POLITYKA OCHRONY DANYCH OSOBOWYCH
W MUZEUM RYBOŁÓWSTWA MORSKIEGO W NIECHORZU

DOKUMENTACJA PODO STANOWI WŁASNOŚĆ I TAJEMNICĘ JEDNOSTKI I NIE PODLEGA PUBLIKACJI I ROZPOWSZECHNIANIU.
TREŚĆ ZAPISÓW PODO, JEST DOSTĘPNA KAŻDEJ OSOBIE PRZETWARZAJĄCEJ DANE OSOBOWE, W UPRAWNIONYM ZAKRESIE, BEZ MOŻLIWOŚCI PRZEKAZYWANIA INFORMACJI OSOBOM NIEUPRAWNIONYM

Imię i nazwisko zatwierdzającego	Data zatwierdzenia	Podpis
Dominika Winiarska-Chodziutko– Administrator	08.08.2024	DYREKTOR Muzeum Rybołówstwa Morskiego w Niechorzu *Dominika Winiarska-Chodziutko*

Opracowali:
Dawid Czerw - Inspektor Ochrony Danych
Dominika Winiarska-Chodziutko– Administrator

Wersja 1.0

Spis treści

REJESTR ZMIAN DOKUMENTU

L.p.	Data aktualizacji	Zakres aktualizacji (rozdział, §, strona)	Podpis osoby (osób) dokonujących aktualizacji

I. SŁOWNICZEK I WYKAZ SKRÓTÓW

1. SŁOWNICZEK

ADO; Administrator;	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28
Aplikacja	Oprogramowanie posiadające funkcje umożliwiające wykonywanie konkretnych zadań merytorycznych wiążących się z przetwarzaniem danych przez użytkowników
Dane osobowe	Wszelkie 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
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu
Poufność danych	Właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom
Integralność	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób
Hasło	Ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi
Identyfikator	Ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną (użytkownika) do przetwarzania danych osobowych w systemie informatycznym
Incydent	Pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji
Inspektor ochrony danych (IOD)	Osoba wyznaczona przez ADO m.in. do monitorowania przestrzegania zasad ochrony danych osobowych oraz do informowania ADO, podmiotu przetwarzającego oraz pracowników o obowiązkach spoczywających na nich na mocy RODO
Naruszenie ochrony danych osobowych	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
Komputer	Komputer stacjonarny, laptop
Nośnik danych	Wszelkie zewnętrzne nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski zewnętrzne SDD i HDD, karty pamięci, pendrive'y, optyczne nośniki danych i inne zewnętrzne nośniki danych
Urządzenie mobilne	Przenośne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymania przewodowego połączenia z siecią np. tablety, smartfony, laptopy, telefony komórkowe
Organ nadzorczy	Urząd Ochrony Danych Osobowych
Przetwarzanie danych osobowych	Operacja 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

Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO
Polityka/PODO	Niniejszy dokument
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 tych danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych osobowych)
System informatyczny	Zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe
Użytkownik	Osoba upoważniona do dostępu do zasobów systemu informatycznego posiadająca upoważnienie do przetwarzania danych osobowych w tym systemie
Usuwanie danych	Zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
Ustawa ODO	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. Z 2019 r. Poz. 1781)
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji
Zakres zbierania danych osobowych	Kategorie danych osobowych, które podlegają przetwarzaniu przez ADO, np. imię, nazwisko, adres
Zbiór danych osobowych	Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
Zgoda	Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych
Adekwatność Lub Minimalizacja danych	Zasada dotycząca przetwarzania danych osobowych polegająca na tym, że ADO danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu, dla którego dane są zbierane
Analiza ryzyka	Proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń
Anonimizacja	Przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań
Audyt zgodności	Czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami RODO oraz innymi przepisami o ochronie danych osobowych, a także czynności mające na celu monitorowanie przestrzegania polityki ochrony danych osobowych
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;
Docelowy Poziom ryzyka	Docelowy poziom pojedynczego ryzyka, jaki ADO zamierza osiągnąć w odniesieniu do konkretnego ryzyka
Działania zaradcze	Środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia
Legalność	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO
Odbiorca	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym

	odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii europejskiej lub prawem państw członkowskiego
Osoba upoważniona	Osoba upoważniona przez ADO do przetwarzania danych osobowych, nad którą ADO sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę
Pracownik Lub Współpracownik	Osoba zatrudniona na podstawie umowy o pracę oraz osoba świadcząca usługi na podstawie umów cywilnoprawnych/kontraktów, a także praktykanci, wolontariusze, stażyści i studenci
Pseudonimizacja	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
Rejestr czynności przetwarzania Danych osobowych	Dokument, o którym mowa w art. 30 ust. 1 RODO
Rejestr wszystkich kategorii czynności przetwarzania	Dokument, o którym mowa w art. 30 ust. 2 RODO
Upoważnienie	Oświadczenie nadane przez ADO wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą ADO sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę
Uwierzytelnianie	Działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej
Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną

2. STOSOWANE SKRÓTY

UODO	Urząd Ochrony Danych Osobowych
PUODO	Prezes Urzędu Ochrony Danych Osobowych
ADO	Administrator
IOD	Inspektor Ochrony Danych

II. DEFINICJE, CELE I ZAKRES ZASTOSOWANIA POLITYKI

Polityka Ochrony Danych Osobowych jest dokumentem określającym zbiór zasad oraz całokształt działań podejmowanych przez ADO w celu uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, na każdym etapie ich przetwarzania.

Tworzy się niniejszą Politykę ochrony danych osobowych celem realizacji obowiązków wynikających z powszechnie obowiązującego prawa, w szczególności **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.**

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Aby móc to wykazać ADO wdraża niniejszą Politykę.

Aby przetwarzanie odbywało się w sposób zapewniający należytą ochronę danych osobowych będących w zasobach ADO, przetwarzanie odbywa się z zachowaniem zasad określonych w art. 5 ust. 1 RODO, tj.:

- zgodności z prawem;
- rzetelności, przejrzystości i ograniczenia celu;
- adekwatności, prawidłowości i okresowości przetwarzanych danych;
- poufności, integralności i rozliczalności danych;

Polityka jest aktualizowana w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych lub w związku ze zmianami stanu faktycznego, które wpływają na treść dokumentu.

Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników i współpracowników mających dostęp do danych osobowych.

Zakres przedmiotowy stosowania niniejszej Polityki obejmuje przetwarzanie danych osobowych w formie papierowej oraz elektronicznej.

Żadna regulacja wewnętrzna obowiązująca u ADO nie może naruszać zasad określonych w niniejszej Polityce.

ADO w trybie art. 37 ust. 1 lit. b) RODO wyznaczył Inspektora Ochrony Danych, który wykonując zadania zgodnie z art. 39 RODO, podlega bezpośrednio najwyższemu kierownictwu.

Dane osobowe chronione niniejszą Polityką przetwarzane są w siedzibie ADO oraz w zasobach podmiotów przetwarzających.

III. OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

1. Zasady ogólne

Organizacja procesów przetwarzania danych osobowych u ADO opiera się na wyodrębnieniu następujących kategorii osób:

- ADO,
- IOD – Inspektor Ochrony Danych,
- Użytkownicy (osoby upoważnione do przetwarzania danych osobowych przez ADO np. pracownicy etatowi bądź osoby współpracujące w oparciu o umowy o współpracy itp.),
- personelu pomocniczego.

2. Nadawanie upoważnień do przetwarzania danych osobowych, zobligowanie do zachowania poufności oraz szkolenie wstępne

1. Obowiązki przed przystąpieniem do pracy z danymi osobowymi

   Pracownicy, których zakres obowiązków obejmuje dostęp do danych osobowych, lecz zakres realizowanych czynności nie wymaga ich przetwarzania, muszą przed przystąpieniem do pracy spełnić następujące wymagania:

   - **Zapoznanie się z zasadami ochrony danych osobowych:**
     - Każdy pracownik jest zobowiązany do zapoznania się z obowiązującymi zasadami ochrony danych osobowych określonymi w Polityce Ochrony Danych Osobowych.
     - Pracownik musi podpisać stosowne oświadczenie potwierdzające zapoznanie się z ww. zasadami (Załącznik Nr 1 do Polityki).
   - **Podpisanie oświadczenia o zachowaniu poufności:**
     - Pracownik musi podpisać oświadczenie o zachowaniu poufności danych osobowych i sposobów ich zabezpieczenia (Załącznik Nr 2 do Polityki).
   - **Zapoznanie się z materiałem szkoleniowym:**
     - Pracownik musi zapoznać się z materiałem szkoleniowym z zakresu ochrony danych osobowych (Załącznik Nr 3 do Polityki).

2. Upoważnienie do przetwarzania danych osobowych

   - Wszystkie osoby, których rodzaj wykonywanej pracy wiąże się z przetwarzaniem danych osobowych, otrzymują formalne upoważnienie do przetwarzania danych osobowych (Załącznik Nr 4 do Polityki).

3. Odpowiedzialność za wydanie i przechowywanie dokumentów

   - **Główny Księgowy**
     - Jest odpowiedzialny za wydanie Załączników Nr 1, 2 każdej osobie, której rodzaj wykonywanej pracy wiąże się z dostępem do danych osobowych, lecz zakres realizowanych czynności nie wymaga ich przetwarzania.
     - Jest odpowiedzialny za wydanie Załączników Nr 1, 2 i 4 każdej osobie, której rodzaj wykonywanej pracy wiąże się z przetwarzaniem do danych osobowych.
     - Jest odpowiedzialny za przechowywanie podpisanych oświadczeń oraz upoważnień.
     - Jest odpowiedzialny za wydanie Pracownikowi do zapoznania się materiał szkoleniowy (Załącznik Nr 3).

3. Obowiązki ADO:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, ADO wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać;
2. Poddawanie przeglądom i uaktualnianie środków technicznych i organizacyjnych;

3. Wdrożenie niezbędnych środków organizacyjnych i technicznych zapewniających rozliczalność, integralność oraz poufność przetwarzanych danych osobowych;
4. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych (Polityka oraz dokumenty z nią związane);
5. Wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności;
6. Spełnienie względem osób, których dane są przetwarzane, obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 oraz 14 ust. 1 i 2 RODO. Procedura realizacji obowiązków informacyjnych stanowi treść **Załącznika Nr 5** do Polityki;
7. Respektowanie praw osób, których dane są przetwarzane, np. Do udzielania informacji co do celów, sposobów, źródeł, zakresu przetwarzania danych osobowych, spełniania żądań sprostowania, uaktualnienia albo uzupełnienia czy też czasowego wstrzymania ich przetwarzania. Zasady realizacji praw osób, których dane są przetwarzane określone są w **Załączniku nr 6** do Polityki;
8. Zarządzanie upoważnieniami do przetwarzania danych;
9. Prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych w postaci elektronicznej lub papierowej;
10. W przypadku zlecenia przetwarzania danych w imieniu ADO podmiotowi zewnętrznemu zgodnie z art. 28 ust. 3 RODO zawarcie stosownej umowy;
11. Wyznaczenie Inspektora Ochrony Danych w trybie art. 37 ust. 1 RODO;
12. Powiadomienie o wyznaczeniu IOD organ nadzorczy, czyli Prezesa Urzędu Ochrony Danych Osobowych (UODO) zgodnie z art. 10 ustawy ODO;
13. Opublikowanie na stronie internetowej danych IOD zgodnie z art. 11 ustawy ODO;
14. Zapewnienie, by w zgodzie z art. 38 ust. 1 RODO, IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
15. Wspieranie IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;
16. Zapewnienie, by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań;
17. Prowadzenie rejestru czynności przetwarzania zgodnie z wymaganiami zawartymi w art. 30 ust. 1 RODO oraz, jeżeli występuje jako podmiot przetwarzający, rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO;
18. Prowadzenie rejestru umów przetwarzania danych osobowych w imieniu ADO, którego wzór stanowi **Załącznik Nr 9** do Polityki.;
19. Zgłoszenie do UODO naruszenia ochrony danych osobowych - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
20. Postępowanie z kluczami do drzwi wejściowych oraz pomieszczeń w zgodzie z Instrukcją postępowania z kluczami, stanowiącą **Załącznik nr 11** do Polityki;
21. Zarządzanie całym systemem informatycznym i podejmowanie działań mających na celu zapewnienie prawidłowego funkcjonowania całego systemu informatycznego, w tym

nadzorowanie prawidłowego funkcjonowania sprzętu, oprogramowania i jego konserwację, koordynowanie techniczno-organizacyjnej obsługi systemów informatycznych, w szczególności służących do przetwarzania danych osobowych. W tym w szczególności:

1) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe oraz nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
2) identyfikowanie i analizowanie zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemie informatycznym,
3) określanie potrzeb w zakresie zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe,
4) zapewnienie instalacji oraz konfiguracji wykorzystywanego oprogramowania,
5) sprawowanie nadzoru nad bezpieczeństwem, zachowaniem poufności, integralności oraz dostępności danych osobowych zawartych w komputerach, urządzeniach mobilnych i nośnikach danych, w których przetwarzane są dane osobowe,
6) monitorowanie działań zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
7) zarządzanie serwerem strony i kont pocztowych,
8) dbanie o niezakłócone działanie kluczowych aplikacji służących do przetwarzania danych,
9) sprawdzanie sposobów zabezpieczenia danych osobowych w systemie informatycznym, a w szczególności sprawdzanie:
   a) metod kontroli dostępu do danych przetwarzanych w systemie informatycznym,
   b) zastosowanych środków ochrony danych osobowych przed utratą na skutek awarii systemu informatycznego, w tym zasilania w energię elektryczną,
   c) zastosowanych zabezpieczeń przed zagrożeniami pochodzącymi z sieci publicznej,
   d) zapewnienie rozliczalności wykonywanych operacji w zakresie systemu informatycznego,
10) zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
11) sporządzenie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych,
12) zarządzanie licencjami programów komputerowych i prowadzenie dokumentacji sprzętu.
13) przydzielanie, cofanie i aktualizowanie uprawnień dostępu do danych.

ADO w zakresie zarządzania całym systemem informatycznym I podejmowania działań mających na celu zapewnienie prawidłowego funkcjonowania całego systemu informatycznego, w tym nadzorowania prawidłowego funkcjonowania sprzętu, oprogramowania i jego konserwację, koordynowania techniczno-organizacyjnej obsługi systemów informatycznych, w szczególności służących do przetwarzania danych osobowych, z uwagi na wiedzę specjalistyczną potrzebną do realizacji części z nich, może zlecić wykonanie poszczególnych usług zewnętrznym usługodawcom.

4. Obowiązki Inspektora Ochrony Danych:

1. Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. Monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz Polityk i procedur obowiązujących u ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,

działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4. Współpraca z UODO;
5. Pełnienie funkcji punktu kontaktowego dla UODO w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
6. Dbanie o aktualność Polityki, a także nadzorowanie przestrzegania określonych w niej zasad;
7. Doradztwo w zakresie opracowywania dodatkowych procedur ochrony danych osobowych, jeśli pojawi się taka konieczność;
8. Doradztwo w zakresie opracowywania wzorów dokumentów dotyczących ochrony danych osobowych;
9. Opiniowanie umów, których przedmiotem – bezpośrednio lub pośrednio – jest przetwarzanie danych osobowych;
10. Analiza sytuacji oraz przyczyn, które doprowadziły do naruszenia zasad bezpieczeństwa, a także zabezpieczania wykrytych dowodów i śladów naruszenia bezpieczeństwa danych osobowych przetwarzanych w sposób tradycyjny (kartoteki papierowe) jak i elektronicznie;

5. Obowiązki użytkowników:

1. Przetwarzanie danych osobowych wyłącznie w zakresie nadanych upoważnień zgodnie z decyzją ADO;
2. Przestrzeganie zasad ochrony danych osobowych określonych w Polityce. Każdy użytkownik zobowiązany jest zapoznać się przed dopuszczeniem do przetwarzania danych z Polityką oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści (**Załącznik Nr 1** do Polityki);
3. Odbycie szkolenia wstępnego w zakresie ochrony danych osobowych poprzez zapoznanie się z materiałem szkoleniowym (**Załącznik Nr 3** do Polityki);
4. Zapoznanie się z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych;
5. Przetwarzanie danych osobowych zgodnie z celami przetwarzania;
6. Zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą;
7. Informowanie ADO lub IOD o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych;
8. Zapewnienie poufności danych osobowych, do których uzyskują dostęp w ramach realizacji czynności służbowych;
9. Dbanie o bezpieczną eksploatację systemu informatycznego. W przypadku wykrycia zagrożenia użytkownik ma obowiązek poinformować o tym fakcie ADO lub IOD;
10. Dbanie o bezpieczeństwo użytkowanego komputera - w tym celu użytkownik ma obowiązek ustawienia „silnego" hasła dostępowego (zawierającego duże i małe litery, cyfry i znaki specjalne) do systemu operacyjnego oraz aplikacji służących do przetwarzania danych osobowych. W przypadku wystąpienia podejrzenia, że hasło mogło zostać poznane przez osobę nieupoważnioną użytkownik ma obowiązek zmiany hasła. Hasła nie mogą być zapisywane i pozostawiane w łatwo dostępnych miejscach;
11. Wykazywanie ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila;
12. Szyfrowanie danych osobowych wysyłanych drogą mailową zgodnie z Instrukcją szyfrowania pliku/katalogu programem 7-zip, która stanowi **Załącznik Nr 15** do Polityki, a także przekazywanie hasła odbiorcy alternatywną drogą komunikacji;
13. Dbanie o to, by dokumenty były przechowywane w zamkniętych szafach lub szufladach. Dostęp do kluczy mogą mieć tylko osoby uprawnione do przetwarzania danych;

14. Zgłaszanie do IOD naruszeń ochrony danych osobowych zgodnie z Procedurą stanowiącą **Załącznik Nr 10** do Polityki;
15. Przetwarzanie danych osobowych, do których przetwarzania użytkownicy zostali upoważnieni przez ADO **wyłącznie przy użyciu służbowego sprzętu komputerowego.**

IV. ZASADA CZYSTEGO BIURKA ORAZ CZYSTEGO EKRANU

1. Zasada czystego biurka:

Należy unikać pozostawiania dokumentów zawierających dane osobowe lub informacje istotne z perspektywy bezpieczeństwa danych osobowych i informacji na biurku bez właściwego nadzoru. Po zakończeniu pracy należy zabezpieczyć dokumenty i nośniki zawierających informacje chronione w zamykanych meblach biurowych.

2. Zasada czystego ekranu:

Każdorazowo podczas opuszczania stanowiska komputerowego, należy zablokować dostęp do tego stanowiska poprzez zastosowanie wygaszacza ekranu zabezpieczonego hasłem lub wylogowanie się z systemu. Zaleca się ustawianie ekranów monitorów komputerowych w taki sposób, aby niemożliwy był podgląd lub odczyt jakichkolwiek danych przez osobę postronną. Po zakończeniu pracy należy wyłączyć wszystkie urządzenia wchodzące w skład zestawu komputerowego.

V. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

1. Zasady ogólne.

Użytkownik w czasie pracy powinien podejmować wszelkie niezbędne czynności zapewniające bezpieczeństwo przetwarzania danych osobowych, a w szczególności:

- w miarę możliwości lokalowych ustawić ekran monitora tak, by uniemożliwić wgląd w przetwarzane dane osobom nieuprawnionym,
- dopilnować by w pomieszczeniach, w których przetwarzane są dane osobowe, osoby trzecie przebywały tylko w obecności osób upoważnionych.

2. Procedura rozpoczęcia pracy w systemie informatycznym.

1) Uruchomić komputer i zalogować się podając swój identyfikator i hasło dostępu do systemu operacyjnego.
   a) hasło dostępu do systemu operacyjnego składa się co najmniej z 8 znaków i zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
   b) hasła nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów itp.,
   c) hasła podlegają okresowej zmianie, dokonywanej nie rzadziej niż raz na rok,
   d) hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitora w formie jawnej,
   e) hasło nie może być ujawnione nawet po utracie przez nie ważności,
   f) zakazuje się przechowywać zapisane hasła w łatwo dostępnych miejscach (np. na monitorach komputerów, pod klawiaturami),
   g) w przypadku podejrzenia, że hasło poznała osoba nieupoważniona do przetwarzania danych osobowych, użytkownik ma obowiązek niezwłocznie zgłosić ten fakt do ADO.

ADO po otrzymaniu takiej informacji niezwłocznie podejmuje kroki zmierzające do zmiany hasła.

2) Uruchomić wymagane do pracy aplikacje (wykorzystywane w ramach bieżącej działalności ADO) i zalogować się podając swój identyfikator i hasło dostępu.

Założenia ogólne w zakresie użytkowania aplikacji:

a) hasło dostępu do aplikacji powinno składać się co najmniej z 8 znaków i zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
b) hasła nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów itp.,
c) hasła podlegają okresowej zmianie, w zależności od możliwości konfiguracji danej aplikacji, nie rzadziej niż raz na rok,
d) należy unikać stosowania tego samego hasła do ochrony różnych zasobów np. to samo hasło do systemu operacyjnego i poszczególnych aplikacji,
e) hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitora w formie jawnej,
f) hasło nie może być ujawnione nawet po utracie przez nie ważności,
g) zakazuje się przechowywać zapisane hasła w łatwo dostępnych miejscach (np. na monitorach komputerów, pod klawiaturami),
h) w przypadku podejrzenia, że hasło poznała osoba nieupoważniona do przetwarzania danych osobowych, użytkownik ma obowiązek niezwłocznie zgłosić ten fakt do ADO. ADO po otrzymaniu takiej informacji niezwłocznie podejmuje kroki zmierzające do zmiany hasła.

3. Ochrona haseł

1. Hasła użytkowników lub inne dane uwierzytelniające do systemu operacyjnego lub aplikacji podlegają szczególnej ochronie.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego ochronę.
3. Hasło użytkownika związane jest z jego identyfikatorem.
4. Każdy użytkownik posiadający dostęp do systemu informatycznego zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie informatycznym,
   2) nieujawniania hasła nawet po utracie przez nie ważności,
   3) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,
   4) niezwłocznej zmiany hasła tymczasowego, przekazanego przez ADO,
   5) poinformowania ADO o podejrzeniu lub rzeczywistym ujawnieniu hasła,
   6) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację liter (małych i wielkich), cyfr lub znaków specjalnych. **Długość znaków może być inna w przypadku uwierzytelniania w ramach poszczególnych aplikacji.**
   7) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
5. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób (np. na monitorach komputerów, pod klawiaturami),
   2) przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej,
   3) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,

4) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
5) udostępnianie haseł innym użytkownikom,
6) przeprowadzanie prób łamania haseł,
7) wpisywanie haseł „na stałe" (np. w skryptach logowania).

4. Procedura zawieszenia pracy w systemie informatycznym.

1. Każdorazowe zawieszenie pracy w systemie informatycznym wymaga zabezpieczenia systemu przed nieuprawnionym dostępem poprzez zablokowanie stacji roboczej przy użyciu komendy „Ctrl+Alt+Del i Zablokuj Komputer".
2. Przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe. Obowiązek ten stosowany jest bezwzględnie, zwłaszcza gdy w pomieszczeniu przebywają również osoby nieupoważnione.
3. Przed opuszczaniem miejsca pracy na dłuższy czas (np. przerwa na posiłek) użytkownik obowiązany jest wylogować się z systemu lub zablokować system.

5. Procedura zakończenia pracy w systemie informatycznym.

1. wylogować się z aplikacji i zamknąć aplikację,
2. zamknąć system.

VI. ZASADY OGÓLNE DLA UŻYTKOWNIKÓW SPRZĘTU INFORMATYCZNEGO

1. Zasady ogólne dla użytkowników sprzętu informatycznego

1. Przydzielanie uprawnień do korzystania z systemu informatycznego realizowane jest w oparciu o następujące zasady:
   1) „minimalnych przywilejów" – każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,
   2) „wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
   3) „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.
4. Każdemu użytkownikowi systemu nadawany jest unikalny identyfikator.
5. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
6. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się lub uruchomić wygaszacz ekranu z opcją ponownego logowania do systemu.
7. Na użytkowniku spoczywa obowiązek zabezpieczenia przed utratą opracowywanych przez siebie danych oraz wszelkich danych źródłowych.
8. Użytkownik ma następujące możliwości zabezpieczenia danych (plików) przed utratą:
   1) umieszczenie danych na nośniku danych (służbowy pendrive lub dysk sieciowy, jeśli występuje) – jest to zalecana forma zabezpieczenia danych,
   2) sporządzenie wydruków z przetwarzanymi danymi.

9. Niedopuszczalne jest umieszczanie w urządzeniach danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
10. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki CD-ROM, DVD, porty USB itp.) nośników danych rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
11. Zabrania się bez pisemnej zgody ADO używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci „flash" dołączane przez porty USB, karty radiowe, urządzenia „bluetooth", dyski wymienne, modemy niebędących własnością ADO.
12. Zabrania się wykorzystywania do celów służbowych bez zgody ADO innych niż dopuszczony do użytku, system poczty elektronicznej.
13. Należy zachować ostrożność przy otwieraniu załączników z nieznanych źródeł w poczcie elektronicznej.
14. Zaleca się wyłączenie opcji auto podglądu załączników w programie pocztowym.
15. Korzystając z programów MS Office i podobnych, zaleca się uaktywnienie wewnętrznego systemu ochrony przed wirusami MAKRO.
16. Należy regularnie przeprowadzać kontrolę antywirusową stanowiska programem zainstalowanym na urządzeniu.
17. Przed odczytaniem danych z nośnika danych, należy sprawdzić go programem antywirusowym.
18. Zabronione jest umożliwianie dostępu do systemu informatycznego osobom nieupoważnionym.
19. Zabronione jest rejestrowanie się w systemie informatycznym na identyfikatorze innego użytkownika.
20. Zabronione jest korzystanie z konta innego użytkownika bez zgody ADO i nadanych przez ADO uprawnień.
21. Zabronione jest przenoszenie informacji (w tym danych osobowych), uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne urządzenia mobilne, nośniki danych, w szczególności na prywatne telefony komórkowe, tablety, laptopy, komputery stacjonarne, pamięci typu pendrive i inne pamięci zewnętrzne lub ich przesyłanie za pośrednictwem prywatnej poczty elektronicznej e-mail.
22. Zabronione jest użytkowanie prywatnych nośników danych w ramach realizacji czynności służbowych.
23. Zabronione jest próbowanie testowania i omijania zabezpieczeń systemu informatycznego.
24. Zabronione jest udostępnianie informacji o zasadach ochrony systemu informatycznego, w tym identyfikatorach.
25. Zabronione jest samowolne modyfikowanie ustawień bezpieczeństwa w systemie informatycznym.
26. Zabronione jest celowe niszczenie danych gromadzonych w systemach informatycznych mających znaczenie archiwalne.
27. Zabronione jest celowe wprowadzanie błędnych danych do systemu informatycznego.
28. Zabronione jest udostępnianie danych osobom nieupoważnionym.
29. Zabronione jest przeglądanie stron internetowych o treściach nieodpowiednich lub szkodliwych.
30. Zabronione jest pobieranie i rozpowszechnianie nieautoryzowanego oprogramowania i danych z Internetu.
31. Zabronione jest korzystanie z usług internetowych, niemających związku z wykonywaną pracą.

2. Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa

1. W przypadku, gdy zachowanie systemu komputerowego odbiega od normy (komunikaty o błędach, nieoczekiwane zniknięcie lub pojawienie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.), należy przeprowadzić kontrolę antywirusową systemu oraz powiadomić o zaistniałej sytuacji ADO.

2. W przypadku gdy program antywirusowy wykryje istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (czytnik dvd-rom, USB itp.), wyraźnie oznaczyć i przekazać nośnik ADO. Następnie należy sporządzić notatkę służbową ze zdarzenia i przeprowadzić kontrolę antywirusową całego systemu.
3. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy, jeśli to możliwe, należy zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt ADO.

VII. ZASADY UŻYTKOWANIA URZĄDZEŃ MOBILNYCH I NOŚNIKÓW DANYCH ORAZ OBOWIĄZEK ICH ZABEZPIECZENIA KRYPTOGRAFICZNEGO

Niniejszy rozdział ma na celu zdefiniowanie wytycznych dotyczących użytkowania nośników danych oraz zapewnienia ich odpowiednich zabezpieczeń kryptograficznych. Dzięki tym zasadom, ADO dąży do skutecznej ochrony poufnych danych i zapewnienia, że przetwarzanie informacji odbywa się zgodnie z obowiązującymi przepisami o ochronie danych osobowych. Wszyscy pracownicy mają obowiązek przestrzegania tych zasad w celu minimalizacji ryzyka naruszenia prywatności danych i zapewnienia wysokiego poziomu bezpieczeństwa w organizacji.

1. Użytkowanie urządzeń mobilnych i nośników danych

W trosce o ochronę danych osobowych oraz zapewnienie bezpiecznej pracy w zakresie przetwarzania danych osobowych, ADO zapewnia dostęp do służbowych urządzeń mobilnych i nośników danych typu pendrive.

2. Obowiązkowe zabezpieczenie kryptograficzne urządzeń mobilnych i nośników danych

Przed dopuszczeniem do użytkowania, ADO zapewnia wdrożenie zabezpieczeń kryptograficznych wszystkich służbowych urządzeń mobilnych (w szczególności laptopy) oraz nośników danych. Zastosowanie kryptografii ma na celu skuteczną ochronę danych osobowych przed dostępem osób nieupoważnionych oraz minimalizację ryzyka utraty danych osobowych w przypadku kradzieży lub utraty urządzenia mobilnego lub nośnika danych. ADO jest odpowiedzialny za wybór i wdrożenie odpowiednich algorytmów kryptograficznych, które są zgodne z aktualnymi standardami branżowymi i normami bezpieczeństwa danych. Algorytmy te powinny zapewnić odpowiedni poziom zabezpieczenia danych i poufności informacji przechowywanych na urządzeniach, na których zastosowano kryptografię. ADO odpowiedzialny jest za wykazanie w razie potrzeby zastosowania zabezpieczenia kryptograficznego na danym sprzęcie.

Instrukcję zarządzania urządzeniami mobilnymi i nośnikami danych stanowi **Załącznik Nr 12** do Polityki.

3. Zakaz przenoszenia danych osobowych na prywatne urządzenia mobilne lub nośniki danych:

W celu zapewnienia najwyższego poziomu bezpieczeństwa i ochrony danych osobowych, wyraźnie zabrania się przenoszenia danych osobowych uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne urządzenia mobilne lub nośniki danych. W szczególności, zabronione jest korzystanie z prywatnych telefonów komórkowych, tabletów, laptopów, komputerów stacjonarnych, pamięci typu pendrive oraz innych pamięci zewnętrznych do przetwarzania czy przechowywania danych osobowych, przetwarzanych w ramach realizacji czynności służbowych. Również przesyłanie danych za pośrednictwem prywatnej poczty elektronicznej (e-mail) jest surowo zakazane, aby uniknąć nieautoryzowanego dostępu do danych osobowych.

VIII. EWIDENCJONOWANIE SPRZĘTU INFORMATYCZNEGO, APLIKACJI ORAZ UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

Prowadzenie:

a) Ewidencji sprzętu informatycznego,
b) Ewidencji aplikacji informatycznych,
c) Ewidencji użytkowników systemu informatycznego, służącego do przetwarzania danych osobowych,

stanowi zadanie ADO.

1. ADO ma obowiązek prowadzenia szczegółowej **ewidencji sprzętu informatycznego**. W ewidencji tej zawarte są informacje o oznaczeniu typu, przeznaczeniu, numerze seryjnym, parametrach technicznych, lokalizacji, użytkowniku przypisanym do danego urządzenia oraz zastosowanych zabezpieczeniach.
2. **Ewidencja aplikacji informatycznych** obejmuje kompleksowe informacje o zainstalowanych aplikacjach, oprogramowaniu oraz jego wersjach (np. program księgowy). ADO odnotowuje wszelkie ważne szczegóły, które umożliwią identyfikację i zarządzanie aplikacją w sposób efektywny i bezpieczny.
3. **Ewidencja użytkowników systemu informatycznego, służącego do przetwarzania danych osobowych** obejmuje swym zakresem informacje o imieniu, nazwisku, identyfikatorze użytkownika w systemie Windows.
4. W celu ułatwienia zarządzania i aktualizacji, prowadzenie w/w ewidencji w formie elektronicznej jest dopuszczalne. Przechowywanie danych w elektronicznej postaci umożliwia szybki dostęp do informacji oraz bieżącą aktualizację danych, co jest kluczowe w dynamicznym środowisku IT.
5. ADO jest odpowiedzialny za rzetelne i aktualne wprowadzanie danych do ewidencji.
6. Ewidencja stanowi cenny dokument podczas audytów związanych z infrastrukturą informatyczną oraz ochroną danych. Zbieranie i aktualizacja szczegółowych informacji o sprzęcie i systemach informatycznych pomaga w udokumentowaniu zgodności z przepisami i standardami bezpieczeństwa.
7. Wzór Ewidencji sprzętu informatycznego, aplikacji oraz użytkowników systemu informatycznego służącego do przetwarzania danych osobowych stanowi **Załącznik nr 17** do Polityki.

IX. ZARZĄDZANIE URZĄDZENIAMI MOBILNYMI I NOŚNIKAMI DANYCH

Zasady postępowania z urządzeniami mobilnymi i nośnikami danych określa Instrukcja zarządzania urządzeniami mobilnymi i nośnikami danych, stanowiąca **Załącznik nr 12** do Polityki.

X. KORZYSTANIE Z URZĄDZEŃ MOBILNYCH I NOŚNIKÓW DANYCH

Zasady użytkowania służbowych urządzeń mobilnych i nośników danych określa Regulamin korzystania z urządzeń mobilnych i nośników danych, stanowiący **Załącznik nr 13** do Polityki.

XI. ZASADY DOTYCZĄCE PRACY POZA SIEDZIBĄ ADMINISTRATORA

1. Praca zdalna określona przepisami Kodeksu Pracy ustanowiona jest odrębnymi od Polityki regulacjami wewnętrznymi Administratora.
2. Osoby pracujące poza siedzibą Administratora zobowiązane są do wykonywania swoich obowiązków wyłącznie przy użyciu służbowych urządzeń mobilnych i nośników danych na zasadach odrębnych.
3. Przy pracy na papierowych dokumentach zawierających dane osobowe należy stosować następujące, minimalne środki bezpieczeństwa:
   1) przy drukowaniu dokumentów należy od razu zabierać je z tacy odbiorczej, nie dopuszczając do gromadzenia się wydruków,
   2) dokumenty służbowe należy po godzinach pracy umieszczać w szufladzie, szafce lub szafie zamykanej na klucz,
   3) zbędne dokumenty służbowe powinny być niezwłocznie niszczone w niszczarce (nie mogą być wyrzucane do kosza na śmieci).
4. W razie zniszczenia, uszkodzenia, kradzieży lub zgubienia służbowego urządzenia użytkownik niezwłocznie zawiadamia o tym fakcie ADO.
5. W sprawach nieuregulowanych użytkownik jest zobowiązany do stosowania:
   1) obowiązującej Polityki Ochrony Danych Osobowych,
   2) innych wytycznych, regulaminów lub instrukcji związanych z ochroną danych osobowych lub bezpieczeństwem informacji,
   3) poleceń ADO.
6. Wszelkie pytania lub wątpliwości dotyczące bezpieczeństwa przetwarzanych danych użytkownik zobowiązany jest kierować niezwłocznie do IOD lub ADO.
7. W przypadkach innych niż wykonywanie pracy zdalnej (wykonywanej w trybie przepisów Kodeksu Pracy), ustanowionej odrębnymi od Polityki regulacjami wewnętrznymi, Pracownicy w przypadkach uzasadnionych mają możliwość złożenia wniosku do Administratora o możliwość okresowego wykorzystywania dla celów służbowych sprzętu służbowego poza siedzibą Administratora. Wniosek dotyczący wykorzystywania sprzętu służbowego poza siedzibą Administratora stanowi **Załącznik nr 18** do Polityki.

XII. ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

Udostępnienie danych osobowych może nastąpić na wniosek podmiotu uprawnionego na podstawie przepisów szczególnych.

1. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
2. W przypadku wniosku o udostępnienie danych, każda osoba, do której wpłynie taki wniosek, a która ma uzasadnione wątpliwości czy udostępnienie danych będzie zgodne z przepisami prawa, jest zobowiązana przekazać wniosek do IOD.
3. IOD rozpatruje przekazany wniosek oraz ustala czy wniosek o udostępnienie:
   a) jest sporządzony w formie pisemnej,
   b) wystarczająco identyfikuje osobę, której dane mają być udostępnione,
   c) wskazuje odpowiednią podstawę prawną udostępnienia danych,

d) określa zakres danych osobowych, których wniosek o udostępnienie danych osobowych dotyczy.

4. IOD ocenia, czy można legalnie udostępnić dane osobowe i wydaje rekomendację, którą następnie ADO przekazuje odbiorcy wniosku.
5. W razie braków formalnych wniosku o udostępnienie danych osobowych, ADO zwraca się do wnioskodawcy o ich usunięcie we wskazanym terminie pod rygorem pozostawienia wniosku bez rozpoznania.
6. Po uzyskaniu pozytywnej opinii od IOD w przedmiocie dopuszczalności udostępnienia danych osobowych, ADO bez zbędnej zwłoki udostępnia dane osobowe.
7. Dane osobowe powinny być udostępnione w sposób zapewniający ich poufność wobec osób postronnych.
8. Po uzyskaniu negatywnej opinii od IOD w przedmiocie dopuszczalności udostępnia danych osobowych, ADO nie udostępnia danych osobowych.
9. W przypadku, gdy wniosek dotyczy udostępnienia dokumentacji w oryginale oraz istnieją przesłanki ku pozytywnego rozpatrzenia takiego wniosku, ADO sporządza kopię udostępnianej dokumentacji.

XIII. ZASADY RESPEKTOWANIA PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Prawa osób, których dane są przetwarzane w ramach realizacji celów ustawowych oraz statutowych ADO realizowane są zgodnie z art. 15-21 RODO.

ADO każdorazowo konsultuje z Inspektorem Ochrony Danych możliwość realizacji w/w praw w odniesieniu do otrzymanego żądania od podmiotu danych.

Szczegółowe zasady dot. realizacji praw osób, których dane są przetwarzane określa **Załącznik Nr 6** do Polityki.

Instrukcja usuwania danych osobowych z kopii zapasowych i sprostowania danych osobowych w kopiach zapasowych stanowi **Załącznik nr 16** do Polityki.

XIV. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W IMIENIU ADMINISTRATORA

Jeżeli przetwarzanie ma być dokonywane w imieniu ADO, odbywa się ono zgodnie z art. 28 RODO w trybie zawartej pomiędzy Stronami umowy. ADO określa zasady przetwarzania danych osobowych z Wykonawcą usługi, uzyskuje potwierdzenie realizacji art. 32-36 RODO, a także dokonuje nadzoru Podmiotu przetwarzającego w trybie art. 28 lit. h RODO.

1. Jeżeli przetwarzanie ma być dokonywane w imieniu ADO, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Przy wyborze podmiotu przetwarzającego w celu zapewnienia najwyższych gwarancji bezpieczeństwa przetwarzanych danych osobowych po uzgodnieniu z Inspektorem Ochrony Danych jest możliwość zastosowania ankiety oceny podmiotu przetwarzającego, która wydawana

jest do uzupełnienia podmiotowi przetwarzającemu przed podpisaniem umowy, o której mowa w ust. 6. Wzór Ankiety oceny podmiotu przetwarzającego stanowi **Załącznik Nr 7** do Polityki.

3. Zakres przedmiotowy Ankiety oceny podmiotu przetwarzającego stanowiący **Załącznik Nr 7** do Polityki może ulec zmianie, w zależności od potrzeb zakresu weryfikacji podmiotu przetwarzającego.
4. ADO może odstąpić od wydania podmiotowi przetwarzającemu Ankiety, na rzecz innej formy jego sprawdzenia pod kątem zapewnienia najwyższych gwarancji bezpieczeństwa przetwarzanych danych osobowych.
5. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje ADO o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym ADO możliwość wyrażenia sprzeciwu wobec takich zmian.
6. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy (wzór umowy stanowi **Załącznik Nr 8** do Polityki), która wiąże podmiot przetwarzający i ADO, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa ADO. Ta umowa stanowi w szczególności, że podmiot przetwarzający:
   a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO,
   b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
   c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO,
   d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 5,
   e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,
   f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ADO wywiązać się z obowiązków określonych w art. 32–36 RODO,
   g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazują przechowywanie danych osobowych,
   h) udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
7. W związku z obowiązkiem określonym w art. 28 ust. 3 lit. h RODO podmiot przetwarzający niezwłocznie informuje ADO, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.
8. Jeżeli do wykonania w imieniu ADO konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między ADO a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji

wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec ADO za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

9. Wystarczające gwarancje, o których mowa w ust. 1 i 4 art. 28 RODO, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.
10. ADO prowadzi Rejestr umów przetwarzania danych osobowych w imieniu Administratora, którego wzór stanowi **Załącznik Nr 9** do Polityki.

XV. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

Administrator ma obowiązek prowadzić rejestr czynności przetwarzania zgodnie z wymaganiami zawartymi w art. 30 ust. 1 RODO oraz, jeżeli występuje jako podmiot przetwarzający, rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO.

Rejestry mają formę pisemną, w tym formę elektroniczną oraz są cyklicznie monitorowane i w razie potrzeby aktualizowane. Za przechowywanie i aktualizację rejestrów jest odpowiedzialny Administrator.

XVI. ZARZĄDZENIE RYZYKIEM

Zarządzenie ryzkiem to szereg skoordynowanych działań podejmowanych przez Administratora w celu identyfikacji i analizy ryzyka oraz określenia adekwatnych reakcji na ryzyko zwiększając poziom bezpieczeństwa przetwarzania danych osobowych w ramach poszczególnych procesów ich przetwarzania.

1. W ramach powyższych działań dla zidentyfikowanych procesów przetwarzania danych osobowych wskazuje się, analizuje oraz szacuje:
   1) zasoby – które będziemy chronić:
      a) sprzęt komputerowy przechowujący dane,
      b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
      c) prawa i wolności osób fizycznych, których dane dotyczą,
      d) aplikacje, w których przetwarzane są dane osobowe,
      e) pomieszczenia, w których pracują osoby upoważnione do przetwarzania danych osobowych.
   2) zastosowane środki bezpieczeństwa – zastosowane środki techniczne i organizacyjne, opisane w niniejszej Polityce,
   3) zagrożenia – zdarzenia, które można wyróżnić ze względu na utratę poufności, dostępności, integralności i rozliczalności przetwarzanych danych osobowych mogące powodować wystąpienie incydentu,
   4) podatności – słabości zasobów, które mogą być wykorzystane przez potencjalne zagrożenia,
   5) skutki – wpływ jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

2. Mając na uwadze powyższe, Administrator zapewnia warunki pracy w systemach informatycznych zapewniające poufność, dostępność, integralność i rozliczalność przetwarzanych danych osobowych.
3. Administrator jest zobowiązany dostosować środki bezpieczeństwa zarówno techniczne, fizyczne, jak i organizacyjne do wyników przeprowadzonej analizy ryzyka.
4. Zmiany związane z ust. 3 należy każdorazowo zaktualizować w Polityce.
5. Zidentyfikowane zagrożenia, podatności oraz skutki, o których mowa w ust. 1, podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka.
6. Identyfikację i analizę ryzyka przeprowadza się okresowo, co najmniej raz na dwa lata, w sposób udokumentowany, odnosząc się do obecnych oraz nowo zidentyfikowanych procesów przetwarzania danych osobowych.
7. Inspektor w ramach niniejszej procedury odpowiada za:

- wsparcie Administratora w zakresie prowadzonej analizy ryzyka,
- nadzór nad przestrzeganiem procedury, a w szczególności nad dokumentowaniem identyfikacji i analizy ryzyka,
- rozstrzyganie kwestii spornych w zakresie stosowanej metodyki zarządzania ryzykiem.

8. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO Administrator przeprowadza dla danego procesu przetwarzania **ocenę jego skutków** w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane. Przy czym podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy Administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

XVII. OCENA SKUTKÓW DLA OCHRONY DANYCH

1. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.
2. Przeprowadzając ocenę skutków dla ochrony danych bierze się pod uwagę nie interesy ADO, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.
3. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem tego przetwarzania dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
4. Dokonując oceny skutków dla ochrony danych, ADO konsultuje z IOD m.in. kwestie dotyczące:
   1) konieczności przeprowadzenia oceny skutków dla ochrony danych,
   2) metodologii przeprowadzenia oceny skutków dla ochrony danych,
   3) decyzji, czy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu,
   4) zabezpieczeń, w tym środków technicznych i organizacyjnych, stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą,
   5) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO, w szczególności czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować.
5. Ocena skutków zawiera co najmniej:
   1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez ADO,
   2) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
   3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
   4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać

przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

6. Oceny skutków dokonuje w ramach współpracy ADO oraz IOD w oparciu o rekomendowaną przez IOD metodologię.

XVIII. PRZEGLĄDY POLITYKI I AUDYTY

1. Przeglądy Polityki

1. Niniejsza Polityka powinna być poddawana przeglądowi przynajmniej raz na dwa lata. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zarządzić przegląd Polityki stosownie do występujących sytuacji i zdarzeń.
2. IOD analizuje, czy Polityka oraz inne dokumenty powiązane z Polityką są adekwatne do:

1) zmian w systemie informatycznym (np. nowe aplikacje służące do przetwarzania danych),
2) zmian organizacyjnych ADO (np. nowe stanowiska pracy wiążące się z przetwarzaniem danych, nowe obszary, gdzie przetwarzane są dane osobowe),
3) zmian w obowiązujących przepisach prawa.

2. Przeprowadzanie audytów zgodności

1. Audyt Ochrony Danych Osobowych ma na celu zapewnienie odpowiedniej ochrony danych osobowych gromadzonych, przetwarzanych i przechowywanych przez organizację. Celem audytu jest sprawdzenie zgodności z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, ocena skuteczności Polityki oraz identyfikacja obszarów wymagających poprawy.
2. Audyt Ochrony Danych Osobowych powinien być przeprowadzany cyklicznie, co najmniej raz na 2 lata. Powtarzające się audyty pozwalają na monitorowanie postępów w zakresie ochrony danych oraz szybką identyfikację nowych ryzyk i zagrożeń.
3. Audytowi podlegają wybrane aspekty, procesy, czynności oraz elementy, które mają wpływ na ochronę danych osobowych. Wybrane obszary podlegające audytowi mogą obejmować m.in.:
   a) Procedury zbierania i przetwarzania danych osobowych.
   b) Mechanizmy bezpieczeństwa i kontroli dostępu do danych.
   c) Polityki dotyczące zabezpieczeń technicznych i organizacyjnych.
   d) Procesy przechowywania i usuwania danych osobowych.
   e) Działania w przypadku naruszeń ochrony danych.
4. Po przeprowadzeniu audytu sporządzane jest sprawozdanie zawierające wyniki oceny, rekomendacje oraz zalecenia dotyczące poprawy ochrony danych osobowych. Wszystkie wyniki audytu i związane z nimi rekomendacje powinny być przedstawione w jasny i przejrzysty sposób, umożliwiający skuteczne wdrożenie zmian.
5. Rekomendacje i zalecenia wynikające z audytu są wcielane w życie w trybie bieżących prac. Administrator jest odpowiedzialny za wdrożenie niezbędnych zmian i usprawnień.

XIX. ZASADY PRZEPROWADZANIA SZKOLEŃ PRACOWNICZYCH

1. Wszyscy pracownicy, których obowiązki zawodowe wiążą się z dostępem do danych osobowych, są zobowiązani do zapoznania się z obowiązującymi zasadami ochrony danych osobowych, określonymi w Polityce oraz materiałem szkoleniowym, stanowiącym **Załącznik nr 3** do Polityki. Przed rozpoczęciem pracy, wymagane jest, aby każdy z pracowników podpisał stosowne oświadczenie potwierdzające wykonanie tej czynności (**Załącznik Nr 1** do Polityki).
2. Przynajmniej raz na dwa lata przeprowadza ADO zapewnia szkolenia grupowe dla wszystkich pracowników, którzy przetwarzają dane osobowe. Szkolenie obejmuje swym zakresem omówienie obowiązków spoczywających na pracownikach przetwarzających dane osobowe na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki.

3. ADO zapewnia odpowiednie warunki do przeprowadzenia szkoleń grupowych.
4. Szkolenie, o którym mowa w pkt. 2 może być prowadzone przez IOD lub wykonawcę zewnętrznego.
5. Pracownicy potwierdzają swój udział w szkoleniu własnoręcznym podpisem na liście obecności, którą przechowuje ADO.
6. Osoba przeprowadzająca szkolenie po jego zakończeniu sporządza szczegółowe sprawozdanie, które następnie przekazywane jest do zatwierdzenia przez ADO. Sprawozdanie zawiera podsumowanie omówionych zagadnień oraz informacje o liczbie uczestników i ich zaangażowaniu w szkoleniu.

Zapewnienie odpowiedniej wiedzy pracownikom w obszarze ochrony danych osobowych jest kluczowym elementem w zapewnieniu zgodności z przepisami oraz skutecznego zarządzania danymi w organizacji. Szkolenia grupowe, które odbywają się regularnie, umożliwiają nie tylko przekazanie aktualnych informacji, ale także wzmacniają świadomość pracowników w zakresie istotności ochrony danych osobowych i roli, jaką każdy z nich odgrywa w tym procesie.

XX. POSTANOWIENIA KOŃCOWE

Aktualizacji niniejszej Polityki dokonuje Administrator.

XXI. WYKAZ ZAŁĄCZNIKÓW

Załącznik Nr 1	– Oświadczenie o zapoznaniu się z systemem ochrony danych osobowych
Załącznik Nr 2	– Oświadczenie o zachowaniu danych osobowych w tajemnicy
Załącznik Nr 3	– Materiał szkoleniowy dla pracowników
Załącznik Nr 4	– Upoważnienie do przetwarzania danych osobowych
Załącznik Nr 5	– Procedura realizacji obowiązków informacyjnych
Załącznik Nr 6	– Instrukcja realizacji praw osób, których dane są przetwarzane
Załącznik Nr 7	– Przykładowa ankieta oceny podmiotu przetwarzającego
Załącznik Nr 8	– Wzór umowy przetwarzania danych osobowych w imieniu ADO
Załącznik Nr 9	– Rejestr umów przetwarzania danych osobowych w imieniu Administratora
Załącznik Nr 10	– Instrukcja postępowania w sytuacji powstania incydentów naruszenia ochrony danych osobowych
Załącznik Nr 11	– Instrukcja postępowania z kluczami
Załącznik Nr 12	– Instrukcja zarządzania urządzaniami mobilnymi i nośnikami danych
Załącznik Nr 13	– Regulamin korzystania z urządzeń mobilnych i nośników danych
Załącznik Nr 14	– Regulamin korzystania z dostępu do Internetu oraz z poczty elektronicznej
Załącznik Nr 15	– Instrukcja szyfrowania/odszyfrowywania pliku/katalogu programem 7-zip
Załącznik Nr 16	– Instrukcja usuwania danych osobowych z kopii zapasowych i sprostowania danych osobowych w kopiach zapasowych
Załącznik Nr 17	– Ewidencja sprzętu informatycznego, aplikacji oraz użytkowników systemu informatycznego służącego do przetwarzania danych osobowych
Załącznik Nr 18	– Wniosek dot. wykorzystania sprzętu służbowego poza siedzibą Administratora