powołuje Inspektora Ochrony Danych jest on odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych.***

**Kwalifikacje IOD:**

Inspektor Ochrony Danych:

- powinien posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,
- posiadać wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz posiadać znajomość aktów prawa z zakresu ochrony danych,
- powinien wykonywać zadania niezależnie i bez konfliktu interesów,

**Uprawnienia IOD**

Inspektora Ochrony Danych jest uprawniony w szczególności do:

- wstępu do pomieszczeń, w których przetwarzane są dane osobowe;
- odbierania wyjaśnień od osób przetwarzających dane osobowe;
- dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, UoODO, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług;
- prowadzeniu wewnętrznej kontroli z zakresie ochrony danych osobowych;
- wydawaniu rekomendacji związanych z poszczególnymi sytuacjami związanymi z ochroną danych osobowych.

**Zadania i obowiązki IOD**

- jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi;
- powinien informować ADO oraz użytkowników/ pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących

przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie;

- powinien współpracować z organem nadzorczym, pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem;
- weryfikuje zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
- powinien wspierać ADO w realizacji i przygotowywaniu odpowiedzi na żądania osób, których dane dotyczą, uzyskania od ADO potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych;
- informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania danych osób, które wystąpiły z takim żądaniem;
- współprowadzi i aktualizuje rejestr czynności przetwarzania;
- aktualizuje rejestr naruszeń bezpieczeństwa, zgodnie ze wzorem wskazanym w „**Załącznik nr 2**"
- przygotowuje i przekazuje do podpisu do Administratora Danych Osobowych zgłoszenia o naruszeniu ochrony danych osobowych do organu nadzorczego oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO;
- współprowadzi i aktualizuje rejestr umów powierzenia przetwarzania danych, zgodnie ze wzorem wskazanym w „**Załącznik nr 8**";
- nadzoruje i monitoruje procesy profilowania (o ile taki ma miejsce);
- opiniuje umowy zawierane z podmiotami trzecimi w zakresie ich zgodności z przepisami prawa powszechnie obowiązującego i wewnętrznego w zakresie ochrony danych osobowych;
- nadzoruje i monitoruje realizację obowiązku informacyjnego, zgodnie z wymogami RODO;
- kontroluje ewidencje upoważnień do przetwarzania danych osobowych oraz dokumentację związaną z udzielaniem upoważnień, zgodnie ze wzorem zawartym w „**Załącznik nr 5**";
- przygotowuje wzory upoważnień do przetwarzania danych osobowych zgodnie ze wzorem zawartym w „**Załącznik nr 4**"oraz konsultuje w zakresie niezbędności upoważniania oraz

zakresu upoważnienia dla poszczególnych użytkowników/pracowników z zachowaniem zasady adekwatności .

- okresowo dokonuje wewnętrznych kontroli, które w szczególności obejmują weryfikację:
  - zabezpieczeń: organizacyjnych i technicznych zbiorów danych osobowych,
  - weryfikację osób upoważnionych do przetwarzania danych osobowych
  - weryfikuje i kontroluje stan wiedzy pracowników w zakresie ochrony danych osobowych
  - zleca informatykowi lub pracownikowi upoważnionemu prze ADO kontrolę systemów informatycznych w jednostce
  - weryfikuje zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w jednostce zabezpieczeniami organizacyjno- technicznymi.

***Szczegółowy zakres uprawnień Inspektora Ochrony Danych określa RODO i UoODO.***

# 11. OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

***Każdy użytkownik/pracownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez ADO i tylko w celu wykonywania powierzonych mu obowiązków.***

***Nieprzestrzeganie zasad ochrony danych osobowych, w tym zasad określonych w Polityce stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności porządkowej określonej w Kodeksie Pracy.***

**Obowiązki wynikające z zasad odnoszących się do zabezpieczeń organizacyjnych**

Każda osoba przetwarzająca dane osobowe na potrzeby jednostki jest zobowiązana do:

- zapoznania się z treścią przedmiotowej Polityki co powinno być potwierdzone podpisanym oświadczeniem „**Załącznik nr 6”,** oraz bezwzględnie stosować się do jej

zapisów. Osoby przetwarzające dane osobowe czynią to na podstawie wydanego przez ADO - upoważnienia „**Załącznik nr 4”;**

- przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych;
- zachowania tajemnicy danych przetwarzanych w siedzibie ADO potwierdzone podpisanym oświadczeniem o zachowaniu danych w poufności „**Załącznik nr 7”,**, w tym także wobec osób najbliższych;
- zgłaszania każdego naruszenia bezpieczeństwa w zakresie ochrony danych osobowych do ADO i IOD, a w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych ADO i dodatkowo Informatykowi obsługującego jednostkę;
- odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieuprawnionym;
- wnioskowania o zewidencjonowanie nowych zbiorów danych osobowych w rejestrze czynności przetwarzania współprowadzonego przez Inspektora Ochrony Danych,
- bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony;
- występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,

**Obowiązki wynikające z zasad odnoszących się do zabezpieczeń technicznych**

Każda osoba przetwarzająca dane osobowe na potrzeby jednostki jest zobowiązana do:

- niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe pod nieobecność osoby upoważnionej do przetwarzania danych osobowych;
- chowania do szaf zamykanych na klucz wszelkich dokumentów, wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
- usuwania przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy;
- nieużywania powtórnego jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe;
- chowania do zamykanych na klucz szaf wszelkich dokumentów zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;

- umieszczaniu kluczy do pomieszczeń i do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy i nieujawnianie osobom nieupoważnionym informacji o miejscu przechowywania kluczy;
- zamykania okien w razie zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
- zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
- zamykania drzwi na klucz i zabierania go ze sobą w przypadku czasowego opuszczenia pomieszczenia;
- niepozostawiania kluczy w drzwiach od strony zewnętrznej pomieszczeń, w których przetwarza się dane osobowe, także podczas obecności wewnątrz pomieszczeń osób upoważnionych;
- zamykania drzwi na klucz po zakończeniu pracy w danym dniu i składania klucza w przeznaczonym do tego miejscu wskazanym przez ADO.

**Obowiązki wynikające z zasad odnoszących się do zabezpieczeń w systemach informatycznych**

Każda osoba przetwarzająca dane osobowe na potrzeby jednostki jest zobowiązana do:

- pilnego strzeżenia nośników danych, w tym akt, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie;
- ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
- zabezpieczenie nośnika, na którym zapisano hasła, w taki sposób by był niedostępny dla osób trzecich;
- niepodłączania prywatnych, nieautoryzowanych nośników danych do infrastruktury;
- niepodłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia;
- dbania o prawidłową wentylację komputerów;

- przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń IOD i informatyka ;
- opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
- przesyłania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej (Procedura nr 2);
- nie wynoszenia poza obszar ADO na jakichkolwiek nośnikach zbiorów danych lub ich części, chyba że pracownik do takiego działania zostanie wyraźnie upoważniony przez ADO lub osobę przez niego upoważnioną, wówczas wynoszone dane muszą mieć postać zaszyfrowaną;
- wykonywania kopii danych, na których się pracuje, tak często, jak jest to niezbędne aby zapobiec ich utracie;
- kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika oraz wyłączeniu komputera, a także zabezpieczenia pomieszczenia, w którym się on znajduje.

**Obowiązki dotyczące użytkowników mających szczególny wpływ na zabezpieczenia w zakresie ochrony danych osobowych**

- osoby odpowiedzialne za zarządzanie kadrami w jednostce informują niezwłocznie ADO i/lub IOD, a także informatyka nadającego zakres upoważnień do systemów informatycznych o każdej zmianie w zakresie czynności użytkowników/ pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania danych osobowych;
- osoba wyznaczona i upoważniona przez ADO do zabezpieczenia systemu informatycznego :
  - przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego zgodnie z zakresem obowiązków oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w polityce, przydzielenie identyfikatora oraz hasła do systemu informatycznego może nastąpić wyłącznie w odniesieniu do osoby posiadającej upoważnienie do przetwarzania danych osobowych;

- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
- nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
- podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
- w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO i IOD o naruszeniu oraz współdziała z nimi przy usuwaniu skutków naruszenia;
- prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
- wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe;
- wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
- dba o aktualizację oprogramowań specjalistycznych, programów antywirusowych i zabezpieczeń systemowych.

***Rozliczenie użytkownika/pracownika z przestrzegania ochrony danych osobowych powinno odbywać się na podstawie wewnętrznych procedur określonych przez ADO.***

# 12. ZASADY DOSTĘPU DO DANYCH OSOBOWYCH PRACOWNIKÓW

***Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby upoważnione przez Administratora Danych Osobowych.***

**Zasady regulujące dostęp do danych osobowych**

- upoważnienie do przetwarzania danych osobowych należy wydawać przed rozpoczęciem wykonywania czynności związanych z ich przetwarzaniem **(Załącznik nr 4)**
- dane osobowe możne przetwarzać wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych, w zawartym upoważnieniu i tylko w celu wykonywania obowiązków służbowych;
- w przypadku odwołania upoważnienia należy dopilnować, by osobie, której odwołuje się upoważnienie, faktycznie odebrano dostępy do dokumentacji papierowej, na której zapisane są dane osobowe, ale również do systemów informatycznych oraz zasobów;
- zakończenie współpracy z podmiotem trzecim powoduje wygaśnięcie upoważnienia do przetwarzania danych udzielonych pracownikom i współpracownikom tego podmiotu;
- rozwiązanie stosunku pracy, stosunku cywilnoprawnego lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
- w dokumentach/aktach osobowych użytkownika/pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez użytkownika/pracownika, co jednocześnie jest potwierdzeniem, że użytkownik/pracownik przyjął treść upoważnienia do wiadomości;
- personel pomocniczy, realizujący pracę fizyczną u ADO zobowiązany jest do podpisania klauzuli poufności zgodnie ze wzorem **(Załącznik nr 7)**, w związku z tym, iż w trakcie wykonywania swoich czynności może mieć dostęp do danych osobowych.

# 13. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

***Art. 28 ust. 1 RODO (uzupełniony treścią motywu 81 RODO), zobowiązuje administratora, do korzystania jedynie z takich podmiotów, które gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających, że przetwarzanie spełnia wymogi RODO oraz chroni prawa osób, których dane są przetwarzane.***

***Powierzenie danych osobowych zachodzi w sytuacji gdy podmiot przetwarzający dokonuje operacji na danych osobowych na zlecenie administratora, który powierza przetwarzanie danych osobowych w drodze umowy zawartej na piśmie.***

**Umowa powierzenia przetwarzania danych osobowych**

Umowa powierzenia przetwarzania danych osobowych **„Załącznik nr 9”,** powinna zawierać:

- określenie administratora danych;
- określenie podmiotu przetwarzającego dane na zlecenie administratora;
- charakter i cel przetwarzania;
- przedmiot i czas trwania przetwarzania;
- rodzaj powierzanych danych osobowych oraz kategorie osób, których dane dotyczą;
- obowiązki i prawa administratora;
- oświadczenia procesora, wskazujące jego obowiązki.

**Podmiot przetwarzający podpisując umowę powierzania z ADO powinien oświadczyć między innymi, że:**

- przetwarza dane osobowe jedynie na polecenie administratora;
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
- podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
- pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

***Jeśli powierzenie danych następuje w związku z realizacją umowy głównej, stosowne zapisy dotyczące powierzenia danych mogą znaleźć się w przedmiotowej umowie.***

## 14. UDOSTĘPNIENIE DANYCH OSOBOWYCH

***Udostępnienie danych osobowych jest przekazaniem określonych informacji do innego podmiotu. W związku z udostępnieniem administrator nie ma kontroli nad przetwarzaniem tych danych, a więc nie decyduje o sposobie i celach przetwarzania przekazanych danych osobowych.***

**Komu ADO może udostępniać dane osobowe**

- ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa zgodnie z (Procedura nr 3);
- Dane osobowe mogą być również udostępniane w następujących przypadkach:
  - na podstawie umowy z innym podmiotem, w ramach, której istnieje konieczność udostępnienia danych;
  - na podstawie wniosku osoby, której dane dotyczą.

**Zasady udostępnienia danych osobowych**

- wniosek o realizację praw powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi (Załącznik nr 10)**;**
- w przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie do 30 dni od daty jego otrzymania;
- udostępnieniu nie powinien podlegać cały zbiór danych osobowych;
- administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych, za każdą kolejną kopie administrator może pobrać opłatę pokrywającą koszty administracyjne;
- udostępnienie danych osobowych nie jest jednoznaczne z udostępnieniem dokumentów zawierających te dane, informacje mogą być udostępnione w formie przetworzonej;
- udostępnienie musi zapewniać poufność;
- jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną, stosując szyfrowanie (Procedura nr 2);
- wnioski o udostępnienie należy przechowywać do celów dowodowych, a także obrony przed ewentualnymi roszczeniami.

**Procedura nr 2**

***Procedura szyfrowania nośników zawierających dane osobowe***

## §1 Cel procedury

Celem procedury jest zdefiniowanie czynności jakie występują w procesie szyfrowania danych osobowych.

## §2 Zakres stosowania

Procedura dotyczy wszystkich osób, które korzystają z systemów teleinformatycznych oraz przesyłają dane osobowe do innych administratorów za pomocą poczty email czy też przenoszą dane na nośnikach fizycznych

## §3 Szyfrowanie systemowe

Aby zaszyfrować dane, które chcemy przesłać czy skopiować na inny nośnik możemy skorzystać z opcji szyfrowania dostępnej w systemie Windows. Aby to zrobić należy postępować zgodnie z krokami opisanymi poniżej.

- Kliknij prawym przyciskiem myszy (lub naciśnij i przytrzymaj) plik lub folder i wybierz pozycję **Właściwości**.
- Kliknij przycisk **Zaawansowane** i zaznacz pole wyboru polecenie **Szyfruj zawartość, aby zabezpieczyć dane**.
- Naciśnij przycisk **OK**, aby zamknąć okno **Atrybuty zaawansowane**, naciśnij przycisk **Zastosuj**, a następnie wybierz pozycję **OK**.

## §4 Tworzenie archiwum

Innym sposobem szyfrowania jest utworzenie archiwum z plikami z wykorzystaniem dostępnych programów. Każdy z programów dostępnych na rynku umożliwia tworzenie archiwum zabezpieczonego hasłem. Korzystanie z nich opisane jest w instrukcji użytkowania tych programów.

## §5 Usuwanie kopii danych

Zbędne dane, które nie są już niezbędne do zrealizowania celu, w jakim zostały skopiowane na nośnik danych, użytkownik usuwa niezwłocznie z nośnika danych.

## §6 Udostępnianie hasła

Hasło do zaszyfrowanych plików najlepiej jest wysłać innym środkiem komunikacji elektronicznej, w taki sposób aby mieć pewność że trafia ono bezpośrednio do osoby upoważnionej do otwarcia danych.

***Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.***

**Procedura nr 3**

***Procedura udostępniania danych osobowych***

**§1 Cel procedury**

Celem procedury jest zdefiniowanie czynności jakie występują w procesie udostępniania danych osobowych oraz ich usystematyzowanie

**§2 Zakres stosowania**

Procedura dotyczy osób uprawnionych do udostępniania danych osobowych przetwarzanych przez administratora oraz wszystkich danych będących danymi osobowymi podlegającymi udostępnieniu.

**§3 Składanie wniosku**

Wnioskodawca ubiegający się udostępnienie danych osobowych ze zbiorów administratora składa stosowny wniosek na wzorze dostępnym u administratora (Załącznik nr 10)

**§4 Weryfikacja**

Przed udostępnieniem danych osobowych konieczna jest weryfikacja podstawy prawnej udostępnienia oraz tożsamości wnioskodawcy, a także konsultacja z wyznaczonym w jednostce inspektorem ochrony danych.

**§5 Obowiązek informacyjny**

Wobec wnioskodawcy należy zrealizować obowiązek informacyjny w związku ze złożonym wnioskiem o udostępnienie oraz jego realizacją.

**§6 Ewidencjonowanie**

Osoba odpowiedzialna za realizację żądania uzupełnia w rejestrze udostępnień danych osobowych (Załącznik nr 11) informacje dotyczące realizacji żądania udostępnienia.

# 15. PRZEKAZANIE DANYCH DO PAŃSTWA TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODOWEJ.

**Zasady przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych**

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
2. W razie braku decyzji, o której mowa w pkt 1 Administrator Danych Osobowych lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowane prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.
3. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 2, w tym wiążących reguł, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:
   - osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
   - przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przed umownych podejmowanych na żądanie osoby, której dane dotyczą,

- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

***Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały określone w RODO. O wyrażenie zgody na przekazanie danych występuje właściciel zbioru, wskazując cel i zakres przekazywanych danych. Zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej może wydać ADO po zasięgnięciu opinii Inspektora Ochrony Danych. ADO zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.***

## 16. OBOWIĄZEK INFORMACYJNY

***Administrator Danych Osobowych zobowiązany jest (niezależnie od tego, czy zbiera dane bezpośredniego od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) spełnić obowiązek informacyjny na zasadach określonych w RODO.***

**Zasady dotyczące spełniania obowiązku informacyjnego**

- wykonanie obowiązku informacyjnego musi nastąpić przy pierwszej czynności skierowanej do strony, chyba że strona posiada już informację o sposobie przetwarzania jej danych, a ich zakres i cel nie uległ zmianie;

- informowanie powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględniać także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu;
- w przypadku zmiany celu przetwarzania danych osobowych na inny cel, niż dla którego dane osobowe zostały zebrane, administrator powinien poinformować osobę, której dane dotyczą, o tym innym celu;
- administrator obowiązany jest do spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą także w sytuacji, w której pozyskuje nowe, ze swojej perspektywy, dane osobowe;
- administrator nie musi przekazywać danych wymagany przez art. 14 RODO w momencie, gdy:
  - okaże się to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja ta może zachodzić w szczególności w przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym o ile obowiązek informacyjny może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania;
  - pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
  - dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

**Treść obowiązku informacyjnego**

Jeżeli dane osobowe pozyskujemy bezpośrednio od osoby, której one dotyczą obowiązek informacyjny, zgodnie z art. 13 RODO, powinien zawierać:

- tożsamość i dane kontaktowe administratora (ewentualnie jego przedstawiciela);
- dane kontaktowe inspektora ochrony danych (jeżeli został powołany);

- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
- wyjaśnienie prawnie uzasadnionego interesu realizowanego przez administratora lub przez stronę trzecią (jeżeli podstawą przetwarzania danych jest art. 6 ust. 1 lit. f RODO);
- listę odbiorców danych osobowych lub ich kategorie (jeżeli przetwarzane dane osobowe będą przekazywane np. do podmiotów przetwarzających dane lub innych administratorów danych);
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia;
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania albo o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- informacje o prawie do cofnięcia zgody (jeżeli stanowiła ona podstawę prawną przetwarzania danych);
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, z uwzględnieniem informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli podstawą realizacji obowiązku informacyjnego będzie art. 14 RODO, oprócz wyżej wymienionych informacji administrator jest zobowiązany podać:

- kategorie danych, które przetwarza;
- źródło pozyskania danych.

# 17. ZASADY REALIZACJI PRAW OSÓB

***Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO administrator danych rozpatruje indywidualnie w oparciu o wniosek o realizacje praw.***

Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

- prawo dostępu do danych,
- prawo do sprostowania danych,
- prawo do usunięcia danych,
- prawo do ograniczenia przetwarzania danych,
- prawo do przenoszenia danych,
- prawo do sprzeciwu wobec przetwarzania danych,
- prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu.

***W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.***

**Zasady realizacji praw osób**

**Dostęp do danych**

- na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane, a także o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących;
- dostęp do danych może być zrealizowany przez wydanie kopii danych;

**Kopie danych**

- na żądanie, Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania kopii danych;
- administrator może naliczyć opłatę za wydania kopii, jeśli jest to proporcjonalne do poniesionych kosztów.

**Sprostowanie danych**

- administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby;
- administrator Danych Osobowych ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga;
- w przypadku sprostowania danych Administrator – na żądanie tej osoby – informuje o odbiorcach danych.

**Uzupełnienie danych**

- na żądanie osoby Administrator Danych Osobowych uzupełnia i aktualizuje dane;
- administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami ich przetwarzania. Administrator Danych Osobowych może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez jednostkę procedur i prawa bądź zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

**Usunięcie danych**

- Na żądanie osoby, Administrator Danych Osobowych usuwa dane, gdy:
    - dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;
    - osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
    - dane były przetwarzane niezgodnie z prawem;
    - konieczność usunięcia wynika z obowiązku prawnego;

- żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

- administrator Danych Osobowych określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikacji, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO;
- jeżeli dane podlegające usunięciu zostały upublicznione przez jednostkę, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich;
- w przypadku usunięcia danych, Administrator informuje osobę (na żądanie) o ich odbiorcach.

**Ograniczenie przetwarzania**

- administrator Danych Osobowych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
  - osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość; przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
  - administrator Danych Osobowych nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
  - osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
- w trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą,

chyba że w celu ustalenia, dochodzenia bądź obrony roszczeń, w celu ochrony praw innej osoby fizycznej lub prawnej, czy też z uwagi na ważne względy interesu publicznego;

- administrator informuje osobę przed uchyleniem ograniczenia przetwarzania;
- w przypadku ograniczenia przetwarzania danych Administrator informuje osobę (na jej żądanie) o ich odbiorcach.

**Przenoszenie danych**

- osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz przetwarzanie odbywa się w sposób zautomatyzowany;
- wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe;
- wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

**Odmowa udostępnienia danych**

- odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

# 18. REJESTR CZYNNOŚCI PRZETWARZANIA ORAZ REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

***Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania to dokumenty, pozwalające usystematyzować, zdefiniować oraz pogrupować czynności przetwarzania danych osobowych.***

**Obowiązek prowadzenia rejestrów czynności przetwarzania danych dotyczy podmiotów:**

- zatrudniających powyżej 250 osób;
- przetwarzających dane w sposób obarczony ryzykiem naruszenia praw lub wolności osób, których dane dotyczą;
- przetwarzających dane w sposób częstszy niż sporadyczny;
- przetwarzających informacje obejmujące szczególne kategorie danych osobowych;
- przetwarzających dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

**Co powinien zawierać rejestr czynności przetwarzania**

- dane administratora, współadministratorów, przedstawicieli administratorów oraz inspektora ochrony danych osobowych – ich imiona i nazwiska lub nazwy oraz dane kontaktowe;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą;
- wskazanie kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- jeśli ma to zastosowanie, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej oraz – w przypadkach szczególnych przekazań – dokumentację odpowiednich zabezpieczeń;
- planowane terminy usunięcia poszczególnych kategorii danych – jeśli administrator ma możliwość podania takiej informacji;

- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa związanych z bezpieczeństwem przetwarzania – jeśli administrator ma możliwość podania takiej informacji.

***Podmiot przetwarzający ma obowiązek prowadzenia rejestru kategorii czynności przetwarzania danych.***

**Co powinien zawierać rejestr kategorii czynności przetwarzania**

- dane administratora, współadministratorów, przedstawicieli administratorów oraz inspektora ochrony danych osobowych – ich imiona i nazwiska lub nazwy oraz dane kontaktowe;
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
- jeśli ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej oraz – w przypadkach szczególnych przekazań – dokumentację odpowiednich zabezpieczeń;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa związanych z bezpieczeństwem przetwarzania – jeśli administrator ma możliwość podania takiej informacji.

## 19. RETENCJA DANYCH OSOBOWYCH

***Art. 5 ust. 1 lit e RODO stanowi że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną***

***odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.***

**Zasady dotyczące retencji danych osobowych**

- RODO nakłada na Administratora Danych obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
- po osiągnięciu celu dane osobowe powinny zostać usunięte lub poddane anonimizacji. W tym celu, Administrator Danych jest zobowiązany do stałego nadzorowania zawartości administrowanych zbiorów danych oraz występujących w ich ramach procesów przetwarzania, pod kątem konieczności usuwania danych zbędnych, albo do których przetwarzania przestał być upoważniony;
- dane osobowe przechowywane są w formie umożlwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
- dane osobowe można przechowywać przez dłuższy czas, i ile będą one przetwarzane wyłącznie do celów: archiwalnych, w interesie publicznym, do celów badań naukowych, historycznych, celów statystycznych na mocy art. 89 ust 1 RODO, jeśli wdrożono odpowiednie środki techniczne, organizacyjne niezbędne do zapewnienia ochrony danych osobowym;
- w związku z powyższym, dla danych osobowych przetwarzanych przez ADO jako ich administratora w rozumieniu art. 4 pkt 7 RODO, ustala się terminy retencji;
- administrator zobowiązany jest do okresowego przeglądania dokumentacji z danymi osobowym, archiwizowania ich lub usuwania w zależności od postawy przetwarzania;
- podstawy do ustalenia terminów retencji jest przepis prawa, umowa, zgoda, uzasadniony interes administratora, obowiązek prawny;
- termin retencji dla danych osobowych przetwarzanych na podstawie umowy liczony jest od dnia zakończenia relacji tj. od rozwiązania, czy też wykonania umowy;
- termin retencji danych liczony jest od dnia wycofania tej zgody przez osobę która jej udzieliła. Co do zasady zgoda jest ważna do jej odwołania i RODO nie nakłada wprost obowiązku jej aktualizowania. Rekomendowane jest jednak „odświeżanie" zgód.

***Retencja danych osobowych dotyczy również danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności zawartych w korespondencjach e-mail. W związku z ciążącym na administratorze obowiązku usuwania bądź archiwizacji danych osobowych, również tych zawartych w skrzynkach e-mail powinno się usystematyzować tą czynności. Zasady retencji danych w poczcie elektronicznej dotyczą wszystkich dotyczy wszystkich użytkowników służbowych skrzynek e-mail oraz wszystkich rodzajów wiadomości, tzn. odebranych, wysłanych, roboczych, powiadomień, spamu, itp.***

**Retencja danych w poczcie e-mail**

W celu wprowadzenia skutecznej retencji wiadomości e-email każdy z użytkowników służbowych skrzynek pocztowych zobowiązany jest do:

- grupowania oraz oznaczania wiadomości, umożliwiającego określenie retencji poprzez nadanie odpowiedniej etykiety czy przenoszenia do właściwego folderu;
- regularnego przeglądu wątków wiadomości oraz usuwania tych dla których ustał czas przechowywania, zgodnie z ustalonymi okresami retencji;
- korzystania z automatycznego archiwizowania i automatycznego usuwania wiadomości w zgodnie z okresami retencji aby zautomatyzować i przyśpieszyć proces retencji danych;
- pobierania niezbędnych załączników na dysk, a jeżeli wiadomość nie jest już niezbędna do kontynuacji sprawy usuwanie jej;
- opróżniania kosza, w którym znajdują się niepotrzebne wiadomości regularnie, przynajmniej raz w miesiącu;
- w przypadku kiedy jest to zasadne stosujemy anonimizację.

**Kryteria ustalania okresów retencji**

W ustaleniu okresów przechowywania informacji zawartych w skrzynkach e-mail należy kierować się poniższymi kryteriami:

- jeżeli istnieją przepisy precyzyjnie definiujące okres przechowywania stosujemy je;
- jeżeli ww. przepisów nie ma to weryfikujemy, czy informacji zawartych w korespondencji potrzebujemy do wykazywania określonych faktów, związanych z roszczeniami prawnymi lub obroną przed takimi roszczeniami i przechowujemy je do czasu przedawnienia tych roszczeń;

- dane zawarte w korespondencjach e-mail weryfikujemy pod kątem przydatności przetwarzania i po ustaniu okresu tej przydatności usuwamy je lub archiwizujemy.

# 20. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH I AUDYTY SYSTEMU

***Polityka powinna być poddawana przeglądowi aktualizacji. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zarządzić przegląd Polityki stosownie do potrzeb.***

**Zasady audytu systemu**

- Do kontroli stanu ochrony danych osobowych w jednostce upoważnieni są:
  - ADO,
  - IOD,
  - osoby wyznaczone przez administratorów.
- ADO analizuje, czy Polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
  - zmian w budowie systemu informatycznego,
  - zmian organizacyjnych ADO, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
  - zmian w obowiązującym prawie.
- Co najmniej raz do roku kontroli podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe;
- IOD po uzgodnieniu z ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami prawa oraz przepisami o ochronie danych osobowych;
- Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z ADO, informatykiem. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez IOD, informatyka, a następnie przedstawiane w formie pisemnej do wiadomości ADO;

- ADO biorąc pod uwagę wnioski, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot;
- Za wyniki przeprowadzonych audytów odpowiedzialność ponosi ADO.

# 21. OCHRONA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

***System informatyczny służący do przetwarzania danych osobowych powinien być zabezpieczony przed nieuprawnionym dostępem z zewnątrz czy przepływem informacji pomiędzy systemem a siecią publiczną poprzez wdrożenie odpowiednich środków fizycznych, organizacyjnych oraz logicznych. Wszyscy użytkownicy systemu są zobligowani do nieustannego monitorowania komunikatów pochodzących z oprogramowania antywirusowego systemu i reagowania na nie.***

**Nadawanie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym**

- do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby upoważnione;
- informatyk jednostki lub osoba upoważniona na wniosek Administratora nadaje/modyfikuje/odbiera pracownikowi uprawnienia dostępu do systemu informatycznego;
- przyznanie uprawnień do obsługi systemu informatycznego polega na wprowadzeniu do systemu identyfikatora, hasła oraz określenia zakresu uprawnień dostępu do danych osobowych;
- uprawnienia w systemie informatycznym przyznawane użytkownikowi, wynikają z zakresu jego obowiązków i powinny być zgodne z upoważnieniem do przetwarzania danych osobowych. Użytkownikom należy przyznawać minimalne uprawnienia, niezbędne do realizacji zadań, wynikających z ich zakresu obowiązków;
- identyfikator użytkownika nie może być przydzielony innej osobie po zakończeniu pracy przez użytkownika;

- powyższe zasady obowiązują również osoby uzyskujące dostęp do danych osobowych na podstawie umowy zlecenia.

**Rejestrowania uprawnień do przetwarzania danych osobowych w systemie informatycznym**

- przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemach informatycznych polega na przypisaniu przez informatyka lub osobę upoważniona przez ADO w systemie dla upoważnionego użytkownika:
  - unikalnego identyfikatora i hasła lub unikalnego identyfikatora i przypisanej do niego karty mikroprocesorowej;
  - wprowadzeniu do systemu zakresu dostępnych dla danego użytkownika danych i dopuszczalnych operacji.
- każdy z użytkowników systemu posiada własny identyfikator;
- ustanowione hasło dostępu, w sposób poufny informatyk lub osoba upoważniona przekazuje użytkownikowi;
- hasło ustanowione podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym;
- użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
- użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła lub karty mikroprocesorowej;
- w przypadku anulowania uprawnień użytkownika jego identyfikator należy niezwłocznie zablokować w systemie oraz unieważnić hasło użytkownika.

**Metody i środki uwierzytelnienia związane z zarządzaniem i użytkowaniem systemu**

- bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła;
- zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.

- identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie;
- użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł;
- hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny;
- hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
- w sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany;
- przy wyborze hasła obowiązują następujące zasady:
  - minimalna długość hasła – 8 znaków,
  - właściwa złożoność hasła - litery duże i małe oraz cyfry lub znaki specjalne.
- zakazuje się stosowania haseł:
  - które użytkownik stosował uprzednio (do sześciu haseł wstecz),
  - będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
  - analogicznych jak identyfikator,
  - zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,
  - stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678 lub abcdefgh.
- w systemach umożliwiających zapamiętanie hasła nie należy korzystać z tego ułatwienia;
- powyższe reguły w zakresie haseł dotyczą obowiązków użytkownika systemu niezależnie od istnienia lub nie mechanizmów wymuszających (ułatwiających) ich stosowanie

***Czynności stanowiące zagrożenie dla systemu informatycznego mogące powodować nieprawidłowe działanie lub być przyczyną wycieku danych osobowych.***

**Zagrożenia systemu informatycznego**

Zabronione jest podejmowanie działań mogących stanowić zagrożenie dla systemu, w tym:

- łamanie haseł,
- dokonywanie włamań na konta innych użytkowników,

- nieprawne uzyskiwanie dostępu do kont administracyjnych,
- zakłócanie działania usług,
- omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),
- doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,
- praca na koncie innego użytkownika.

***W celu zmniejszenia prawdopodobieństwa wystąpienia skutków potencjalnych zagrożeń należy podczas pracy z systemem stosować się do zasad oraz obowiązujących procedur dla użytkowników systemu.***

**Procedura nr 4**

***Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu***

**§1 Cel procedury**

Celem procedury jest zdefiniowanie czynności, które należy wykonać w związku z podjęciem, zawieszeniem lub zakończeniem pracy w systemie informatycznym.

**§2 Zakres stosowania**

Procedura dotyczy wszystkich użytkowników systemu informatycznego oraz wszystkich fizycznych stanowisk umożliwiających przetwarzanie danych osobowych przy pomocy systemu.

**§3 Odpowiedzialność**

Użytkownik systemu teleinformatycznego może być kontrolowany oraz rozliczany z stosowania się do zaleceń procedury. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do ADO, informatykowi lub osobie upoważnionej w tym IOD.

**§4 Rozpoczęcie pracy**

Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła lub identyfikatora i przypisanej do niego karty mikroprocesorowej. Po zalogowaniu należy sprawdzić poprawność działania systemów antywirusowych.

**§4 Zawieszenie pracy**

Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub zablokowanie, wylogowanie sesji użytkownika, np. poprzez użycie kombinacji klawiszy na klawiaturze komputera:

- „Ctrl+Alt+Delete" i wybór polecenia „zablokuj ten komputer" lub „wyloguj",
- „logo systemu Windows+L" dla zablokowania komputera.

Udostępniając stanowisko komputerowe innemu upoważnionemu pracownikowi należy wykonać funkcję wylogowania z systemu.

**§4 Zakończenie pracy**

Przed wyłączeniem komputera należy bezwzględnie wylogować się z użytkowanych programów zakończyć ich pracę oraz wylogować się z systemu czy konta użytkownika.

**Kopie zapasowe**

**Poniżej przedstawione zostały ogólne zasady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania**

- w celu zagwarantowania bezpieczeństwa danych przechowywanych w systemie wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa;
- za systematyczne przygotowanie kopii zapasowych odpowiada użytkownik danego systemu, ASI, informatyk lub osoba upoważnia pełni nadzór nad tworzeniem kopii. W przypadku części aplikacji ich tworzenie odbywa się automatycznie;
- bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa;
- należy wykonywać następujące kopie bezpieczeństwa:
  - przed dokonaniem zmian w konfiguracji systemów lub oprogramowania;

- przed dokonaniem zmian w programach (np. zmiana wersji);
- zgodnie z przyjętym harmonogramem.

**Nośniki informacji**

**Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.**

- kopie zapasowe.
  - kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, tj. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
  - w przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. taśmach, płytach CD, DVD nośniki te należy sprawdzać pod kątem ich dalszej przydatności oraz odtwarzalności;
  - kopie zapasowe należy usunąć niezwłocznie po upływie okresów przechowywania lub w przypadku ustania ich użyteczności.
- elektroniczne nośniki informacji.
  - dopuszcza się używanie służbowych elektronicznych nośników informacji, zwanych dalej nośnikami, w celu przenoszenia i archiwizowania danych osobowych, w tym płyt DVD, dysków zewnętrznych oraz nośników przenośnych typu pendrive.
  - w przypadku konieczności zapisania na służbowych elektronicznych nośnikach informacji danych osobowych należy stosować wobec tych danych środki ochrony kryptograficznej.
  - zabronione jest używanie nośników do przenoszenia danych osobowych na prywatne komputery lub inne, prywatne urządzenia mogące służyć do przechowywania danych.
  - nośniki, zawierające dane osobowe, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny;
  - nośniki, zawierające dane osobowe, podlegają szczególnemu nadzorowi i są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w zamykanych szafach biurowych lub kasetkach;

- w przypadku zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika zawierającego dane osobowe poza obszar przetwarzania danych osobowych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą lub zniszczeniem;
- nośniki, zawierające dane osobowe, należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych np. w samochodach, przypiętych do pasków itp.);
- nośniki, zawierające dane osobowe, przeznaczone do:
  - likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
  - przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
  - naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.

**Zabezpieczenie systemu**

**Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej**

- oprogramowanie stosowane, wdrażane, modyfikowane, zakupione może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych oraz powinno spełniać wymagania przepisów z zakresu ochrony danych osobowych;
- dozwolone jest jedynie uruchamianie oprogramowania związanego merytorycznie z wykonywaną pracą oraz dopuszczonego przez Administratora do użytkowania w systemach;
- korzystanie z zasobów informatycznych poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w

szczególności firewall-i oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.

- w celu ochrony systemów przed szkodliwym oprogramowaniem oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym systemu. Za prawidłowość realizacji powyższego obowiązku odpowiada informatyk lub osoba upoważniona;
- sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń;
- użytkownicy zobowiązani są do niezwłocznego zgłaszania do informatyka lub osoby upoważnionej każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów). Informatyk lub osoba upoważniona podejmuje działania mające na celu eliminację nieprawidłowości w tym zakresie, jak również informuje o zaistniałym zdarzeniu Administratora i/lub IOD;
- programy antywirusowe winny być uaktywnione cały czas podczas pracy danego systemu;
- wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania szkodliwego oprogramowania najnowszą dostępną wersją programu antywirusowego;
- każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego;
- zabrania się używania elektronicznych nośników informacji niewiadomego pochodzenia;
- zabrania się pobierania z Internetu plików niewiadomego pochodzenia;
- w przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik winien zawiadomić ADO lub IOD, informatyka o zaistniałym zdarzeniu;

**Przeglądy i konsekracje**

**Zasady wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.**

- przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w jednostce dokonywane są przez osobę upoważnioną do tego typu czynności;

- dopuszcza się realizację czynności określonych w ust. 1 przez specjalistyczne firmy świadczące usługi w tym zakresie; w takim przypadku konieczne jest zawarcie stosownej umowy cywilnoprawnej;
- umowy w zakresie świadczenia usług teleinformatycznych wiążące się z przetwarzaniem danych osobowych powinny być traktowane jako powierzenie przetwarzania danych osobowych;
- pracownicy firm świadczących usługi, o których mowa w ust. 2 powyżej wykonują zlecone zadania tylko za zgodą Administratora, lub innego uprawnionego pracownika i pod jego nadzorem;
- w przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania;
- przeglądy i konserwacje wykonywane są cyklicznie oraz w przypadku pojawienia się usterki lub awarii systemów informatycznych;
- przeglądy mają na celu weryfikację elementów systemu informatycznego i poprawności ich funkcjonowania;
- konserwacje mają na celu utrzymanie systemu;
- szczegółowy harmonogram i zakres czynności wynikających z przeglądu i konserwacji dla każdego systemu ustala Administrator przy współpracy z informatykiem.

**Komputery przenośne**

**Zasady przetwarzanie danych osobowych na komputerach przenośnych.**

- za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy;
- użytkownicy komputerów przenośnych mogą z nich korzystać jedynie w siedzibie Administratora;
- użytkownicy komputerów przenośnych są odpowiedzialni za ich bezpieczeństwo oraz są oni zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych;
- komputery przenośne po zakończonej pracy winny być przechowywane przez użytkownika w miejscu wyznaczonym przez Administratora, w warunkach zapewniających ich bezpieczeństwo;

- komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.

**Urządzenia przenośne inne niż komputery**

**Zasady przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż komputery.**

- pracownicy korzystający z teleinformatycznych urządzeń przenośnych, tj. m.in. telefonów służbowych, tabletów, aparatów fotograficznych, kamer wideo, są zobowiązani chronić dane osobowe zawarte w pamięci tych urządzeń przed dostępem osób nieupoważnionych.
- wszelkie dane osobowe wprowadzone do pamięci urządzeń przenośnych powinny być usunięte po zakończeniu korzystania z urządzeń. Osobą właściwą do ich usunięcia jest pracownik korzystający z danego urządzenia.

**WYKAZ ZAŁĄCZNIKÓW**



**WYKAZ PROCEDUR**

**Załącznik nr 1**

***Karta szkolenia***

…… ……

*(nazwa i siedziba administratora danych)* *(miejscowość i data)*

| | |
|---|---|
| Imię i nazwisko osoby prowadzącej szkolenie | |
| Temat szkolenia | |

| Lista uczestników | |
|---|---|
| Imię i nazwisko | Podpis |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

…… ……

*(podpis szkolącego)* *(podpis pracodawcy)*

**Załącznik nr 2**

***Rejestr naruszeń bezpieczeństwa***

Miejsce i dzień i godzina naruszenia:

Dzień i godzina zgłoszenia naruszenia:

Numer naruszenia:

| | | |
|---|---|---|
| **Rodzaj naruszenia** | Naruszenie ochrony danych osobowych, które nie podlega zgłoszeniu organowi nadzorczemu (naruszenie ochrony danych osobowych nie spowodowało ryzyka naruszenia praw i wolności osób fizycznych) | |
| | Naruszenie, o którym trzeba zawiadomić zarówno organ nadzorczy, jak i osobę, której dane dotyczą (naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych) | |
| | Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu (jest mało prawdopodobne, aby naruszenie skutkowało wysokim ryzykiem naruszenia praw lub wolności osób fizycznych) | |
| | Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu (naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jednakże zawiadomienie osoby, której dane dotyczą, nie jest konieczne ze względu na wypełnienie przesłanek:<br>1.Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.<br>2.Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub | |

| | | |
|---|---|---|
| | wolności osoby, której dane dotyczą, wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku Administrator wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. | |
| **Kategoria i przybliżona liczba osób, których dane dotyczą** | | |
| **Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie** | | |
| **Skutki naruszenia ochrony danych osobowych** | | |
| **Podjęte działania zaradcze** | | |
| **Dzień zgłoszenia incydentu naruszenia ochrony danych osobowych organowi nadzorczemu (jeżeli dotyczy)** | | |
| **Dzień zawiadomienia osób, których dane dotyczą (jeżeli dotyczy)** | | |

**Załącznik nr 3**

***Zawiadomienie o naruszeniu bezpieczeństwa Państwa danych osobowych***

Miejsce i dzień i godzina naruszenia: ……..

Dzień i godzina zgłoszenia naruszenia:……

Numer naruszenia:……..

**Charakter naruszenia ochrony danych osobowych**

*Informujemy, że na skutek naruszenia osoba trzecia uzyskała dostęp do Pani/Pana danych osobowych przetwarzanych w systemach naszej jednostki.*

*Zakres danych które zostały naruszone:*

*a)……..*

*b)……..*

**Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji**

*Jeżeli mają Państwo jakiekolwiek pytania w związku z zaistniałą sytuacją, prosimy o kontakt pod wskazanym (adresem/telefonem/e-mailem) z Panem/Panią (imię i nazwisko)*

**Opis możliwych konsekwencji naruszenia ochrony danych osobowych;**

*Następstwem naruszenia Pana danych osobowych może być:*

*a)……..*

*b)……..*

**Opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.**

*W związku z zaistniałym naruszeniem ochrony danych osobowych dokonaliśmy:*

*a)……..*

*b)……..*

**Co może Pan/Pani zrobić?**

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy

*a)……..*

*b)……..*

**Załącznik nr 4**

…… ……

(nazwa i siedziba administratora danych) (miejscowość i data)

**UPOWAŻNIENIE nr…….**

**do przetwarzania danych osobowych**

1. Działając na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1) z dniem upoważniam Panią/Pana*)

……

*(imię i nazwisko pracownika)*

w związku z zatrudnieniem na stanowisku

……w……

*(nazwa stanowiska)* *(nazwa komórki organizacyjnej)*

do dostępu i przetwarzania danych osobowych zgodnie z zakresem obowiązków.

2. Upoważnienie do dostępu i przetwarzania danych osobowych zawartych w zbiorach/rejestrach danych obejmuje dostęp i przetwarzanie w następujących formach danych:
   - papierowej ❑ Tak ❑ Nie
   - elektronicznej ❑ Tak ❑ Nie
   -
3. W zbiorach danych prowadzonych w formie papierowej i w formie elektronicznej upoważnienie obejmuje następujące rodzaje przetwarzania:
   - Wgląd do danych ❑ Tak ❑ Nie
   - Wprowadzanie danych ❑ Tak ❑ Nie
   - Usuwanie danych ❑ Tak ❑ Nie
   - Aktualizacja danych ❑ Tak ❑ Nie

- Udostępnianie danych ❑ Tak ❑ Nie

4. Zobowiązuje Pana/Panią do przetwarzania danych osobowych zgodnie z niniejszym upoważnieniem, powszechnie obowiązującymi przepisami prawa oraz obowiązującymi u Pracodawcy wewnętrznymi procedurami.
5. Upoważnienie wygasa z chwilą ustania Pana/Pani*) zatrudnienia.
6. Osoba upoważniona do przetwarzania danych osobowych, zobowiązana jest do zachowania ich w tajemnicy, również po ustaniu zatrudnienia jak i do zachowania w tajemnicy informacji o ich zabezpieczeniu. Pracownik zobowiązuje się do zachowania tajemnicy zawodowej i nie rozpowszechniania bez zgody Pracodawcy, w jakiejkolwiek formie, wszystkich dostępnych mu informacji dotyczących Pracodawcy, do których będzie miał dostęp z tytułu wykonywania swoich obowiązków służbowych, a nie przeznaczonych przez Pracodawcę do publicznego rozpowszechniania, zarówno w czasie trwania umowy o pracę jak i po jej wygaśnięciu.
7. Upoważnienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla pracodawcy i pracownika.

…….. ……

*(data i podpis pracownika)* *(data, pieczęć i podpis pracodawcy)*

**Załącznik nr 5**

……

*(nazwa i siedziba administratora)*

***Ewidencja osób upoważnionych do przetwarzania danych osobowych***

| L.P. | Imię i nazwisko osoby upoważnionej | Data nadania upoważnienia | Data ustania upoważnienia | Zakres upoważnienia | Identyfikator Systemu Informatycznego |
|---|---|---|---|---|---|
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| 4. | | | | | |
| 5. | | | | | |
| 6. | | | | | |
| 7. | | | | | |
| 8. | | | | | |
| 9. | | | | | |
| 10. | | | | | |
| 11. | | | | | |
| 12. | | | | | |
| 13. | | | | | |
| 14. | | | | | |
| 15. | | | | | |
| 16. | | | | | |
| 17. | | | | | |
| 18. | | | | | |
| 19. | | | | | |

**Załącznik nr 6**

…… ……

*(nazwa i siedziba administratora danych)* *(miejscowość i data)*

**OŚWIADCZENIE O ZAPOZNANIU SIĘ Z POLITYKĄ BEZPIECZEŃSTWA**

Oświadczam, iż w dniu …….. zostałam/em* zapoznana/y* z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem 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 oraz z wprowadzoną i wdrożoną do stosowania przez Administratora Polityką Bezpieczeństwa Danych Osobowych.

Zobowiązuję się do:

- przestrzegania Polityki Bezpieczeństwa Danych Osobowych i innych procedur, instrukcji obowiązujących u Administratora odnoszących się do przetwarzania danych osobowych;

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą zastosowania kary porządkowej albo wypowiedzenie przez Pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy, bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j. Dz. U. z 2020 r. poz. 1320, z 2021 r. poz. 1162, z 2022 r. poz. 655.). Naruszenie zasad bezpieczeństwa danych osobowych może spowodować odpowiedzialność karną na zasadach określonych w Rozporządzeniu lub przepisach odrębnych**

…… ……

*(data i podpis pracownika)* *(data, pieczęć i podpis pracodawcy)*

**Załącznik nr 7**

…….. ……
*(nazwa i siedziba administratora danych)* *(miejscowość i data)*

## OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

**……**

w związku z zatrudnieniem na stanowisku

**……**

Oświadczam, iż:
zapoznano mnie z regulacjami wewnętrznymi z zakresu ochrony danych osobowych zgodnie z przepisami dotyczącymi ochrony danych osobowych – Rozporządzeniem 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).

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w fizycznym obszarze przetwarzania w związku z wykonywaniem zadań służbowych i obowiązków pracowniczych, zarówno w trakcie wiążącego mnie stosunku pracy jak i po jego ustaniu, których oraz do nierozpowszechniania jakichkolwiek danych do jakich będę miał/a dostęp w trakcie wykonywania czynności służbowych,
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu, IOD lub ADO,
- przestrzegania regulaminów, instrukcji i procedur obowiązujących u administratora, związanych z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał/a ww. danych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów prawa, co może wiązać się z nałożeniem odpowiednich sankcji pracowniczych.

Klauzulę poufności sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla pracodawcy i pracownika.

…… ……
*(data i podpis pracownika)* *(data, pieczęć i podpis pracodawcy)*

**Załącznik nr 8**

***Rejestr umów powierzenia przetwarzania danych***

| *Lp.* | *Data zawarcia umowy* | *Oznaczenie podmiotu z którym zawarta jest umowa powierzenia* | *Cel i zakres powierzenia wynikający z umowy* | *Okres na jaki została zawarta umowa lub termin jej wygaśnięcia* |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

…… …….. ……..

data aktualizacji podpis ADO podpis IOD

**Załącznik nr 9**

**UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

Zawarta w dniu ..... w ..... (zwana dalej umową) pomiędzy:

.....
reprezentowaną przez: .....,
zwaną dalej Administratorem, a

.....
reprezentowaną przez: .....,
zwanym dalej Podmiotem przetwarzającym

zwanymi łącznie w dalszej części umowy Stronami, a każda z osobna Stroną.

**Zważywszy, że**

1. Strony zawarły umowę nr..... z dnia ..... (zwana dalej umową podstawową), w związku z wykonaniem której Administrator powierzy Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą umową.
2. Celem umowy jest ustalenie warunków, na jakich Podmiot przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora.
3. Strony dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO) (Dz.Urz. UE L 119 z 4.05.2016 r., s. 1).
4. Administrator oświadcza, że jest uprawniony do przetwarzania danych, które powierza Podmiotowi przetwarzającemu w celu realizacji umowy podstawowej oraz że jest uprawniony do ich przetwarzania, w zakresie, w jakim powierzył je Podmiotowi przetwarzającemu.
5. Podmiot przetwarzający oświadcza, że dysponuje odpowiednimi środkami technicznymi i

organizacyjnymi, by przetwarzanie powierzonych danych osobowych było zgodne z aktualnymi przepisami o ochronie danych osobowych i chroniło prawa osób, których dane dotyczą.

6. Ankietę bezpieczeństwa danych osobowych w zakresie oceny podmiotu przetwarzającego zawiera załącznik A do umowy.

**Strony zgodnie postanowiły, co następuje.**

**§1**

**Definicje**

1. **Administrator danych osobowych** – podmiot, który powierza dane osbowe.
2. **Podmiot przetwarzający** – podmiot, któremu powierzono dane osobowe do przetwarzania.
3. **Podmiot podprzetwarzający** – podmiot, któremu podmiot przetwarzający powierzył dane.
4. **Osoba fizyczna -** rozumie się pracownika, inna osobę świadczącą usługi na podstawie umów cywilnoprawnych
5. **Dane osobowe** – 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,
6. **Dni Robocze** – dni od poniedziałku do piątku, poza dniami ustawowo wolnymi od pracy,
7. **Naruszenie** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
8. **Organ nadzorczy** – Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa**.**

9. **Podpowierzenie** – dalsze powierzenie przetwarzania Danych osobowych przez Podmiot przetwarzający,
10. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady 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).

**§ 2**

**Przedmiot umowy**

1. W związku z zawarciem umowy podstawowej Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wskazanych w § 2 umowy.
2. Podmiot przetwarzający będzie przetwarzał powierzone przez Administratora dane osobowe wyłącznie w celu realizacji umowy podstawowej, tj. ..... (*należy określić cel przetwarzania danych przez podmiot przetwarzający wynikający z umowy podstawowej*).
3. Podmiot przetwarzający jest uprawniony/ nie jest uprawniony do wykonywania, w sposób zautomatyzowany oraz niezautomatyzowany, operacji przetwarzania danych osobowych, takich 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.

**§ 3**

**Dane osobowe**

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie niniejszej umowy, następujące rodzaje danych osobowych

Dane zwykłe:

- imię,
- nazwisko,
- numer ewidencyjny PESEL,
- adres e-mail,

- inne jakie

2. Przetwarzanie danych będzie dotyczyć następujących kategorii osób:
   - klienci Administratora;

**§ 4**

**Obowiązki Podmiotu przetwarzającego**

1. Podmiot przetwarzający zobowiązuje się do przetwarzania danych wyłącznie w celu, dla którego zostały one powierzone.
2. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek przetwarzania danych osobowych wynika z przepisów prawa, w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający ma obowiązek niezwłocznie informować Administratora, jeżeli jego zdaniem polecenie Administratora jest niezgodne z prawem.
4. Podmiot przetwarzający zobowiązuje się nie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej ani nie korzysta z usług innych podmiotów przetwarzających, które przekazują dane osobowe do państwa trzeciego lub organizacji międzynarodowej.
5. Podmiot przetwarzający zobowiązuje się do wdrożenia odpowiednich środków technicznych i organizacyjnych zmierzających do zapewnienia bezpieczeństwa przetwarzania, tak aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.
6. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych każdej osobie fizycznej, która będzie przetwarzała powierzone dane osobowe, przy czym będą to jedynie osoby, które posiadają odpowiednie przeszkolenie z zakresu ochrony danych osobowych.
7. Podmiot przetwarzający zobowiązuje się zapewnić, aby każda osoba fizyczna, która ma dostęp do danych osobowych z upoważnienia Podmiotu przetwarzającego, zobowiązała się do zachowania ich w tajemnicy.

8. Podmiot przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych, w tym do prowadzenia rejestru kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Administratora, w przypadku obowiązku prowadzenia takiego rejestru.
9. Podmiot przetwarzający oświadcza, że wyznaczył Inspektora Ochrony Danych w osobie: .....
10. Podmiot przetwarzający zobowiązuje się do współpracy z Administratorem, przy uwzględnieniu charakteru przetwarzania, w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej prawa do uzyskania informacji, prawa dostępu do danych, prawa do sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych oraz prawa sprzeciwu, poprzez odpowiednie środki techniczne i organizacyjne. W razie wpływu takiego żądania Podmiot przetwarzający niezwłocznie przekazuje je Administratorowi pocztą elektroniczną na adres: ....., nie później jednak niż w terminie trzech dni od otrzymania żądania.
11. Podmiot przetwarzający zobowiązuje się do współpracy z Administratorem w zakresie realizacji obowiązków określonych w art. 32–36 RODO, tj. zabezpieczenia danych, zgłaszania naruszenia ochrony danych, zawiadamiania osób, których dane dotyczą, o naruszeniu, dokonywania oceny skutków dla ochrony danych oraz uprzednich konsultacji z organem nadzorczym w zakresie powierzonych danych.
12. Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później jednak niż w terminie 24 godzin, informować Administratora o wszelkich stwierdzonych naruszeniach danych osobowych pocztą elektroniczną na adres .....

**§ 5**

**Obowiązki Administratora**

1. Administrator zobowiązuje się współdziałać z Podmiotem przetwarzającym w wykonaniu umowy, w tym do udzielenia Podmiotowi przetwarzającemu wszelkich informacji, niezbędnych do wykonania umowy.
2. Administrator zobowiązuje się dokumentować w formie pisemnej wszystkie polecenia dotyczące przetwarzania danych osobowych dla Podmiotu przetwarzającego.

3. Administrator zobowiązuje się do przekazania informacji osobom, których dane dotyczą, o operacjach przetwarzania w momencie zebrania danych.

**§ 6**

**Odpowiedzialność Procesora i kary umowne**

1. Podmiot przetwarzający ponosi odpowiedzialność za wszelkie szkody majątkowe lub niemajątkowe poniesione przez osoby trzecie wskutek przetwarzania danych osobowych w sposób naruszający obowiązujące przepisy o ochronie danych osobowych lub Umowę.
2. Strony zgodnie postanawiają, że w przypadku naruszenia obowiązujących przepisów o ochronie danych osobowych w ramach realizacji Umowy z przyczyn leżących po stronie Podmiotu przetwarzającego w następstwie, którego jakakolwiek osoba trzecia, w tym osoba, której Dane osobowe dotyczą, wystąpiłaby przeciwko Administratorowi Danych z jakimikolwiek roszczeniami cywilnoprawnymi, opartymi na naruszeniu praw tej osoby, Podmiot przetwarzający zobowiązany jest do:
   1) zwolnienia Administratora Danych z obowiązku zapłaty jakichkolwiek odszkodowań lub zadośćuczynień z tytułu naruszenia praw osoby trzeciej;
   2) pokrycia kosztów poniesionych przez Administratora Danych w związku z podniesieniem przez osobę trzecią powyższych roszczeń, a w szczególności kosztów obsługi prawnej;
   3) zwolnienia z wszelkich innych roszczeń niż określone powyżej oraz pokrycia wszelkich kosztów poniesionych przez Administratora Danych w związku z podniesieniem tych roszczeń przeciwko niemu.
3. Podmiot przetwarzający jest zobowiązany do pokrycia wszelkich grzywien, kar administracyjnych i tym podobnych należności publicznych wynikających z naruszenia obowiązujących przepisów o ochronie danych osobowych w ramach realizacji Umowy z przyczyn leżących po stronie Podmiotu przetwarzającego terminie 14 (słownie: czternastu) dni od dnia wezwania Procesora przez Administratora Danych do zapłaty tych kwot.
4. Podmiot przetwarzający w przypadku podpowierzenia danych za podmiot podprzetwarzający odpowiada jak za swoje działania.
5. Administrator Danych jest uprawniony do dochodzenia odszkodowania przekraczającego wysokość zastrzeżonych w Umowie kar umownych na zasadach ogólnych.

## § 7
## Kontrola

1. Na wniosek Administratora, Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.

2. Administrator zastrzega sobie możliwość do przeprowadzenia kontroli wykonywania umowy, nie rzadziej niż co 12 miesięcy oraz zawsze w przypadku stwierdzenia naruszenia ochrony danych osobowych przez Podmiot przetwarzający. Podmiot przetwarzający zobowiązuje się do należytego współdziałania z Administratorem w czynnościach kontrolnych. W szczególności Podmiot przetwarzający zobowiązany jest do:

- udostępnienia Administratorowi dokumentacji przetwarzania danych osobowych;
- udostępnienia Administratorowi dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
- umożliwienia Administratorowi sporządzania kopii dokumentów dotyczących przetwarzania danych osobowych.

3. Kontrola będzie przeprowadzona po uprzednim zawiadomieniu Podmiotu przetwarzającego o terminie kontroli. Kontrola przeprowadzona będzie w godzinach pracy Podmiotu przetwarzającego.

4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli i wdrożenia zaleceń Administratora w terminie nie dłuższym niż 10 dni. Podmiot przetwarzający niezwłocznie przekaże Administratorowi informacje o podjętych działaniach.

5. Uprawnienia określone w § 5 pkt 1–2 umowy przysługują Administratorowi odpowiednio w stosunku do podmiotów, którym Podmiot przetwarzający powierzył dalsze przetwarzanie danych osobowych zgodnie z § 6 pkt 1 umowy.

6. Administrator zastrzega sobie prawo korzystania z usług osób trzecich celem przeprowadzenia kontroli (audytorów), jak również do przeprowadzenia takiej kontroli samodzielnie.

7. Podmiot przetwarzający przed podpisaniem umowy zobowiązuje się udzielić informacji dotyczących zabezpieczeń technicznych i organizacyjnych dotyczących powierzonych przez Administratora danych osobowych, celem weryfikacji rękojmi bezpiecznego i zgodnego z

prawem przetwarzania danych osobowych.

**§ 8**

**Podpowierzenie**

1. Podmiot przetwarzający może/ nie może powierzyć konkretne operacje na danych osobowych do dalszego przetwarzania w drodze pisemnej umowy zawartej z innym podmiotem przetwarzającym, wyłącznie po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający zobowiązuje się zapewnić, aby podmiot, któremu powierzono dalsze przetwarzanie danych osobowych zgodnie z § 6 pkt 1 umowy, spełniał co najmniej te same gwarancje i wymagania dotyczące ochrony danych osobowych, jakie zostały nałożone na Podmiot przetwarzający na mocy umowy. W szczególności wymóg ten dotyczy obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
3. Podmiot przetwarzający ma obowiązek niezwłocznie informować Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających. Administrator ma prawo wyrazić sprzeciw wobec zamierzonych przez podmiot przetwarzający zmian.
4. Podmiot przetwarzający nie może powierzyć innemu podmiotowi przetwarzającemu całości wykonania umowy.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków wynikających z umowy.

**§ 8**

**Wynagrodzenie**

Wynagrodzenie należne Podmiotowi przetwarzającemu na podstawie umowy podstawowej obejmuje wynagrodzenie należne z tytułu umowy.

**§ 9**

**Czas**

1. Umowa zostaje zawarta na czas obowiązywania umowy podstawowej określonej w § 1 ust. 2.
2. Z chwilą zakończenia obowiązywania umowy podstawowej Podmiot przetwarzający zobowiązuje się w zależności od żądania Administratora zwrócić lub usunąć powierzone dane Administratorowi oraz usunąć wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych.

**§ 10**

**Postanowienia końcowe**

1. Wszelkie zmiany i uzupełnienia postanowień niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie zastosowanie mają przepisy kodeksu cywilnego, RODO, a także przepisy innych ustaw regulujących ochronę danych osobowych.
3. Wszelkie spory mogące wyniknąć w związku z zawarciem lub wykonaniem umowy rozstrzygane będą przez sąd miejscowo właściwy dla siedziby Administratora.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Umowa wchodzi w życie z dniem podpisania.

..... .....

Administrator Podmiot przetwarzający

Załącznik do umowy powierzenia:

**Załącznik A**

**do umowy powierzenia przetwarzania danych osobowych**

**ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**

**do umowy powierzenia danych osobowych nr:…… z dnia:……**

*Poniższa ankieta ma na celu ustalenie czy podmiot zewnętrzny zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. W tym celu należy odpowiedzieć na poniższe pytania.*

| | |
|---|---|
| **Podmiot przetwarzający:** | |
| **Imię i Nazwisko osoby wypełniającej** | |
| **Stanowisko** | |
| **Adres e-mail i nr telefonu** | |

| L.p. | Pytanie | Odpowiedź | | Nie dotyczy | Uwagi/Wyjaśnienia |
|---|---|---|---|---|---|
| | | TAK | NIE | | |
| 1. | Czy Podmiot zewnętrzny ma wdrożony system zarządzania bezpieczeństwem informacji lub znak jakości i oznaczeń w zakresie ochrony danych osobowych, o których mowa w art. 42 RODO, i które obejmują całość operacji przetwarzania danych w ramach realizacji Umowy? | | | | |
| 2. | Czy Podmiot zewnętrzny wdrożył i stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO? | | | | |
| 3. | Czy system ochrony danych osobowych Podmiotu zewnętrznego był poddawany w ciągu ostatnich 3 lat sprawdzeniu przez audytorów zewnętrznych i uzyskał pozytywną opinię w tym zakresie (np.: posiada certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z normą ISO/IEC 27001 w pełnym zakresie)? | | | | |
| 4. | Czy Podmiot zewnętrzny posiada | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | doświadczenie w świadczeniu usług polegających na zarządzaniu zbiorami danych osobowych w imieniu innego podmiotu (pełnił rolę podmiotu przetwarzającego)? | | | | |
| 5. | Czy w trakcie świadczenia usług, doszło do naruszenia ochrony danych osobowych w zakresie powierzonych danych z winy podmiotu przetwarzającego? | | | | |
| 6. | Czy Podmiot zewnętrzny wyznaczył w strukturach wewnętrznych Inspektora Ochrony Danych lub osobę/komórkę odpowiedzialną za nadzór nad ochroną danych osobowych? | | | | |
| 7. | Czy Podmiot zewnętrzny opracował i wdrożył metodykę oraz procedury zarządzania ryzykiem związanym z bezpieczeństwem informacji? | | | | |
| 8. | Czy Podmiot zewnętrzny prowadzi rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO? | | | | |
| 9. | Czy Podmiot zewnętrzny prowadzi rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO? | | | | |
| 10. | Czy Podmiot zewnętrzny przeprowadza regularne (co najmniej raz w roku) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? | | | | |
| 11. | Czy Podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, określonych w art. 15-22 RODO? | | | | |
| 12. | Czy Podmiot zewnętrzny zapewnia, aby każdy nowozatrudniony pracownik przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami o ochronie danych osobowych, w tym wewnętrznymi? | | | | |
| 13. | Czy podmiot przetwarzający prowadzi cykliczne szkolenia doskonalące dla swojego personelu lub podejmuje inne działania mające na celu podnoszenie świadomości pracowników i uaktualnianie wiedzy z zakresu ochrony danych osobowych? | | | | |
| 14. | Czy osoby wykonujące operacje na danych osobowych otrzymały stosowne upoważnienia do przetwarzania danych, spełniające wymogi przepisu art. 29 RODO? | | | | |
| 15. | Czy Podmiot zewnętrzny wdrożył i stosuje w | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | swojej organizacji sformalizowane procedury nadawania uprawnień do systemów informatycznych przetwarzających dane osobowe? | | | | |
| 16. | Czy Podmiot zewnętrzny prowadzi cykliczne przeglądy nadanych uprawnień? | | | | |
| 17. | Czy Podmiot zewnętrzny stosuje środki kontroli dostępu fizycznego do budynku/budynków ograniczające dostęp tylko dla autoryzowanego personelu? | | | | |
| 18. | Czy Podmiot przetwarzający posiada odpowiednio wyposażone i zabezpieczone pomieszczenia umożliwiające bezpieczne przetwarzanie danych osobowych? | | | | |
| 19. | Czy każdy pracownik otrzymuje unikalny identyfikator do systemów informatycznych? | | | | |
| 20. | Czy w systemach informatycznych Podmiotu zewnętrznego zapewniono wymuszanie na użytkownikach stosowania haseł o odpowiedniej sile (kombinacja liter, cyfr i znaków specjalnych, min. 8 znakowe), także ich okresowej zmiany oraz zmian w razie zaistniałej potrzeby? | | | | |
| 21. | Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego ekranu" polegającą na automatycznym wygaszaniu ekranu i blokowaniu systemu, po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła? | | | | |
| 22. | Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego biurka" polegającą na obowiązku chowania dokumentów zawierających dane osobowe do zamykanych szaf na koniec dnia pracy? | | | | |
| 23. | Czy w systemach informatycznych Podmiotu zewnętrznego są wdrożone zabezpieczenia wykrywające lub zapobiegające użyciu nieautoryzowanego oprogramowania? | | | | |
| 24. | Czy urządzenia mobilne (laptopy, tablety, telefony komórkowe, itp.) wykorzystywane do przetwarzania danych osobowych, którymi Podmiot zewnętrzny dysponuje, są szyfrowane? | | | | |
| 25. | Czy Podmiot zewnętrzny posiada wdrożone procedury bezpiecznego zbywania sprzętu, uwzględniające całkowite usuwanie danych z nośników informacji? | | | | |
| 26. | Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | incydentami związanymi z bezpieczeństwem informacji? | | | | |
| 27. | Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania ciągłością działania? | | | | |
| 28. | Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe. | | | | |
| 29. | Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych? | | | | |
| 30. | Jeśli tak to w jakim kraju? | | | | |
| 31. | Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych? | | | | |
| 32. | Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO? | | | | |
| 33. | Czy Podmiot zewnętrzny wyraża zgodę na ewentualną weryfikację w siedzibie Podmiotu zewnętrznego, opisanych powyżej zasad ochrony danych osobowych? | | | | |

.....

(data i podpis osoby wypełniającej)

**Załącznik nr 10**

***Wniosek o realizację praw***

| | |
|---|---|
| Białe pola wypełnia wnioskodawca<br>DRUKOWANYMI literami.<br>Szare pola wypełnia Administrator danych. | .....<br>miejscowość i data |
| .....<br>Oznaczenie Administratora Danych<br>[pieczęć] | .....<br>numer kolejny wniosku |
| ***WNIOSEK O REALIZACJĘ**** | |
| ☐ prawa dostępu do danych<br>☐ prawa do sprostowania danych<br>☐ prawa do usunięcia danych ("prawo do bycia zapomnianym")<br>☐ prawa do ograniczenia przetwarzania | ☐ prawa do przeniesienia danych do innego administratora<br>☐ prawa do sprzeciwu<br>☐ prawa do niepodlegania profilowaniu |
| **podstawa prawna** | 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) |
| **1. Dane osoby wnioskującej** | |
| imię/imiona:<br>Nazwisko:<br>Adres zamieszkania:<br>inne dane pozwalające na identyfikację np. nr | .....<br>.....<br>.....<br>.....<br>.... |

* właściwe zaznaczyć

| | |
|---|---|
| dowodu osobistego/PESEL: | ……. . …… …… .. |
| **2. Informacje identyfikujące osobę wnioskującą w zasobach Administratora Danych Osobowych** | |
| …… …… …… | |
| **3. Sposób odbioru danych osobowych przez osobę wnioskującą*** | |
| ☐ wiadomość e-mail<br>☐ doręczenie pocztą**<br>☐ odbiór osobisty | ……<br>……<br>…… |
| **4. Uzasadnienie/uwagi osoby wnioskującej*** ** | |
| …… …… …… …… …… …… …… …… | |
| ……<br>*podpis wnioskodawcy* | |
| **5. Informacje dotyczące wykonania/niewykonania prawa osoby której dane dotyczą:** | |

* * uzupełnić wykropkowane pole w przypadku, gdy adres korespondencyjny jest inny niż adres zamieszkania

| | |
|---|---|
| ☐ Administrator przychyla się do wniosku | ☐ Administrator odrzuca wniosek |
| | |

**Uzasadnienie decyzji administratora**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

| |
|---|
| ……<br>data i podpis ADO |
| zatwierdzenie Inspektora Ochron Danych: |
| ……<br>data i podpis IOD |

**Załącznik nr 11**

## Rejestr udostępnień danych osobowych

| L.P. | Data udostępnienia | Imię i nazwisko, stanowisko służbowe pracownika udostępniającego dane | Zakres udostępnionych danych | Nazwa podmiotu, któremu udostępniono dane | Podstawa udostępnienia danych | Uwagi |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |