Załącznik Nr 1
do Polityki Ochrony Danych Osobowych

OŚWIADCZENIE
O ZAPOZNANIU SIĘ Z SYSTEMEM OCHRONY DANYCH OSOBOWYCH

Ja, niżej podpisana(y):

Imię	
Nazwisko	

oświadczam, że:

1. Zapoznałam/em się z zasadami bezpiecznego przetwarzania danych osobowych w świetle przepisów 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 tych danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych),
   - Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Zapoznałam/em się z obowiązującymi u Administratora dokumentami dot. ochrony danych osobowych, które stanowi Polityka Ochrony Danych Osobowych.
3. Zapoznałam/em się z materiałem szkoleniowym z obszaru ochrony danych osobowych, stanowiącym Załącznik nr 3 do Polityki Ochrony Danych Osobowych.

_____

(data i czytelny podpis składającego oświadczenie)

Załącznik Nr 2
do Polityki Ochrony Danych Osobowych

OŚWIADCZENIE
O ZACHOWANIU DANYCH OSOBOWYCH W TAJEMNICY

Ja niżej podpisana(y):

Imię	
Nazwisko	

zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobu i formy ich przetwarzania i zabezpieczania, do których mam/ będę miał(a) dostęp w związku z wykonywaniem zadań służbowych i obowiązków wynikających z Umowy zawartej z Administratorem, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, prac zleconych, stażu, praktyki jak i po ustaniu zatrudnienia/zobowiązania.

Zobowiązuję się przestrzegać obowiązujących regulaminów, instrukcji i procedur, wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał(a) danych osobowych ze zbiorów Administratora.

Oświadczam, że zapoznałam(em) się z materiałami szkoleniowymi z obszaru ochrony danych osobowych i zrozumiałam(em) treść definicji danych osobowych w rozumieniu art. 4 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, *Dz. U. UE. L. 2016.119.1* z dnia 4 maja 2016 r.).

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może powodować pociągnięcie do odpowiedzialności karnej i cywilnej oraz może skutkować rozwiązaniem Umowy w trybie natychmiastowym.

_____

(data i czytelny podpis składającego oświadczenie)

Załącznik Nr 3
do Polityki Ochrony Danych Osobowych

SZKOLENIE WSTĘPNE DOT. PODSTAW OCHRONY DANYCH OSOBOWYCH

Rozpoczynając współpracę z Administratorem obowiązkiem pracownika/współpracownika jest poznanie podstawowych pojęć oraz obowiązujących zasad z zakresu ochrony danych osobowych.

W razie pytań lub wątpliwości, które nasuną się Pani/Panu w ramach zapoznawania się z niniejszym materiałem – zachęcam do kontaktu:

Dawid Czerw
Inspektor Ochrony Danych
722-309-224

Niniejszy materiał szkoleniowy przybliży Pani/Panu następujące zagadnienia:

1. Kto jest Administratorem danych osobowych?
2. Czym są dane osobowe?
3. Czym jest przetwarzanie danych osobowych?
4. Istota ochrony danych osobowych
5. Przetwarzanie danych osobowych przez pracownika oraz jego obowiązki z tym związane
6. Odpowiedzialność pracownika za bezpieczeństwo przetwarzanych danych osobowych
7. Kim jest Inspektor Ochrony Danych?
8. Współpraca z Inspektorem Ochrony Danych
9. Postępowanie w sytuacji naruszenia ochrony danych osobowych
10. Postępowanie w sytuacji udostępnienia danych osobowych innemu podmiotowi
11. Postępowanie w sytuacji zlecenia przetwarzania danych osobowych innemu podmiotowi [tzw. powierzenie danych].

1. Kto jest Administratorem danych osobowych?

Zgodnie z art. 4 pkt. 7 Według Rozporządzenia Ogólnego o Ochronie Danych Osobowych [RODO] - Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

2. Czym są dane osobowe?

Według Rozporządzenia Ogólnego o Ochronie Danych Osobowych [RODO], danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę możliwą do zidentyfikowania uważa się osobę, której tożsamość można określić na podstawie numeru identyfikacyjnego lub też ze względu na unikalne czynniki określające jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Danymi osobowymi są m.in. takie informacje jak:

Imię, nazwisko, wizerunek, data urodzenia, PESEL, nr dowodu tożsamości, miejsce urodzenia, miejsce zamieszkania, adres do korespondencji, numer telefonu, adres e-mail, dane o lokalizacji, adres IP, dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

W związku z powyższym, każda osoba, z którą będzie mieć Pani/Pan do czynienia w ramach realizacji czynności służbowych będzie cechowała się danymi osobowymi o różnym zakresie.

Przede wszystkim będziecie Państwo przetwarzać dane osobowe dzieci, rodziców/opiekunów prawnych, zleceniobiorców, wykonawców etc.

Poznacie Państwo imię, nazwisko kolegi/koleżanki z pracy. Niejednokrotnie uzyskacie też informacje o ich życiu prywatnym, aspektach zdrowotnych lub rodzinnych, poglądach politycznych. Warto mieć na uwadze ich prawo do prywatności i tego typu informacje pozostawić wyłącznie dla siebie.

Pamiętajcie Państwo, informacje uzyskane w ramach pracy zawodowej muszą zostać zachowane w całkowitej poufności w ramach relacji prywatnych.

3. Czym jest przetwarzanie danych osobowych?

Przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.

Będzie Pani/Pan przetwarzał dane osobowe w momencie ich pozyskiwania, utrwalania, porządkowania, przechowywania, przeglądania, wykorzystywania ujawniania, przesyłania, rozpowszechniania, usuwania (i inne określone w art. 4 RODO].

W związku z powyższym przetwarzanie danych osobowych będzie Pani/Panu towarzyszyło permanentnie w ramach realizacji czynności służbowych.

4. Istota ochrony danych osobowych

Fundamentalne jest zrozumienie, iż każda osoba na gruncie Konstytucji RP ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym [art. 47 Konstytucji]. Konstytucja wskazuje również na prawo ochrony danych osobowych, precyzując, iż **nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby.**

Wszystko to wynika z przyrodzonej i niezbywalnej godności człowieka, która stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych.

Powyższe podsumować można w dwóch punktach:

1) Przetwarzanie danych osobowych musi odbywać się w granicach przepisów prawa
2) Administrator ma obowiązek zapewnić ochronę przetwarzanych danych osobowych

Ochrona danych osobowych to zabezpieczenie tych danych przed ich utratą, wyciekiem, czy nieuprawnionym dostępem - niedopuszczenie do sytuacji, aby te dane były przetwarzane przez osoby nie mające do tego uprawnienia.

Przepisy o ochronie danych osobowych nie wskazują konkretnych rodzajów zabezpieczeń, ponieważ ich dobór uzależniony jest od specyfiki działania danej jednostki. **Dlatego w ramach regulacji wewnętrznych funkcjonuje dokument regulujący zasady przetwarzania danych osobowych oraz odpowiedzialność osób je przetwarzających. Jest to Polityka Ochrony Danych Osobowych.**

Do tego dokumentu posiada wgląd każdy pracownik, dlatego jeżeli chce Pan/Pani zagłębić dany aspekt systemu ochrony danych osobowych, aby efektywnie uczestniczyć w ochronie danych osobowych, zachęcam do jego okresowego przeglądania.

5. Przetwarzanie danych osobowych przez pracownika/współpracownika oraz jego obowiązki z tym związane

Czy pracownik/współpracownik może przetwarzać dane osobowe?

Tak. Każda z osób zatrudnionych (niezależnie od formy współpracy), której czynności wiążą się z przetwarzaniem danych osobowych tuż przed rozpoczęciem pracy zostaje upoważniona do przetwarzania danych osobowych.

Czy każdy pracownik ma dostęp do wszystkich danych osobowych przetwarzanych w jednostce?
Nie. Każdy z pracowników zostaje upoważniony do przetwarzania danych osobowych w zakresie adekwatnym do realizowanych czynności służbowych.

Jakie obowiązki spoczywają na pracowniku/współpracowniku?

- Zobowiązana/y jest Pani/Pan do przestrzegania zasad ochrony danych osobowych określonych w dokumentacji wewnętrznej – co skwitować można jako **świadome oraz odpowiedzialne przetwarzanie danych osobowych, oparte na poszanowaniu prawa do prywatności osób, których danymi dysponujemy.**
  Podczas wykonywania czynności służbowych często się spieszymy, tracimy czujność – wtedy najczęściej dochodzi do naruszeń ochrony danych osobowych. Dlatego ważne jest zachowanie szczególnej staranności w trakcie przetwarzania danych.
- Zobowiązana/y jest Pani/Pan do dbania o bezpieczną eksploatację sprzętu informatycznego, stosowanie polityki haseł, zachowania szczególnej ostrożności w zakresie użytkowania korespondencji mailowej.
- Zobowiązana/y jest Pani/Pan do dbania, by dokumenty były przechowywane w zamkniętych szafach lub szufladach. Dostęp do kluczy mogą mieć tylko osoby uprawnione do przetwarzania danych.
- Zobowiązana/y jest Pani/Pan do włączania przełożonego oraz Inspektora Ochrony Danych we wszelkie sprawy wymagające konsultacji w zakresie stosowania przepisów ochrony danych osobowych.
- Zobowiązana/y jest Pani/Pan do dostarczania przełożonemu oraz Inspektorowi Ochrony Danych projektów umów, wzorów formularzy, druków, umów powierzenia do konsultacji ich treści.

1. **Użytkownicy przetwarzają dane osobowe, do których przetwarzania zostali upoważnieni przez Administratora wyłącznie przy użyciu służbowego sprzętu komputerowego;**
2. **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.**
3. **Zabronione jest użytkowanie prywatnych nośników danych w ramach realizacji czynności służbowych.**
4. **Zabronione jest rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika.**

Złamanie powyższych zasad obarczone jest sankcją karną w trybie art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Szczegółowy zakres zadań pracownika określony został w Polityce Ochrony Danych Osobowych.

6. Odpowiedzialność pracownika za bezpieczeństwo przetwarzanych danych osobowych

Nieprzestrzeganie zasad postępowania określonych w dokumentacji wewnętrznej może nieść za sobą szereg konsekwencji, od zwolnienia dyscyplinarnego, aż po postępowanie cywilne oraz karne.

Przykład 1.
Jeżeli Pracownik w ramach służbowych działań wykorzysta prywatny pendrive i przeniesie na niego dokumenty zawierające dane osobowe (w tym też fotografie zawierające wizerunek innych osób), a następnie go zgubi – dochodzi do naruszenia ochrony danych osobowych, a pracownik ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora.
Jaką odpowiedzialność pracownik może ponieść w opisanej sytuacji? Z pewnością dyscyplinarna, w zależności od okoliczności – cywilna lub karna. Otóż na ten aspekt składa się wiele okoliczności, takich jak np. umyślność działania, formy zabezpieczenia pendrive'a, rodzaj dokumentów, okoliczności zagubienia etc.
Należy mieć na uwadze fakt, iż zagubienie takiego nośnika należy zgłosić niezwłocznie do Administratora, ponieważ po odnalezieniu nośnika przez osobę nieuprawnioną wydarzyć się mogą różne scenariusze (żądanie znaleźnego, rozpowszechnienie informacji o znalezisku w mediach, szantaż etc.).

Przykład 2.
Jeżeli Pracownik w ramach realizacji czynności służbowych przesyła dokumenty zawierające dane osobowe poprzez korespondencję mailową, może omyłkowo przesłać dokument do innego adresata. Ważne jest niezwłoczne poinformowanie Administratora o zaistniałym zdarzeniu, ponieważ od analizy tego czy dokument został przez Pracownika zabezpieczony hasłem, jaki zakres danych osobowych mieścił się w dokumencie oraz czy dokument rzeczywiście dotarł do błędnie wskazanego adresata, będzie zależało dalsze postępowanie w sprawie.
Istotne jest, aby Pracownik w zakresie opisanej powyżej korespondencji zabezpieczał plik hasłem, które przesłane zostanie alternatywną drogą komunikacji. Dzięki temu ryzyko nieuprawnionego dostępu do danych osobowych jest dużo mniejsze.

7. Kim jest Inspektor Ochrony Danych?

Inspektor Ochrony Danych [IOD] to osoba wyznaczana przez administratora, wspierająca Administratora przy realizacji obowiązków wynikających z przepisów o ochronie danych osobowych.

Funkcję Inspektora Ochrony Danych pełni p. Dawid Czerw, tel.: 722-309-224.

Zadania Inspektora Ochrony Danych to:

- informowanie administratora 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;
- monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora 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;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego 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.

8. Współpraca z Inspektorem Ochrony Danych

Bardzo ważna jest współpraca z Inspektorem Ochrony Danych, przede wszystkim komunikacja oraz informowanie o incydentach godzących w prawo do prywatności oraz wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych.

Z Inspektorem Ochrony Danych komunikować się powinien każdy pracownik, który potrzebuje wsparcia w zakresie stosowania przepisów o ochronie danych osobowych podczas tworzenia lub aktualizacji regulaminów druków, formularzy, umów, a także podczas chęci modyfikacji aktualnych procesów, w zakresie których przetwarzane są dane osobowe.

W przypadku nawiązywania współpracy z podmiotami zewnętrznymi oraz w ogólnych relacjach z podmiotami, których istotą jest dysponowanie danymi osobowymi - kontakt z Inspektorem Ochrony Danych jest wskazany.

9. Postępowanie w sytuacji naruszenia ochrony danych osobowych

Zgodnie z art. 4 pkt. 12 RODO 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.

Każdorazowy przypadek naruszenia (świadomy lub nie) należy **bezzwłocznie** zgłosić przełożonemu oraz Inspektorowi Ochrony Danych – proszę telefonować do Inspektora Ochrony Danych niezwłocznie i opowiedzieć co się stało.

Dlaczego bezzwłocznie? Otóż IOD za zadanie ma ocenić wagę naruszenia praw i wolności osób, których dane osobowe objęte są naruszeniem. Szczegółowa analiza pozwala ocenić, czy naruszenie podlega zgłoszeniu do organu nadzorczego tj. Urzędu Ochrony Danych Osobowych.

Co istotne, jeżeli waga naruszenia będzie wskazywała na potrzebę powiadomienia organu, należy to zrobić w ciągu 72 godzin od momentu wykrycia naruszenia.

Szczegóły znajdują się w Załączniku nr 10 do Polityki Ochrony Danych Osobowych - **Instrukcja postępowania w sytuacji powstania incydentów naruszenia ochrony danych osobowych**

10. Postępowanie w sytuacji udostępnienia danych osobowych innemu podmiotowi

Do udostępnienia danych osobowych dochodzi w sytuacji, gdy uprawniony podmiot [np. Policja, Prokuratura, Sąd, ABW, SKW, SOP i inne] wystąpi z wnioskiem o udostępnienie pewnego zakresu danych o osobie.

W tej sytuacji uprawniony podmiot jest Administratorem danych, który posiada własny cel przetwarzania danych osobowych np. czynności wyjaśniające.

W związku z tym, podmiot wnioskujący musi posiadać stosowną podstawę prawną, która zobliguje Administratora do udostępnienia danych.

Co ważne – wniosek musi mieć formę pisemną, musi również posiadać podstawę prawną żądania udostępnienia danych, musi wystarczająco identyfikować osobę, której dane mają zostać udostępnione, a także określać zakres tych danych.

W sytuacji wątpliwości, gdy wniosek trafi do Państwa, należy skonsultować się z Inspektorem Ochrony Danych, w celu wykluczenia żądania bezprawnego.

11. Postępowanie w sytuacji zlecenia przetwarzania danych osobowych innemu podmiotowi

Zlecenie przetwarzania danych osobowych innemu podmiotowi to umocowanie przez Administratora innego podmiotu do przetwarzania danych w jego imieniu (tzw. powierzenie danych).

W relacji powierzenia danych mamy zatem do czynienia z Administratorem, który zleca podmiotowi [procesorowi] przetwarzanie danych osobowych w jego imieniu, na jego rzecz i na jego zasadach.

Powierzając dane, Administrator w żadnym stopniu nie traci nad nimi kontroli. Posiada pełną władzę nad tym co dzieje się z przekazanymi danym. Administrator może w każdej chwili zażądać np. zwrotu lub usunięcia danych osobowych.

Z drugiej strony, procesor nie nabywa żadnej kontroli. Dlatego nie może samodzielnie decydować o celach i sposobach przetwarzania przekazanych mu danych osobowych.

Ramy przetwarzania powierzonych danych osobowych określa umowa powierzenia. Dla procesora stanowi ona podstawę przetwarzania, a dla Administratora podstawę przekazania danych. Przetwarzanie dokonywane poza umową powierzenia będzie podwójnym naruszeniem. Nie tylko zobowiązań kontraktowych, ale również naruszeniem przepisów RODO. Skutkuje wieloma dodatkowymi ryzykami, w tym – ryzykiem otrzymania kary finansowej od organu nadzoru.

W związku z powyższym każdorazowo, podczas przekazywania danych osobowych podmiotom zewnętrznym np. firmom szkoleniowym, zlecając prace fotografowi, korzystając z serwisu komputerowego, który będzie miał dostęp do dysków twardych, należy skonsultować się z Inspektorem Ochrony Danych.

Uprzejmie Państwa proszę o respektowanie poufności oraz o świadomość i uważność w zakresie dysponowania danymi osobowymi. Przyczyni się to do wzmacniania kultury ochrony danych osobowych w naszej organizacji.
Dziękując Państwu za ostrożność zachęcam do systematycznej konsultacji i doradztwa, co pozwoli uniknąć zakłóceń.

Z poważaniem
Dawid Czerw
Inspektor Ochrony Danych

Załącznik Nr 4
do Polityki Ochrony Danych Osobowych

....., dnia ..... r.

UPOWAŻNIENIE Nr .....

Na podstawie art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych *Dz. U. UE . L. 2016.119.1* z dnia 4 maja 2016 r.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną/zatrudnionego w Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, na stanowisku: ..... do przetwarzania danych osobowych w zakresie wykonywania zadań, zgodnie z przyjętym zakresem obowiązków.

Uprawniam do przetwarzania danych osobowych w w/w zakresie od dnia ..... do dnia ..... / na czas nieokreślony.*

***niepotrzebne skreślić**

Wyżej wymieniona osoba została wpisana do ewidencji osób upoważnionych do przetwarzania danych oraz pouczona o obowiązku zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczania.

.....
(podpis Administratora)

.....
(podpis Osoby Upoważnionej)

ADNOTACJE W ZAKRESIE ODWOŁANIA UPOWAŻNIENIA

Z dniem ..... r., odwołuję niniejsze upoważnienie do przetwarzania danych osobowych wydane w dniu ..... r.

.....
Czytelny podpis Administratora

Załącznik Nr 4
do Polityki Ochrony Danych Osobowych

....., dnia ..... r.

UPOWAŻNIENIE Nr .....

Na podstawie art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych *Dz. U. UE . L. 2016.119.1* z dnia 4 maja 2016 r.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

świadczącą/świadczącego usługi na rzecz Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, na podstawie Umowy o współpracy z dnia ..... do przetwarzania danych osobowych w zakresie wykonywania zadań, zgodnie z przyjętym zakresem obowiązków.

Uprawniam do przetwarzania danych osobowych w w/w zakresie od dnia ..... do dnia ..... / na czas nieokreślony.*

***niepotrzebne skreślić**

Wyżej wymieniona osoba została wpisana do ewidencji osób upoważnionych do przetwarzania danych oraz pouczona o obowiązku zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczania.

.....
(podpis Administratora)

.....
(podpis Osoby Upoważnionej)

ADNOTACJE W ZAKRESIE ODWOŁANIA UPOWAŻNIENIA

Z dniem ..... r., odwołuję niniejsze upoważnienie do przetwarzania danych osobowych wydane w dniu ..... r.

.....
Czytelny podpis Administratora

Załącznik Nr 5
do Polityki Ochrony Danych Osobowych

PROCEDURA REALIZACJI OBOWIĄZKÓW INFORMACYJNYCH

§ 1

Słowniczek pojęć

Ilekroć w Procedurze jest mowa o:

1) Klauzuli informacyjnej – oznacza informacje o przetwarzaniu danych osobowych, które należy podać osobie, której dane dotyczą zgodnie z wymogami art. 13 -14 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).
2) RODO lub rozporządzeniu – oznacza 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).
3) Muzeum - oznacza Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28.
4) Procedura- oznacza niniejszą Procedurę realizacji obowiązków informacyjnych wynikających z art. 13-14 RODO.

§ 2

Podstawy prawne

Art. 13 RODO - Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą.

Art. 14 RODO - Informacje podawane osobie, której dane dotyczą w przypadku pozyskania danych osobowych w sposób inny niż od osoby, której dane dotyczą.

§ 3

Sposób realizacji obowiązków informacyjnych.

1. Wykaz oraz szczegółowy sposób realizacji obowiązków informacyjnych przedstawia tabela, stanowiąca załącznik nr 1 do Procedury.
2. Wzór klauzuli informacyjnej stanowi załącznik nr 2 do Procedury.
3. Administrator prowadzi wykaz klauzul informacyjnych jednostki i dokonuje systematycznego przeglądu i aktualizacji ich treści (nie rzadziej niż raz na dwa lata).

§ 4

Terminy realizacji obowiązków informacyjnych.

a. Obowiązek informacyjny z art. 13 RODO - w momencie pozyskiwania danych osobowych.

b. Obowiązek informacyjny z art. 14 RODO- najpóźniej w ciągu miesiąca od pozyskania danych.

§ 5

Przesłanki wyłączenia w zakresie realizacji obowiązków informacyjnych.

1) art. 13 RODO- gdy osoba, której dane dotyczą posiada już te informacje – w tym konkretnym celu i zakresie.
2) art. 14 RODO, gdy:
   - osoba, której dane dotyczą dysponuje już tymi informacjami
   - udzielenie takich informacji okazuje się niemożliwe lub wymagałaby niewspółmiernie dużego wysiłku
   - realizacja obowiązku informacyjnego może uniemożliwić lub znacząco utrudnić realizację celów takiego przetwarzania
   - pozyskanie lub ujawnienie danych jest wyraźne uregulowane w przepisach prawa
   - dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania w tajemnicy zawodowej określonym w przepisach prawa.

§ 6

Postanowienia końcowe.

1. Każda klauzula informacyjna stosowana w jednostce otrzymuje numer początkowy, według wzoru KI-1. W przypadku aktualizacji druku należy wskazać kolejną wersję druku według schematu: KI-1.1, KI-1.2.

2. W jednostce prowadzony jest wykaz klauzul informacyjnych, według wzoru:

Czynność/cel przetwarzania danych osobowych	Rodzaj obowiązku informacyjnego	Nr klauzuli /wersja	Osoba odpowiedzialna za realizację obowiązku	Sposób realizacji obowiązku informacyjnego	Czynność/cel przetwarzania danych osobowych

   Wykaz prowadzony jest wyłącznie w formie elektronicznej.
   ** w pole uwagi należy wpisać datę zaprzestania korzystania z druku i powód.

3. W sprawach nieuregulowanych w Procedurze stosuje się zapisy art. 13-14 RODO, a także:
   a) przepisy aktów prawnych określające sposób realizacji obowiązków informacyjnych,
   b) postanowienia polityk i procedur z zakresu ochrony danych osobowych w Szpitalu, w tym Procedury realizacji praw osób, których dane dotyczą,
   c) wytyczne inspektora ochrony danych,
   d) opinie prawne oraz polecenia wydawane przez Dyrektora Szpitala.

Załącznik nr 1
do Procedury realizacji obowiązków
informacyjnych

WYKAZ KLAUZUL INFORMACYJNYCH

Czynność/cel przetwarzania danych osobowych	Rodzaj obowiązku informacyjnego	Nr klauzuli /wersja	Osoba odpowiedzialna za realizację obowiązku	Sposób realizacji obowiązku informacyjnego
Informacja dot. przetwarzania danych osobowych osób zwiedzających Muzeum	Art. 13	KI-1		Informacja wywieszona jest w Siedzibie Muzeum. https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych osób fizycznych, osób fizycznych prowadzących działalność gospodarczą oraz reprezentantów osób prawnych	Art. 13	KI-2		Informacja dołączana jako paragraf w umowie Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja o przetwarzaniu danych osobowych osób wskazanych do kontaktu i realizacji umowy	Art. 13 lub art. 14 RODO	KI-3		Informacja dołączana jako załącznik do umowy Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13. Stosując niniejszą informacje należy zastosować w umowie następujący zapis: "Wykonawca zobowiązany jest przekazać osobie wyznaczonej do kontaktów z Zamawiającym informację o przetwarzaniu jej danych osobowych, która znajduje się pod linkiem https://bip.muzeum.rewal.pl/dokumenty/menu/13"
Informacja o przetwarzaniu danych osobowych – zamówienie publiczne poniżej 130 000 zł	Art. 13	KI-4		Informacja dołączana jako część formularza oferty Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja o przetwarzaniu	Art. 13	KI-5		Informacja dołączana jako część formularza oferty

danych osobowych w procesie zamówień publicznych				Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych osób składających wniosek o udostępnienie informacji w trybie ustawy o dostępie do informacji publicznej	Art. 13	KI-6		Informacja dołączana jako załącznik do odpowiedzi Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych osób biorących udział w rekrutacji na stanowisko pracy	Art. 13	KI-7		Ogłoszenie o rekrutacji/naborze Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych w zakresie prowadzenia akt osobowych pracowników i realizowaniu ustawowych obowiązków związanych z zatrudnieniem	Art. 13	KI-8		Umowa/kwestionariusz osobowy dla pracownika Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych praktykantów	Art. 13	KI-9		Informacja dołączana jako paragraf w umowie/porozumieniu Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych stażystów	Art. 13	KI-10		Informacja dołączana jako paragraf w umowie/porozumieniu Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych wolontariuszy	Art. 13	KI-11		Informacja dołączana jako paragraf w umowie/porozumieniu Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.
Informacja dot. przetwarzania danych osobowych osób składających skargi, wnioski lub podania (i inne) w trybie ustawy z	Art. 13	KI-12		Strona BIP - https://bip.muzeum.rewal.pl/dokumenty/menu/13.

dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego				

KI-1

Informacja dot. przetwarzania danych osobowych osób zwiedzających Muzeum

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu realizacji zadań statutowych, a także dla celów ustawowych z nimi związanych, w związku z wypełnieniem obowiązków wynikających z przepisów prawa. Obowiązki te wynikają m.in. z

- ustawy z dnia 21 listopada 1996 r. o muzeach;
- ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej;

Pani/Pana dane osobowe przetwarzane będą w celu:

1) realizacji uprawnień zwiedzających dotyczących ulg przy zakupie biletów wstępu do Muzeum - podstawą prawną przetwarzania danych jest niezbędność wypełnienia obowiązku prawnego ciążącego na administratorze danych, art. 6 ust. 1 lit. c RODO, w związku z ustawą z dnia 21 listopada 1996 r. o muzeach,
2) sprzedaży biletów, usług i towarów - podstawą prawną przetwarzania jest niezbędność przetwarzania danych do wykonywania umowy, art. 6 ust. 1 lit. b RODO,
3) wypełnienia obowiązków dokumentacyjnych dla celów podatkowych - podstawą prawną przetwarzania danych jest niezbędność wypełnienia obowiązku prawnego ciążącego na administratorze danych, art. 6 ust. 1 lit. c RODO.

4. Okres przetwarzania danych

Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji wskazanych powyżej celów przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z przepisów prawa.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. podmioty serwisujących nasze oprogramowanie, podmioty świadczące usługi IT, audytorskie, usługi archiwizacji, niszczenie, przewożenie i przechowywania dokumentacji, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. obsługa prawna, podmioty prowadzące działalność pocztową lub kurierską.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych

Podanie danych osobowych jest dobrowolne, jednakże jest niezbędne do wejścia i przybywania na terenie Muzeum, skorzystania z ulgowych biletów, zakupu usług i towarów.

KI-2

Informacja dot. przetwarzania danych osobowych osób fizycznych, osób fizycznych prowadzących działalność gospodarczą oraz reprezentantów osób prawnych

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu zawarcia i realizacji umowy.

Podstawą przetwarzania Pani/Pana danych osobowych jest zawarcie i realizacja umowy oraz spełnienie ciążących na Administratorze obowiązków prawnych wynikających z prawa Unii lub prawa polskiego w tym przepisów podatkowych i rachunkowości, a także przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów Administratora np.: ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami, co stanowi o zgodnym z prawem przetwarzaniu Pani/Pana danych osobowych zgodnie z art. 6 ust. 1 lit. b, lit. c oraz lit. f RODO.

4. Okres przetwarzania danych

Pani/Pana dane osobowe będą przetwarzane przez okres realizacji umowy oraz okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych Administratora w zakresie archiwizacji dokumentów, oraz przepisów o rachunkowości, a także przez okres przedawnienia roszczeń przysługujących Administratorowi i w stosunku do niego tj. 6 lat.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. podmioty świadczące usługi informatyczne, usługi dostarczania oprogramowania księgowego, usługi hostingowe, usługi archiwizacji, niszczenia i przewożenia dokumentów, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu np.: Poczta Polska.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii, zgodnie z art. 15 RODO;
b) prawo do sprostowania (poprawiania) swoich danych osobowych, zgodne z art.16 RODO;
c) prawo do usunięcia danych, zgodnie z art. 17 RODO;
d) prawo do ograniczenia przetwarzania danych osobowych, zgodnie z art. 18 RODO;
e) prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych w celu określonym w pkt. 3 z przyczyn związanych z Pani/Pana szczególną sytuacją, zgodnie z art. 21 RODO.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych

Podanie przez Pani/ Pana danych ma charakter dobrowolny, ale jest konieczne do zawarcia i realizacji umowy.

KI-3

Informacja o przetwarzaniu danych osobowych osób wskazanych do kontaktu i realizacji umowy

Zgodnie z art. 14 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Pani/Pana dane osobowe będą przetwarzane w celu bieżącego kontaktu w związku z realizacją zawartej umowy. Podstawą przetwarzania Pani/Pana danych osobowych jest prawnie uzasadniony interes administratora, co stanowi o zgodnym z prawem przetwarzaniu Pani/Pana danych osobowych zgodnie z art. 6 ust. 1 lit. f RODO.

4. Okres przetwarzania danych

Pani/Pana dane osobowe będą przetwarzane przez okres realizacji umowy oraz okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych administratora w zakresie archiwizacji dokumentów, oraz przepisów o rachunkowości, a także przez okres przedawnienia roszczeń przysługujących administratorowi i w stosunku do niego tj. 6 lat.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu administratora, np. podmioty świadczące usługi informatyczne, usługi dostarczania oprogramowania księgowego, usługi hostingowe, usługi archiwizacji, niszczenia i przewożenia dokumentów jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu np.: Poczta Polska.

6. Źródło pochodzenia danych oraz kategorie danych osobowych

Pani/Pana dane pozyskaliśmy w związku z zawarciem umowy Administrator przetwarza Pani/Pana dane osobowe w zakresie: imienia, nazwiska, nr telefonu, adresu email.

7. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii, zgodnie z art. 15 RODO;
b) prawo do sprostowania (poprawiania) swoich danych osobowych, zgodne z art. 16 RODO;
c) prawo do usunięcia danych, zgodnie z art. 17 RODO;
d) prawo do ograniczenia przetwarzania danych osobowych, zgodnie z art. 18 RODO;
e) prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych w celu określonym w pkt. 3 z przyczyn związanych z Pani/Pana szczególną sytuacją, zgodnie z art. 21 RODO.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Informacja o przetwarzaniu danych osobowych – zamówienie publiczne poniżej 130 000 zł

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celach związanych z prowadzonym postępowaniem o udzielenie zamówienia publicznego prowadzonego w trybie zapytania ofertowego, zawarciem umowy oraz dochodzeniem ewentualnych roszczeń związanych z postępowaniem.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy),
- art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze, w tym przepisów ustawy z dnia 23 kwietnia 1964 r. – kodeks cywilny, ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych).

4. **Okres przetwarzania danych**

Pani/Pana dane osobowe będą przetwarzane do czasu osiągnięcia celów, dla których zostały pozyskane wskazanych w ust. 3, a następnie przez okresy przewidziane w wewnętrznych uregulowaniach Administratora oraz przez okres wymagany przepisami prawa w tym Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych tj. przez okres 5 lat od zakończenia postępowania o udzielenie zamówienia.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora na podstawie zawartych umów powierzenia przetwarzania danych osobowych np. podmioty świadczące usługi informatyczne, usługi hostingowe, usługi archiwizacji i niszczenia dokumentów, jak również inni administratorzy danych osobowych przetwarzające dane we własnym imieniu np. podmioty prowadzące działalność pocztową.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO, przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;
d) prawo do usunięcia swoich danych osobowych w sytuacji, kiedy dane osobowe nie są już niezbędne do celów, w których zostały zebrane zgodnie z art. 17 RODO,

Jeśli chce Pni/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych wskazany w ust. 2 lub pisemnie na adres korespondencyjny wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych

Obowiązek podania przez Panią/Pana danych osobowych jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.

KI-5

Informacja o przetwarzaniu danych osobowych w procesie zamówień publicznych

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w trybie art. 6 ust. 1 lit. c RODO w związku z ustawą z dnia 11 września 2019 r. – Prawo zamówień publicznych w celu związanym z postępowaniem o udzielenie zamówienia publicznego.

4. Okres przechowywania

Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w ust. 3, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.

5. Odbiorcy danych

Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych - dalej „ustawa Pzp".

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora na podstawie zawartych umów powierzenia przetwarzania danych osobowych np. podmioty świadczące usługi informatyczne, usługi hostingowe, usługi archiwizacji i niszczenia dokumentów, uczestnicy procesu inwestycyjnego i ich umocowani przedstawiciele jak również inni administratorzy danych osobowych przetwarzające dane we własnym imieniu np. podmioty prowadzące działalność pocztową.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;
b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;
c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych

Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych wynikają z ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.

KI-6

Informacja dot. przetwarzania danych osobowych osób składających wniosek o udostępnienie informacji w trybie ustawy o dostępie do informacji publicznej

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu prowadzenia spraw związanych z udzielaniem odpowiedzi na wniosek o udzielenie informacji publicznej.

Podstawą pozyskania i przetwarzania przez Administratora Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO. Oznacza to, że Pani/Pana dane osobowe będą przetwarzane, kiedy przetwarzanie będzie niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze. Obowiązki te wynikają z ustawy o dostępie do informacji publicznej oraz z Kodeksu Postępowania Administracyjnego.

4. Okres przetwarzania danych

Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celów przetwarzania oraz przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych Administratora, tj. 10 lat.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. usługi informatyczne, usługi archiwizacji i niszczenia dokumentów, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu np.: Poczta Polska.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;
b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;
c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter dobrowolny. Zasady ich pozyskania są uregulowane w/w przepisach.

KI-7

Informacja dot. przetwarzania danych osobowych osób biorących udział w rekrutacji na stanowisko pracy

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu prowadzenia rekrutacji na stanowisko pracy w Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. a oraz art. 9 ust. 2 lit. a RODO (zgoda pracownika na przetwarzanie danych wykraczających poza wymagane przepisami prawa),
- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą),
- art. 6 ust. 1 lit. c (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) w związku z ustawą z dnia 26 czerwca 1974 r. - Kodeks pracy oraz w związku z ustawami sektorowymi, regulującymi wymagania wobec kandydata na określone stanowisko pracy.

4. Okres przetwarzania danych

Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celów przetwarzania oraz przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych Administratora.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. podmioty świadczące usługi IT, audytorskie, usługi archiwizacji i niszczenia dokumentacji.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) usunięcia danych osobowych – jeżeli administrator przetwarzałby dane osobowe w sposób niezgodny z prawem, zgodnie z art. 17 RODO.

d) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;
e) wniesienia sprzeciwu wobec przetwarzania danych osobowych – jeżeli osoba które dane dotyczą uważa, że Administrator nie ma prawa przetwarzać jej danych osobowych, może wnieść sprzeciw, zgodnie z art. 21 RODO.
f) wycofania zgody w zakresie danych osobowych wykraczających poza wymagane przepisami prawa. Cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie tych danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

KI-8

Informacja dot. przetwarzania danych osobowych w zakresie prowadzenia akt osobowych pracowników i realizowaniu ustawowych obowiązków związanych z zatrudnieniem

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. **Administrator danych osobowych**

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. **Inspektor ochrony danych**

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. **Cele i podstawy prawne przetwarzania**

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu prowadzenia akt osobowych, a także realizacji czynności związanych z zatrudnieniem w Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. a RODO (zgoda pracownika na przetwarzanie danych wykraczających poza wymagane przepisami prawa),
- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą),
- art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze oraz niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy) m.in. w związku z ustawą z dnia 26 czerwca 1974 r. - Kodeks pracy.

4. **Okres przetwarzania danych**

Dane osobowe będą przetwarzane w formie papierowej oraz elektronicznej przez okres zgodny z zasadami określonymi w art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach – 10 lub 50 lat w zależności od daty rozpoczęcia pracy przez pracownika.

5. **Odbiorcy danych**

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. podmioty świadczące usługi IT, podmiot zapewniający oprogramowanie kadrowo-płacowe, audytorskie, usługi archiwizacji i niszczenia dokumentacji.

6. **Prawa osób, których dane dotyczą:**

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;
c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;
d) wniesienia sprzeciwu wobec przetwarzania danych osobowych – jeżeli osoba które dane dotyczą uważa, że Administrator nie ma prawa przetwarzać jej danych osobowych, może wnieść sprzeciw, zgodnie z art. 21 RODO.
e) wycofania zgody w zakresie danych osobowych wykraczających poza wymagane przepisami prawa. Cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie tych danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

Informacja dot. przetwarzania danych osobowych praktykantów

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu zawarcia i realizacji porozumienia o wykonywaniu świadczeń związanych realizacją praktyk.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. a RODO (zgoda praktykanta na przetwarzanie danych wykraczających poza wymagane przepisami prawa),
- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą),
- art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze oraz niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy) w związku z ustawą z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce.

4. Okres przetwarzania danych

Dane osobowe będą przetwarzane w formie papierowej oraz elektronicznej przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych administratora w zakresie archiwizacji dokumentów, okres przedawnienia roszczeń przysługujących administratorowi i w stosunku do niego.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. usługi informatyczne, audytorskie, usługi archiwizacji, niszczenie, przewożenie i przechowywania dokumentacji.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;
d) wniesienia sprzeciwu wobec przetwarzania danych osobowych – jeżeli osoba które dane dotyczą uważa, że Administrator nie ma prawa przetwarzać jej danych osobowych, może wnieść sprzeciw, zgodnie z art. 21 RODO.
e) wycofania zgody w zakresie danych osobowych wykraczających poza wymagane przepisami prawa. Cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie tych danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

KI-10

Informacja dot. przetwarzania danych osobowych stażystów

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w związku z odbyciem stażu.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. a RODO (zgoda stażysty na przetwarzanie danych wykraczających poza wymagane przepisami prawa np. prywatny numer telefonu lub adres e-mail),
- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą),
- art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) w związku z ustawą z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy.

4. Okres przetwarzania danych

Dane osobowe będą przetwarzane w formie papierowej oraz elektronicznej przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych administratora w zakresie archiwizacji dokumentów, okres przedawnienia roszczeń przysługujących administratorowi i w stosunku do niego.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. usługi informatyczne, audytorskie, usługi archiwizacji, niszczenie, przewożenie i przechowywania dokumentacji.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

d) wniesienia sprzeciwu wobec przetwarzania danych osobowych – jeżeli osoba które dane dotyczą uważa, że Administrator nie ma prawa przetwarzać jej danych osobowych, może wnieść sprzeciw, zgodnie z art. 21 RODO.

e) wycofania zgody w zakresie danych osobowych wykraczających poza wymagane przepisami prawa. Cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie tych danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

KI-11

Informacja dot. przetwarzania danych osobowych wolontariuszy

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. Administrator danych osobowych

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. Cele i podstawy prawne przetwarzania

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w związku z odbyciem wolontariatu.

Pani/Pana dane osobowe są przetwarzane w trybie:

- art. 6 ust. 1 lit. a RODO (zgoda wolontariusza na przetwarzanie danych wykraczających poza wymagane przepisami prawa np. prywatny numer telefonu lub adres e-mail),
- art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą),
- art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) w związku z ustawą z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie.

4. Okres przetwarzania danych

Dane osobowe będą przetwarzane w formie papierowej oraz elektronicznej przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych administratora w zakresie archiwizacji dokumentów, okres przedawnienia roszczeń przysługujących administratorowi i w stosunku do niego.

5. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. usługi informatyczne, audytorskie, usługi archiwizacji, niszczenie, przewożenie i przechowywania dokumentacji.

6. Prawa osób, których dane dotyczą:

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;

b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;

c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

d) wniesienia sprzeciwu wobec przetwarzania danych osobowych – jeżeli osoba które dane dotyczą uważa, że Administrator nie ma prawa przetwarzać jej danych osobowych, może wnieść sprzeciw, zgodnie z art. 21 RODO.

e) wycofania zgody w zakresie danych osobowych wykraczających poza wymagane przepisami prawa. Cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie tych danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie.

KI-12

Informacja dot. przetwarzania danych osobowych osób składających skargi, wniosku lub podania (i inne) w trybie ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. **Administrator danych osobowych**

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. **Inspektor ochrony danych**

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. **Cele i podstawy prawne przetwarzania**

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w celu rozpatrzenia wniosku, skargi, podania (i innych) złożonych w trybie ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

Pani/Pana dane osobowe są przetwarzane w trybie art. 6 ust. 1 lit. c RODO - oznacza to, że Pani/Pana dane osobowe będą przetwarzane, kiedy przetwarzanie będzie niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze. Obowiązki te wynikają z ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego

4. **Okres przetwarzania danych**

Dane osobowe będą przetwarzane w formie papierowej oraz elektronicznej przez okres przewidziany przepisami prawa w tym zakresie, w tym przez okres przechowywania dokumentacji określony w przepisach powszechnych i uregulowaniach wewnętrznych administratora w zakresie archiwizacji dokumentów, okres przedawnienia roszczeń przysługujących administratorowi i w stosunku do niego.

5. **Odbiorcy danych**

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. obsługa informatyczna systemu elektronicznego obiegu dokumentów, jak również inni administratorzy danych osobowych, przetwarzający dane we własnym imieniu np.: Poczta Polska lub obsługa prawna.

6. **Prawa osób, których dane dotyczą:**

Zgodnie z RODO przysługuje Pani/Panu:

a) prawo dostępu do swoich danych osobowych oraz otrzymania ich kopii – każda osoba, której dane przetwarzamy jest uprawniona do uzyskania informacji o swoich danych osobowych zgodnie z art. 15 RODO;
b) prawo do sprostowania (poprawiania) swoich danych osobowych – w przypadku, gdy dane osobowe przetwarzane przez Administratora są nieprawidłowe lub niekompletne to każda osoba, której dane dotyczą może żądać odpowiednio ich poprawienia lub uzupełnienia zgodnie z art. 16 RODO;
c) ograniczenia przetwarzania danych osobowych – z ważnych przyczyn, np.: kwestionowanie legalności przetwarzania danych osobowych, zgodnie z art. 18 RODO;

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. Informacja o wymogu/dobrowolności podania danych osobowych

Podanie przez Panią/Pana danych osobowych ma charakter obligatoryjny. Zasady ich pozyskania są uregulowane w w/w przepisach.

Załącznik nr 2

do Procedury realizacji obowiązków informacyjnych

Informacja dot. przetwarzania danych osobowych w celu .....

Zgodnie z art. 13 ust. 1 i ust. 2 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, dalej jako RODO) (Dz. U. UE. L. z 2016 r. Nr 119, z późn. zm.), informujemy, iż:

1. **Administrator danych osobowych**

Administratorem państwa danych osobowych jest Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28, reprezentowane przez Dyrektora. Z Administratorem może się Pani/Pan skontaktować poprzez adres e-mail: muzeum@rewal.pl telefonicznie: tel. +48 91 38 63 250 lub pisemnie na adres korespondencyjny Muzeum.

2. **Inspektor ochrony danych**

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania swoich danych osobowych pod adresem e-mail: muzeum@rewal.pl lub pisemnie na adres naszej siedziby, wskazany w ust. 1.

3. **Cele i podstawy prawne przetwarzania**

Jako Administrator będziemy przetwarzać Pani/Pana dane osobowe w związku z .....

Pani/Pana dane osobowe są przetwarzane w trybie .....

4. **Okres przetwarzania danych**

Dane osobowe będą przetwarzane w formie .....

5. **Odbiorcy danych**

Pani/Pana dane osobowe mogą być udostępniane innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa.

Do Pani/Pana danych mogą też mieć dostęp podmioty przetwarzające dane w imieniu Administratora, np. .....

6. **Prawa osób, których dane dotyczą:**

Zgodnie z RODO przysługuje Pani/Panu:

a) .....
b) .....
c) .....

Jeżeli chce Pani/Pan skorzystać z któregokolwiek z tych uprawnień prosimy o kontakt z Inspektorem Ochrony Danych, który został wskazany w ust. 2 lub pisemnie na adres korespondencyjny, wskazany w ust. 1.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Panu danych osobowych. Organem właściwym dla ww. skargi jest: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

7. **Informacja o wymogu/dobrowolności podania danych osobowych**

Podanie przez Panią/Pana danych osobowych ma charakter .....

Załącznik Nr 6
do Polityki Ochrony Danych Osobowych

INSTRUKCJA REALIZACJI PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE, WSKAZANYCH W ART. 15 – 21 RODO

1. ZASADY OGÓLNE

1. Niniejsza instrukcja zawiera opis zasad stosowanych przez pracowników i współpracowników Przedszkola w celu zapewnienia realizacji praw osób, których dane osobowe przetwarza Przedszkole jako ADO, wskazanych w art. 15 – 21 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) – dalej RODO.
2. ADO ma obowiązek reagowania na wszelkie żądania osób w zakresie ich praw, określonych w art. 15- 22 RODO.
3. ADO rozpatruje żądania osób, których dane dotyczą (podmiotu danych), z należytą starannością, uwzględniając stosowane przepisy prawa oraz prawa i wolności innych osób, których dane mogą dotyczyć.
4. W przypadku braku możliwości identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa przetwarzanych danych osobowych, ADO może zażądać dodatkowych danych potwierdzających tożsamość wnoszącego.
5. Realizacja praw podmiotu danych nie może naruszać praw osób trzecich, w tym celu ADO zapewnia środki ochrony praw tych osób. Przede wszystkim zabronione jest podejmowanie przy realizacji uprawnień podmiotu danych takich działań, w efekcie których dojdzie do nieuprawnionego ujawnienia danych osób trzecich.
6. ADO jest obowiązany odpowiadać na żądania podmiotów danych i przekazać takim osobom informacje o podjętych w związku z takim żądaniem działaniach niezwłocznie, nie później jednak niż w terminie miesiąca od otrzymania żądania.
7. Jeżeli w związku z żądaniem podmiotu danych nie są podejmowane żadne działania, ADO informuje podmiot danych, że działania nie zostaną podjęte, wyjaśnia z jakiego powodu, a także poucza o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
8. ADO jest obowiązany podejmować działania w związku z żądaniami podmiotów danych nieodpłatnie.
9. Pobranie opłaty w rozsądnej wysokości za realizację żądania podmiotu danych jest możliwe jedynie wtedy, gdy żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. W takim przypadku na ADO ciąży obowiązek wykazania tych okoliczności.

2. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ (art. 15 – 21 RODO)

Każda osoba, której dane dotyczą, jest uprawniona do wniesienia do ADO żądania o zrealizowanie praw, o których mowa w art. 15 – 21 RODO, tj.:

1) prawo dostępu do danych – art. 15 RODO,
2) prawo do sprostowania danych – art. 16 RODO,
3) prawo do usunięcia danych („prawo do bycia zapomnianym") – art. 17 RODO,
4) prawo do ograniczenia przetwarzania – art. 18 RODO,

5) prawo do przenoszenia danych – art. 20 RODO,
6) prawo do sprzeciwu wobec przetwarzania danych osobowych – art. 21 RODO.

1. Prawo dostępu do danych zgodnie z art. 15 RODO

1) osoba, której dane dotyczą, ma prawo uzyskać od ADO informację, czy przetwarza on dane jej dotyczące, a w przypadku zaistnienia takiego przetwarzania osoba ta ma prawo dostępu do swoich danych oraz uzyskania informacji obejmujących:
   a) cele przetwarzania,
   b) kategorie zebranych danych osobowych,
   c) wyszczególnienie odbiorców, którym zostaną lub zostały ujawnione dane osobowe,
   d) planowany okres przechowywania danych lub kryteria ustalania tego okresu,
   e) poinformowanie o prawie do sprostowania danych, usunięcia danych lub ograniczenia przetwarzania, prawie do wniesienia sprzeciwu wobec przetwarzania,
   f) prawie do wniesienia skargi do organu nadzorczego,
   g) źródła danych, jeśli dane pochodzą z innego źródła niż od osoby, której dane dotyczą,
   h) poinformowanie o występowaniu zautomatyzowanego podejmowania decyzji, w tym profilowania, a także znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
   i) przekazanie informacji o odpowiednich zabezpieczeniach związanych z przekazaniem, jeśli dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej.
2) prawo dostępu do danych obejmuje wszystkie dane które dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, łącznie z danymi zaobserwowanymi i wywnioskowanymi na jej temat,
3) jeżeli ADO przetwarza duże ilości informacji o osobie, której dane dotyczą, przed podaniem informacji, może żądać, aby osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie (motyw 63 RODO),
4) jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny (motyw 61 RODO).
5) żądanie realizacji praw dotyczy także danych zarchiwizowanych już przez ADO,
6) podmiot danych ma także prawo do uzyskania kopii danych,
7) prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji,
8) ADO dostarcza osobie, której dane dotyczą kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, ADO może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych,
9) jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.

2. Prawo do sprostowania danych zgodnie z art. 16 RODO

1) osoba, której dane dotyczą może wnieść do ADO żądanie dotyczące niezwłocznego sprostowania danych jej dotyczących, jeśli stwierdzi, że dane są nieprawidłowe,
2) podmiot danych może także wnieść (np. w formie dodatkowego oświadczenia) żądanie uzupełnienia danych, jeśli uzna, że są niekompletne,
3) uzupełnienie danych nie może obejmować danych, które byłyby nadmierne, tj. takich, które nie spełniałyby przesłanki niezbędności – stanowiłoby to naruszenie zasady minimalizacji danych.

Przedmiotem uzupełnienia nie mogą być też dane, które są nieprawidłowe. Należy weryfikować czy realizacja prawa z art. 16 RODO nie naruszy innych zasad wskazanych w art. 5 RODO,

4) ADO ma obowiązek poinformować o sprostowaniu danych osobowych, którego dokonał w ramach żądania podmiotu danych, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda,
5) „ujawnienie" danych należy rozumieć szeroko jako jakąkolwiek możliwość zapoznania się z danymi osobowymi. ADO ma obowiązek informować osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda. W związku z czym należy określić i udokumentować krąg odbiorców danych.

3. Prawo do usunięcia danych („prawo do bycia zapomnianym") zgodnie z art. 17 RODO

1) osoba, której dane dotyczą ma prawo wniesienia do ADO żądania usunięcia dotyczących jej danych osobowych, jeśli zachodzi jedna z poniższych okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na mocy art. 21 ust. 1 lub ust. 2 RODO,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega ADO.
2) jeśli ADO upublicznił dane osobowe osoby wnoszącej o usunięcie danych, ma on obowiązek – uwzględniając dostępną technologię oraz koszt realizacji – podjąć działania w celu poinformowania innych administratorów przetwarzających te dane osobowe o fakcie, że osoba, której dane dotyczą, złożyła żądanie o usunięcie przez tych administratorów wszelkich łącz do tych danych, kopie danych lub ich replikacje (powielenia),
3) ADO niezwłocznie realizuje prawo osoby do usunięcia danych, chyba że zaistnieje jedna z poniżej wyszczególnionych przesłanek:
   a) przetwarzanie danych osobowych jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji,
   b) przetwarzanie danych osobowych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega ADO,
   c) przetwarzanie danych osobowych jest niezbędne do celów archiwalnych w interesie publicznym, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
   d) przetwarzanie danych osobowych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
4) ADO informuje o usunięciu danych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

4. Prawo do ograniczenia przetwarzania zgodnie z art. 18 RODO

1) osoba, której dane dotyczą może wnieść do ADO żądanie o ograniczenie przetwarzania dotyczących jej danych osobowych w następujących przypadkach:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO sprawdzić prawidłowość tych danych,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c) ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2) jeżeli przetwarzanie zostało ograniczone, to dane osobowe można przetwarzać, z wyjątkiem przechowywania:
a) wyłącznie za zgodą osoby, której dane dotyczą,
b) w celu ustalenia, dochodzenia lub obrony roszczeń,
c) w celu ochrony praw innej osoby fizycznej lub prawnej,
d) z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

3) przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

5. Prawo do przenoszenia danych zgodnie z art. 20 RODO

1) osoba, której dane dotyczą, jest uprawniona do wniesienia żądania przeniesienia danych jej dotyczących,
2) prawo do przenoszenia danych przysługuje wyłącznie, gdy:
a) przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych osobowych w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.
3) osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym (np. .csv), powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące,
4) wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe,
5) wykonanie prawa do przeniesienia danych nie wyklucza wniesienia żądania o usunięcie danych osobowych,
6) prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych,
7) należy zdefiniować zakres danych dostarczonych ADO, które podlegać będą przekazaniu,
8) dane wywnioskowane i wywiedzione przez ADO z danych przekazanych przez podmiot danych nie wchodzą w zakres prawa do przenoszenia danych.

6. Prawo do sprzeciwu zgodnie z art. 21 RODO

1) osoba, której dane dotyczą, może w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych, jeśli przetwarzanie jest oparte na art. 6 ust. 1 lit. f) RODO (prawnie uzasadnione interesy realizowane przez ADO),
2) do czasu rozpatrzenia sprzeciwu, nawet jeżeli nie zgłoszono żądania ograniczenia przetwarzania, należy rozważyć taką możliwość i konieczność,
3) ADO nie może przetwarzać danych osobowych względem, których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych postaw do przetwarzania danych, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. ZASADY REALIZACJI PRAW

1. Sposób składania wniosków o realizację praw

1) w celu zapewnienia udostępnienia danych jedynie osobom, których dane dotyczą dopuszcza się trzy kanały komunikacji:
   a) elektroniczny – poprzez adres mailowy służący do kontaktu z ADO lub poprzez adres mailowy IOD,
   b) tradycyjny – w formie papierowej opatrzony własnoręcznym podpisem,
   c) ustnie (nie dotyczy kontaktu telefonicznego) – należy taką osobę wylegitymować w celu potwierdzenia tożsamości i sporządzić notatkę z podpisem wnioskodawcy. Notatka winna być włączona w akta sprawy.
2) osoba, której dane dotyczą, składa do ADO wniosek o realizację prawa w formie pisemnej lub elektronicznej z uwzględnieniem wymogów dotyczących korespondencji, tj.:
   a) wskazania imienia, nazwiska wnioskodawcy,
   b) adresu lub innego kanału komunikacji,
   c) innych danych umożliwiających bezsprzeczną identyfikację tożsamości osoby, której dane dotyczą.
3) w związku z wyznaczeniem przez ADO Inspektora Ochrony Danych (IOD), który pełni rolę punktu kontaktowego dla osób, których dane dotyczą, osoby te mogą kontaktować się bezpośrednio z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

2. Obsługa wniosków

1) każdy wniosek o realizację praw osób wpływający do ADO musi zostać zarejestrowany.
2) ADO przekazuje wniosek do IOD, który koordynuje jego realizację i wykonuje czynności konsultacyjne,
3) po otrzymaniu żądania IOD:
   a) rejestruje wniosek w prowadzonym rejestrze wniosków o realizację praw podmiotów (zgodnie z załącznikiem do niniejszej instrukcji),
   b) weryfikuje rodzaj żądania i w razie wątpliwości prosi osobę żądającą o podanie dodatkowych informacji umożliwiających sprecyzowanie żądania,
   c) ustala w ramach jakiej kategorii podmiotów (np. kandydaci do pracy, pracownicy, byli pracownicy, klienci) należy identyfikować zgłaszającego,
   d) ustala w ramach, których procesów przetwarzania danych (wskazanych w rejestrze czynności) dane zgłaszającego (tej kategorii podmiotów) mogą być przetwarzane (może to być jeden lub więcej procesów przetwarzania danych).
4) w przypadku braku możliwości zidentyfikowania osoby, której dane dotyczą, w miarę możliwości ADO informuje o tym wnioskodawcę. W takich przypadkach zastosowania nie mają art. 15–20 RODO, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować,
5) obowiązuje zakaz przekazywania informacji zwrotnej przed zweryfikowaniem tożsamości. Prosząc o dodatkowe dane np. w celu sprecyzowania żądania, w celu identyfikacji lub weryfikacji tożsamości należy wyraźnie poinformować osobę żądającą o celu pozyskania tych dodatkowych informacji (można wyznaczyć dodatkowy termin na ich przekazanie oraz wskazać, że bez tych informacji realizacji praw w całości lub w części nie będzie możliwa),
6) przy realizacji praw podmiotu należy przestrzegać zasad ogólnych RODO, w tym w zakresie minimalizacji danych a także reguł bezpieczeństwa np. przekazując kopie danych,

7) weryfikacja tożsamości nie może prowadzić do gromadzenia danych w sposób nadmierny i powinna być adekwatna do poziomu ryzyka,
8) należy zawsze weryfikować podstawę umocowania, gdy osoba żądająca wskazuje, że działa w imieniu innego podmiotu,
9) sprawdzeniu podlega możliwość zrealizowania żądania, w tym czy nie zachodzą przesłanki wyłączające możliwość realizacji żądania, ewentualnie przesłanki pobrania opłaty (w tym zakresie należy uwzględnić wymogi wskazane w ust. 2 opisujące poszczególne żądania), czas oraz środki potrzebne na realizację żądania, a także kto będzie odpowiedzialny za techniczną obsługę żądania,
10) jeżeli żądanie jest zasadne należy przekazać odpowiedź podmiotowi, który wniósł żądanie, wskazując sposób realizacji żądania,
11) decyzję dotyczącą sposobu realizacji wniosku podejmuje ADO,
12) sposób realizacji żądania należy odnotować w rejestrze wniosków o realizację praw podmiotów.

3. Termin realizacji żądań

1) ADO bez zbędnej zwłoki – nie później niż w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO,
2) w razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań,
3) w terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy,
4) jeżeli ADO nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa UODO oraz skorzystania ze środków ochrony prawnej przed sądem.

4. Sposób realizacji odpowiedzi

1) odpowiadając na żądanie należy uwzględnić sposób zgłoszenia żądania,
2) jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy,
3) jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną (art. 15 ust. 3 RODO).
4) informacje powinny być przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Załącznik Nr 1

do Instrukcji realizacji praw osób, których dane są przetwarzane

REJESTR WNIOSKÓW O REALIZACJĘ PRAW PODMIOTÓW

Imię i nazwisko	Telefon	Adres	e-mail	Treść żądania	Określenie typu żądania (usunięcie, sprzeciw itp.)	Data wpływu żądania	Kanał wpływu żądania	Data realizacji żądania	Sposób realizacji żądania	Oznaczenie kategorii podmiotu	Dane, które posłużyły weryfikacji podmiotu	Oznaczenie systemu, w którym dane są przetwarzane	Data przekazania żądania procesorowi	Osoba realizująca żądanie

Załącznik Nr 7
do Polityki ochrony danych osobowych

ANKIETA OCENY PODMIOTU PRZETWARZAJĄCEGO (WYKONAWCY)

Podstawa prawna art. 28 ust. 1 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 (dalej zwane: RODO)

Uprzejmie prosimy o wyczerpujące wypełnienie poniższej ankiety. Ankieta jest przeprowadzana w związku z podejmowaną przez Państwa współpracą z Administratorem i ma na celu ocenić stopień zabezpieczenia danych osobowych, których przekazanie Państwu jest niezbędne do realizacji umowy pomiędzy Stronami.

W kwestionariuszu znajdują się pytania zamknięte, na które odpowiedzi należy udzielić zaznaczając TAK lub NIE. Na pytania otwarte należy udzielić odpowiedzi we wskazanych polach.

W razie pytań prosimy o kontakt z Administratorem.

Nazwa Wykonawcy:	
Adres Wykonawcy:	
Kontakt Wykonawcy:	
Data wypełnienia ankiety przez Wykonawcę	

I. Ocena zasobów

Lp.		Tak	Nie	RODO
1	Czy podmiot przetwarzający opracował i wdrożył **politykę ochrony danych** lub podobną procedurę?			art. 24
2	Czy podmiot przetwarzających wdrożył instrukcję/procedurę postępowania w sytuacji naruszenia ochrony danych osobowych?			
3	Czy podmiot przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych (jako ADO)?			art. 30

4	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora?			art. 30
5	Czy podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania pod kątem ryzyka ochrony prywatności)?			odniesienie do art. 24, 25 i 32
6	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania?			
7	Czy podmiot przetwarzający okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?			
8	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:			art. 32 ust. 1 lit. a-c
a) pseudonimizację i szyfrowanie danych,				
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,				
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.				
9	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? Jeśli tak, kiedy przeprowadzono ostatni audyt? Odpowiedź:			art. 32 ust. 1 lit. d
12	Czy osoby delegowane do obsługi ADO posiadają nadane upoważnienia do przetwarzania danych?			
13	Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały obowiązane do zachowania ich w tajemnicy?			

14	Czy dokonywany jest transfer przetwarzanych danych do państw poza EOG?			
15	Jeżeli tak, to czy zapewniony jest mechanizm legalizujący taki transfer?			art. 44-48

II. Ocena wiedzy fachowej

Lp.		Tak	Nie	RODO
1	Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył inspektora ochrony danych?			art. 37
2	Czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych?			art. 37
3	Czy osoby po stronie podmiotu przetwarzającego dedykowane do obsługi administratora zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane? Jeśli tak, kiedy przeprowadzono ostatnie szkolenie? Odpowiedź:			

III. Ocena wiarygodności

Lp.		Tak	Nie	RODO
2	Czy w przeciągu ostatnich 6 miesięcy doszło do naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia organowi nadzorczemu?			
3	Czy stwierdzono prawomocną decyzją GIODO/UODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?			

Data i podpis Podmiotu Przetwarzającego

Załącznik Nr 8
do Polityki Ochrony Danych Osobowych

WZÓR UMOWY
przetwarzania danych osobowych w imieniu administratora
zawarta w Warszawie w dniu ..... r. pomiędzy:
(zwana dalej: ***Umową***)

....., reprezentowany przez ..... -
zwaną dalej ***„Administratorem"***

oraz
..... z siedzibą w ....., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez ....., pod numerem KRS: ....., posiadającą NIP: ....., REGON: ....., reprezentowaną przez ..... – .....
/
Panią/Panem ....., prowadzącą/ym działalność gospodarczą w ..... przy ul. ....., pod nazwą ....., wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej, posiadającym/ą NIP: ....., REGON: .....

zwanym w dalszej części Umowy ***Podmiotem Przetwarzającym***

Preambuła lub bez preambuły

Mając na uwadze, że:

1. Strony zawarły Umowę nr ..... z dnia ..... (Umowa Podstawowa), w związku z wykonywaniem której Podmiot Przetwarzający będzie wykonywał operacje przetwarzania danych osobowych w imieniu Administratora w zakresie określonym Umową.
2. Celem Umowy jest ustalenie warunków, na jakich Podmiot Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora.
3. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom 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) – dalej „Rozporządzenie",

Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1
Przetwarzanie danych osobowych w imieniu administratora

1. Na podstawie art. 28 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 (zwanego w dalszej części ***Rozporządzeniem***) Podmiot Przetwarzający będzie dokonywał w imieniu Administratora przetwarzania danych osobowych na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot Przetwarzający zobowiązuje się przetwarzać dane osobowe zgodnie z Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującymi, które chronią prawa osób, których dane dotyczą.

3. Podmiot Przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia oraz innych przepisów, o których mowa w ust. 2.

§2

Zakres i cel przetwarzania danych

1. Podmiot Przetwarzający będzie przetwarzał następujący rodzaj danych osobowych ....., który dotyczy .....
2. Dane osobowe będą przetwarzane przez Podmiot Przetwarzający w celu realizacji ...../ Umowy Podstawowej.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot Przetwarzający zobowiązuje się, przy przetwarzaniu danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu danych osobowych.
3. Podmiot Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały dane w celu realizacji Umowy.
4. Podmiot Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust 3 lit. b Rozporządzenia, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie Przetwarzającym, jak i po jego ustaniu.
5. Podmiot Przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie w ciągu .... dni, chyba że przepisy powszechnie obowiązującego prawa nakazują przechowywanie danych osobowych. Po wykonaniu zobowiązania, o którym mowa w zdaniu poprzedzającym, Podmiot Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich danych.
6. W miarę możliwości Podmiot Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin od chwili uzyskania informacji o potencjalnym naruszeniu, oraz umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu faktycznego naruszenia.
8. Planując dokonanie zmian w sposobie przetwarzania danych, Podmiot Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 Rozporządzenia i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Podmiot Przetwarzający zmiany w opinii Administratora grożą bezpieczeństwu danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Podmiot Przetwarzający.

§4

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot Przetwarzający przy przetwarzaniu i zabezpieczeniu danych osobowych spełniają postanowienia Umowy i Rozporządzenia.

2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu Przetwarzającego i z minimum ..... dniowym uprzedzeniem.
3. Podmiot Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora, nie dłuższym niż 7 dni.
4. Podmiot Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Przetwarzanie danych w imieniu administratora przez inny podmiot przetwarzający

1. Podmiot Przetwarzający może korzystać do wykonania w imieniu Administratora konkretnych czynności przetwarzania z usług innego podmiotu przetwarzającego po uzyskaniu uprzedniej pisemnej zgody Administratora. Zgoda Administratora musi mieć formę pisemną pod rygorem nieważności.
2. W przypadku, gdy Podmiot Przetwarzający do wykonania konkretnych czynności przetwarzania korzysta z usług innych podmiotów przetwarzających (tzw. Podprocesorów), zobowiązany jest on do wypełnienia wykazu, stanowiącego Załącznik nr 1 do niniejszej umowy.
   Po analizie przeprowadzonej przez Administratora, wykaz podlegać będzie akceptacji.
3. Przekazanie danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot Przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. 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.
4. Jeżeli do wykonywania w imieniu Administratora konkretnych czynności przetwarzania Podmiot Przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone są te same wymogi i obowiązki ochrony danych, jakie zostały nałożone na Podmiot Przetwarzający w niniejszej Umowie, w szczególności w zakresie gwarancji ochrony przetwarzania danych osobowych.
5. Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na innym podmiocie przetwarzającym obowiązku ochrony danych.

§ 6

Odpowiedzialność Podmiotu Przetwarzającego

1. Podmiot Przetwarzający jest odpowiedzialny za przetwarzanie danych osobowych niezgodnie z treścią Umowy, przepisami Rozporządzenia lub innymi przepisami, o których mowa w § 1 ust. 2, a w szczególności za udostępnienie do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot Przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu Przetwarzającego, a także o wszelkich planowanych, ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie Przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia ..... do .....
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... okresu wypowiedzenia.

§8

Rozwiązanie umowy

Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, w przypadku gdy Podmiot Przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z Umową, Rozporządzeniem lub innymi przepisami, o których mowa w § 1 ust. 2;
c) korzystał z usług innego podmiotu przetwarzającego bez uprzedniej zgody Administratora.

§9

Zasady zachowania poufności

1. Podmiot Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej (dalej: ***Dane Poufne***)
2. Podmiot Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy Danych Poufnych nie będą one wykorzystywane, ujawniane ani udostępniane, bez pisemnej zgody Administratora, w innym celu, niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, Rozporządzenia oraz inne przepisy prawa, o których mowa w § 1 ust. 2.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd powszechny właściwy miejscowo dla Administratora.
4. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

Administrator	Podmiot Przetwarzający

Załącznik nr 1 do Umowy przetwarzania danych osobowych w imieniu Administratora

WYKAZ PODMIOTÓW, Z KTÓRYCH KORZYSTA PODMIOT PRZETWARZAJĄCYCH (TZW. PODPROCESORÓW)

Nazwa i adres podmiotu	Zakres czynności

_____
Administrator

_____
Podmiot Przetwarzający

REJESTR UMÓW PRZETWARZANIA DANYCH OSOBOWYCH W IMIENIU ADMINISTRATORA

****Rejestr stworzony jest w związku z art. 24 oraz art. 32 RODO[1] i stanowi wykaz umów zawartych w trybie art. 28 RODO.***

LP	DANE PODMIOTU	CEL	DATA ZAWARCIA UMOWY	KATEGORIE OSÓB POWIERZONYCH DANYCH OSOBOWYCH	CZAS OBOWIĄZYWANIA UMOWY	LOKALIZACJA DOKUMENTU	STATUS UMOWY
1							
2							
3							
4							
5							
6							

[1] 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).

7							
8							

.....

(PIECZĄTKA I PODPIS ADMINISTRATORA)

Załącznik Nr 1
do Instrukcji postępowania
w sytuacji powstania incydentów
naruszenia ochrony danych osobowych

Przykłady zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania	
		Użytkownik	IOD
I Formy naruszenia danych osobowych przez użytkownika zatrudnionego przy przetwarzaniu danych			
1	W zakresie wiedzy		
a)	Ujawnienie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD	Sporządzić raport z opisem, jaka informacja została ujawniona.
b)	Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD	Sporządzić raport z opisem, jaka informacja została ujawniona
c)	Dopuszczenie i stwarzanie warunków, aby ktokolwiek mógł pozyskać informację o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji	Natychmiast przerwać czynność prowadzącą do ujawnienia informacji. Powiadomić IOD	Sporządzić raport z opisem, jaka informacja została ujawniona
d)	Wysłanie wiadomości e-mail do wielu odbiorców bez zastosowania kopii ukrytej (Nie dotyczy korespondencji wewnętrznej włączając w to departament)	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
2	W zakresie sprzętu i oprogramowania		
a)	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Pouczyć osobę, która dopuściła do takiej sytuacji. Przekazać informacje do IOD	Przyjąć informację, sporządzić raport
b)	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła się do takiej sytuacji. Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
c)	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym,	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD	Sporządzić raport

	zapisanego hasła dostępu do bazy danych osobowych i sieci		
d)	Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport
e)	Kradzież nośnika danych (np. pendrive)	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
f)	Kradzież urządzenia (np. laptop, komputer)	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
g)	Przekazanie do serwisu sprzętu z niezabezpieczonymi danymi	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
h)	Włamanie na skrzynkę mailową	Niezwłocznie powiadomić IOD i ASI	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport
i)	Uruchomienie szkodliwego oprogramowania szyfrującego dane	Natychmiastowe wyłączenie komputera. Niezwłocznie powiadomić IOD i ASI	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport
j)	Podszycie się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań	Natychmiastowe wyłączenie komputera. Niezwłocznie powiadomić IOD i ASI	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport
k)	Zgubienie klucza do pokoju, w którym są przetwarzane dane osobowe	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
3	W zakresie dokumentów zawierających dane osobowe		
a)	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
b)	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	Zabezpieczyć niewłaściwie zniszczone dokumenty. Sporządzić raport. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
c)	Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane – sporządzić raport. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
d)	Kradzież lub zgubienie dokumentów zawierających dane osobowe	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
e)	Błędnie wysłana korespondencja drogą mailową	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
f)	Błędnie wysłana korespondencja drogą tradycyjną	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport

g)	Przekazanie danych usługodawcy bez odpowiedniej umowy lub innego instrumentu prawnego	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
h)	Przewożenie dokumentów zawierających dane osobowe bez właściwego zabezpieczenia tych danych	Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
4	W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych		
a)	Pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych	Zabezpieczyć (zamknąć) pomieszczenie. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
b)	Pozostawienie otwartych okien, drzwi po zakończeniu pracy	Zabezpieczyć (zamknąć) pomieszczenie. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
c)	Pozostawienie dokumentów w koszu na śmieci	Zabezpieczyć dokumenty. Przekazać informację do IOD	Przyjąć informację, sporządzić raport
d)	Pożar, zalanie	Podjąć próbę odzyskania dokumentacji i sprzętu. Powiadomić IOD	Przyjąć informację, sporządzić raport
II	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych		
1	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie IOD lub ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji	Przyjąć informację, sporządzić raport
2	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD	Przyjąć informację, sporządzić raport
3	Przechowywanie haseł w niewłaściwy sposób	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
4	Przekazywanie haseł innym osobom	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Przyjąć informację, sporządzić raport
5	Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport
6	Nieuprawniona zmiana danych lub ich uszkodzenie	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Wezwać ASI w celu przywrócenia stanu pierwotnego. Sporządzić raport

7	Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji	Powiadomić o zaistniałej sytuacji ASI. Przyjąć informację, sporządzić raport
8	Kradzież sprzętu przetwarzającego informacje	Niezwłocznie powiadomić IOD oraz ASI	Powiadomić o zaistniałej sytuacji ASI. Przyjąć informację, sporządzić raport

Załącznik Nr 2
do Instrukcji postępowania
w sytuacji powstania incydentów
naruszenia ochrony danych osobowych

Raport z zagrożenia bezpieczeństwa danych osobowych

Sporządzający raport:

Imię i nazwisko	
Stanowisko	

1. Miejsce, dokładny czas i data stwierdzenia zagrożenia ochrony danych osobowych (piętro, nr pokoju, itp.):
.....
.....
.....

2. Osoby powodujące naruszenie, które swoim działaniem lub zaniechaniem przyczyniły się do zagrożenia ochrony danych osobowych:
.....
.....
.....

3. Osoby, które uczestniczyły w zdarzeniu związanym z zagrożeniem ochrony danych osobowych:
.....
.....
.....

4. Informacje o danych, które mogły zostać ujawnione:
.....
.....
.....

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
.....
.....
.....

6. Krótki opis wydarzenia związanego z zagrożeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania zapobiegawcze):
.....
.....
.....

.....
(data i podpis)

Załącznik Nr 3
do Instrukcji postępowania
w sytuacji powstania incydentów
naruszenia ochrony danych osobowych

Raport z incydentu naruszającego bezpieczeństwa danych osobowych ze względu na poufność, dostępność i integralność

Sporządzający raport:

Imię i nazwisko	
Stanowisko	

7. Miejsce, dokładny czas i data stwierdzenia incydentu naruszającego bezpieczeństwa danych osobowych (nr pokoju, itp.):

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

8. Osoby powodujące naruszenie, które swoim działaniem lub zaniechaniem przyczyniły się do incydentu naruszającego bezpieczeństwa danych osobowych:

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

9. Osoby, które uczestniczyły w incydencie naruszającym bezpieczeństwo danych osobowych:

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

10. Informacje o danych, które mogły zostać ujawnione:

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

11. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

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

12. Krótki opis wydarzenia związanego z incydentem naruszającym bezpieczeństwo danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania zapobiegawcze):

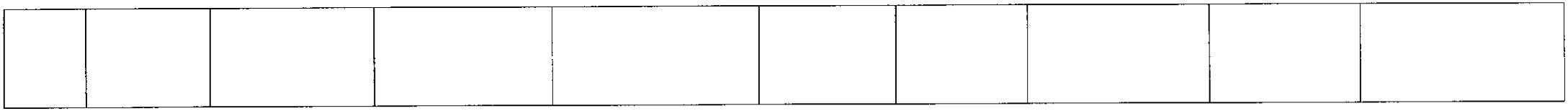
.....

.....
(data i podpis)

Załącznik **Nr 4**
do Instrukcji postępowania
w sytuacji powstania incydentów
naruszenia ochrony danych osobowych

Rejestr incydentów i zagrożeń

Nr raportu zagrożenia /incydentu	Kod formy naruszenia	Użytkownik		Podjęte działania			Wyniki podjętych działań	Data zamknięcia zagrożenia /incydentu	Uwagi
		Zgłaszający	Powodujący naruszenia	Zapobiegawcze	Korekcyjne	Korygujące			
1	2	3	4	5	6	7	8	9	10



Załącznik Nr 5
do Instrukcji postępowania
w sytuacji powstania incydentów
naruszenia ochrony danych osobowych

METODA OCENY WAGI NARUSZENIA

W celu określenia czy naruszenie wymaga zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych wykorzystuje się metodę oceny wagi naruszenia wg. Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[1].

Wzór: WN=KPD*PI+ON, gdzie:

- **WN – Waga Naruszenia**
- **KPD – Kontekst Przetwarzania Danych** - główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania
- **PI- Prawdopodobieństwo Identyfikacji** - czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich
- **ON – Okoliczności Naruszenia** - czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku

➢ **Kontekst Przetwarzania Danych**

Wzór: KPD=A+B, gdzie:

A – rodzaj i poziom wrażliwości danych:

- Dane podstawowe = 1
- Dane dotyczące zachowań osoby = 2
- Dane finansowe = 3
- Dane szczególnych kategorii = 4

B- kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę:

- Szeroki zakres danych/wolumen danych (+).
- Charakter danych (+/-).
- Specyfika podmiotu danych lub administratora (+/-).
- Możliwe negatywne skutki dla podmiotu danych (+).
- Publiczna dostępność danych przed naruszeniem (-).
- Nieważność danych (-).

Wartość kontekstu przetwarzania zawiera się w przedziale liczbowym 1-4.

➢ **Prawdopodobieństwo Identyfikacji:**

- Znikome = 0,25.
- Ograniczone = 0,5.
- Wysokie = 0,75.

[1] https://www.enisa.europa.eu/publications/dbn-severity/

- Maksymalne = 1.

➢ **Okoliczności Naruszenia:**

Naruszenie Poufności – Dane ujawnione:

- Znanym odbiorcom (+0,25).
- Nieznanej liczbie odbiorców danych (+0,5).

Naruszenie Integralności – Dane zmienione i:

- Możliwe jest ich odzyskanie (+0,25).
- Brak jest możliwości ich odzyskania (+0,5).

Naruszenie Dostępności – Niedostępność danych:

- Czasowa (+0,25).
- Pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5).

Intencjonalne działanie sprawcy (+0,5)

➢ **Ocena wagi naruszenia:**

Wynik	Waga naruszenia	Opis
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<=WN<3	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=WN<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=WN		Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

Jeżeli tak wyliczona waga naruszenia będzie większa niż niska, należy zgłosić je do UODO. Wskazana metoda ma charakter jedynie pomocniczy. Może się zdarzyć, że pod uwagę przy ocenie wagi naruszenia powinny być wzięte inne, specyficzne dla danego rodzaju przetwarzania/dla Zespołu przesłanki, które będą miały istotny wpływ na tę ocenę. Zgodnie z art. 33 ust. 1 RODO zgłoszenia nie dokonuje się jedynie, kiedy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Załącznik Nr 10
do Polityki Ochrony Danych Osobowych

INSTRUKCJA POSTĘPOWANIA W SYTUACJI POWSTANIA INCYDENTÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 1

Definicje:

a) incydent – naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność,
b) zagrożenie – możliwość wystąpienia incydentu,
c) działanie korekcyjne – działanie przeprowadzone w celu wyeliminowania/usunięcia skutków zidentyfikowanego incydentu,
d) działanie korygujące – działanie przeprowadzone w celu wyeliminowania przyczyny zidentyfikowanego incydentu lub innej niepożądanej sytuacji,
e) działanie zapobiegawcze – działanie przeprowadzone w celu wyeliminowania przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej,
f) kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

§ 2

Celem niniejszej instrukcji jest określenie zadań użytkowników w zakresie:

1. Ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych.
2. Prawidłowego reagowania użytkowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego.
3. Ograniczenia ryzyka powstania zagrożeń oraz minimalizacja skutków wystąpienia zagrożeń.

§ 3

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

- stanu urządzeń technicznych,
- zawartości zbiorów danych osobowych,
- sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
- metod pracy (w tym obiegu dokumentów).

§ 4

1. Każdy użytkownik w przypadku stwierdzenia incydentu zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest bezzwłocznie powiadomić IOD lub ADO.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez użytkowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, szyfrowania plików, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania),
b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata danych),
c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Szerszy katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych stanowi Załącznik Nr 1.

4. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, IOD prowadzi postępowanie wyjaśniające, w toku, którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   c) dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu z zagrożenia bezpieczeństwa danych osobowych (Załącznik Nr 2), podejmuje działania zapobiegawcze.
5. W przypadku stwierdzenia naruszenia bezpieczeństwa danych tj. wystąpienia incydentu, IOD prowadzi postępowanie wyjaśniające, w toku, którego dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu (Załącznik Nr 3) o naruszeniu ochrony danych osobowych wg załączonego wzoru, który zawiera co najmniej:
   a) kod formy naruszenia danych osobowych wg katalogu zagrożeń i incydentów bezpieczeństwa danych osobowych (Załącznik Nr 1),
   b) datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki oraz wielkość szkód, które zaistniały,
   c) zabezpiecza ewentualne dowody winy,
   d) ustala osoby odpowiedzialne za naruszenia,
   e) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   f) rekomenduje działania prewencyjne (korekcyjne, korygujące, zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.
6. IOD sporządza raport i ewidencjonuje zdarzenia niepożądane w rejestrze incydentów i zagrożeń stanowiącym Załącznik Nr 4.

§ 5

1. W wyniku zaistniałych naruszeń i zagrożeń bezpieczeństwa i ochrony danych przeprowadza się działania korekcyjne, korygujące i zapobiegawcze.
2. Działania korekcyjne, korygujące i zapobiegawcze obejmują wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad działaniami korekcyjnymi, korygującymi i zapobiegawczymi jest IOD.

§ 6

1. Obowiązek zgłaszania do IOD incydentów ciąży na każdym użytkowniku.
2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych IOD lub osoba przełożona pracownika/współpracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska użytkownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.

§ 7

1. IOD zobowiązany jest do powiadomienia o zaistniałym incydencie ADO, który podejmuje decyzję o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

2. ADO w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je do UODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Metoda oceny wagi naruszenia stanowi Załącznik Nr 5.

Wykaz załączników:

Załącznik Nr 1 – Przykłady zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych
Załącznik Nr 2 – Raport z zagrożenia bezpieczeństwa danych osobowych
Załącznik Nr 3 – Raport z incydentu naruszającego bezpieczeństwo danych osobowych ze względu na poufność, dostępność i integralność
Załącznik Nr 4 – Rejestr incydentów i zagrożeń
Załącznik Nr 5 – Metoda oceny wagi naruszenia

Załącznik nr 1 do Instrukcji postępowania z kluczami

WZÓR WYKAZU KLUCZY DO DRZWI WEJŚCIOWYCH ORAZ DO POMIESZCZEŃ

BUDYNEK/POMIESZCZENIE	Sekretariat	Indywidualne
Muzeum/drzwi wejściowe	1 komplet	5 kompletów
Muzeum/ biuro Dyrektora	1 komplet	2 komplet
Muzeum/biuro Gł. Księgowego	1 komplet	2 komplet
Muzeum/sale wystawowe	3 komplety	-

Załącznik nr 2 do Instrukcji postępowania z kluczami

WZÓR UPOWAŻNIENIA DO STAŁEGO DYSPONOWANIA KLUCZAMI

Upoważnienie nr .....

Na podstawie Instrukcji postępowania z kluczami powierzam Pani(u) ..... zatrudnionej(mu) na stanowisku ..... komplet kluczy do **Sekretariatu/drzwi wejściowych do budynku*** [NALEŻY WSKAZAĆ].

***skreślić niewłaściwe**

W skład kompletu wchodzą następujące klucze:

1. .....
2. .....
3. .....
4. .....

---------- ----------

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

Oświadczenie pracownika

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

(data i podpis pracownika)

Załącznik nr 3 do Instrukcji postępowania z kluczami

WZÓR UPOWAŻNIENIA DO DORAŹNEGO DYSPONOWANIA KLUCZAMI

Upoważnienie nr .....

Ja niżej podpisany ....., zwracam się z prośbą o udostępnienie kluczy do **Sekretariatu/drzwi wejściowych do budynku*** [NALEŻY WSKAZAĆ].

***skreślić niewłaściwe**

Uzasadnienie wniosku:
.....
.....
.....

(data i podpis Pracownika)

Akceptuję/nie akceptuję

(Dyrektor)

Oświadczenie pracownika

Potwierdzam odbiór w/w kluczy w dniu ..... godz. .....

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem, a także że ponoszę materialną odpowiedzialność za stan budynku/pomieszczeń w czasie posiadania w/w kluczy.

Klucz/e zostanie/ą zdany/e w dniu ..... godz.....

(data i podpis Pracownika)

Oświadczam, że klucz/e został/y zdany/e w dniu .....

....
Pracownik Dyrektor

Załącznik nr 4 do Instrukcji postępowania z kluczami

WZÓR EWIDENCJI OSÓB UPOAWŻNIONYCH DO DYSPONOWANIA KLUCZAMI

NUMER UPOWAŻNIENIA	IMIĘ	NAZWISKO	BUDYNEK/POMIESZCZENIE	DATA WYDANIA	DATA ZDANIA	STAŁE/DORAŹNE
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik Nr 11
do Polityki Ochrony Danych Osobowych

INSTRUKCJA POSTĘPOWANIA Z KLUCZAMI

Słowniczek:
Pomieszczenia – pomieszczenia, w których przetwarzane są dane osobowe.
Drzwi wejściowe – drzwi wejściowe główne do MUZEUM RYBOŁÓWSTWA MORSKIEGO W NIECHORZU

1. Ogólne zasady oraz dostęp do Muzeum:

    1) polityka kluczy obejmuje drzwi wejściowe oraz następujące pomieszczenia:
        a) biuro Dyrektora
        b) biuro Głównego Księgowego
        c) sale wystawowe
    2) dostęp do pomieszczeń możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Drzwi wejściowe umożliwiające dostęp do pomieszczeń powinny być trwale zamknięte na klucz po godzinach pracy.
    3) Klucze do pomieszczeń w Muzeum znajdują się w recepcji.
    4) Klucz do biura znajduje się w skrzynce w recepcji Muzeum.
    5) Klucze do wejścia głównego do Muzeum znajdują się w skrzynce w recepcji.
    6) Klucz do pomieszczenia biurowego Głównej Księgowej znajduje się w skrzynce w recepcji Muzeum.
    7) Klucz do archiwum znajduje się w biurze Głównej Księgowej.
    8) Klucze, o których mowa w pkt. 3-7 pobierane są przez pracowników przed rozpoczęciem pracy oraz zdawane po jej zakończeniu.
    9) kluczami do drzwi wejściowych oraz do Sekretariatu dysponują osoby upoważnione pisemnie przez Dyrektora.
    10) Wzór wykazu kluczy do drzwi wejściowych oraz do poszczególnych pomieszczeń stanowi Załącznik nr 1 do niniejszej Instrukcji. Wykaz prowadzi Administrator.
    11) Nadawanie uprawnienia do dysponowania kluczami do drzwi wejściowych oraz Sekretariatu obejmuje:
        a) Wzór upoważnienia do stałego dysponowania kluczami, w związku z powierzonym zakresem czynności i pełnioną funkcją stanowi Załącznik nr 2 do niniejszej procedury.
        b) Wzór upoważnienia do doraźnego dysponowania kluczami na indywidualny wniosek Pracownika stanowi Załącznik nr 3 do niniejszej procedury.
    12) Ewidencja osób upoważnionych do dysponowania kluczami stanowi Załącznik nr 4 do niniejszej Instrukcji.

2. Wydawanie i zdawanie kluczy do drzwi wejściowych i pomieszczeń dla osób upoważnionych

    1) Wydawanie kluczy opisane w ust. 1 pkt. 11 lit. a następuje po uzyskaniu upoważnienia Dyrektora a ich zdanie w momencie cofnięcia upoważniania lub najpóźniej w dniu rozwiązania umowy.

    2) Wydawanie i zdawanie kluczy opisane w ust. 1 pkt. 11 lit. b następuje zgodnie z wydanym upoważnieniem.

3. Ogólne zasady dysponowania kluczami

1) Klucze do budynku pozostają pod osobistym nadzorem osób upoważnionych oraz znajdują się w Sekretariacie,
2) Klucze do pomieszczeń znajdują się w Sekretariacie pod osobistym nadzorem osób upoważnionych.
3) Wykaz kluczy oraz ewidencja osób upoważnionych do dysponowania kluczami do drzwi wejściowych i pomieszczeń znajduje się pod nadzorem Dyrektora.

4. Bieżące postępowanie w trakcie dnia pracy
   1) pracownik, który pobrał klucz od pomieszczenia przed uruchomieniem zamków sprawdza od strony wizualnej stan tych zamków i ewentualnych zabezpieczeń zastosowanych przy zamykaniu pomieszczenia,
   2) po otwarciu pomieszczenia, jeszcze przed przystąpieniem do pracy, pracownik sprawdza stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tym pomieszczeniu dokumentacji i innego wyposażenia,
   3) w przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, o których wyżej mowa, pracownik, który to stwierdził, natychmiast powiadamia o tym Dyrektora,
   4) w godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie,
   5) po zakończeniu dnia pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, głównie polegających na:
      a) zabezpieczeniu dokumentacji,
      b) zabezpieczeniu komputerów i haseł,
      c) zamknięciu okien i drzwi,
      d) oddaniu klucza, z wyłączeniem osób posiadających upoważnienie zgodnie z ust. **1** pkt. 11.
5. Klucze do biurek, stanowisk i szaf biurowych są w posiadaniu korzystających z tego pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
6. Naruszenie zasad niniejszej instrukcji może spowodować wyciągnięcie konsekwencji dyscyplinarnych przewidzianych w trybie przepisów prawa pracy.

Załącznik Nr 12
do Polityki Ochrony Danych Osobowych

INSTRUKCJA ZARZĄDZANIA URZĄDZENIAMI MOBILNYMI I NOŚNIKAMI DANYCH

§ 1

Użytkowanie nośników

1. Niniejsza instrukcja reguluje zasady postępowania z urządzeniami mobilnymi i nośnikami danych.
2. Urządzenia mobilne oraz nośniki danych podlegają ewidencji prowadzonej i aktualizowanej przez ADO.
3. Urządzenia mobilne oraz nośniki danych są przechowywane i eksploatowane przez użytkowników zgodnie z zaleceniami producenta, z uwzględnieniem wymagań obowiązujących u Administratora w zakresie ochrony danych osobowych.
4. Urządzenia mobilne oraz nośniki danych zawierające dane osobowe przechowuje się w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym.

§ 2

Zabezpieczanie nośników danych

1. Urządzenia mobilne oraz nośnik danych przed udostępnieniem do użytku zostają zabezpieczone hasłem poprzez zastosowanie ochrony kryptograficznej np. przy użyciu stosownego oprogramowania np. BitLocker.
2. Długość hasła dostępowego do danych na nośniku powinna wynosić co najmniej 8 znaków.
3. Hasło powinno zawierać kombinację liter, cyfr lub znaków specjalnych.
4. Realizację zabezpieczenia, o którym mowa w ust. 1 zapewnia ADO.
5. Administrator przechowuje wykaz haseł oraz kluczy odzyskiwania do wszystkich urządzeń mobilnych i nośników danych.

§ 3

Wydawanie nośników danych użytkownikom oraz ich użytkowanie

1. Udostępnienie urządzenia mobilnego i/lub nośnika danych użytkownikowi wymaga zastosowania protokołu zdawczo-odbiorczego, którego wzór stanowi Załącznik nr 1 do niniejszej Instrukcji. Protokół wydawany jest w dwóch egzemplarzach. Jeden egzemplarz przechowywany jest przez ADO.
2. Protokoły zdawczo-odbiorcze przechowuje ADO.
3. Hasło dostępowe, o którym mowa w §2 ust. 1 przekazywane jest użytkownikowi urządzenia z zachowaniem poufności.
4. Za fizyczne bezpieczeństwo udostępnionego urządzenia mobilnego i/lub nośnika danych odpowiada użytkownik.
5. Użytkownik ponosi pełną odpowiedzialność za ochronę hasła.
6. Zakazuje się przechowywać hasło w łatwo dostępnych miejscach (np. na monitorach komputerów, pod klawiaturami),
7. 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.

8. W przypadku zagubienia, kradzieży lub uszkodzenia nośnika danych użytkownik jest zobowiązany niezwłocznie powiadomić o tym fakcie ADO.

§ 4

Wycofanie z eksploatacji nośników danych

1. Wycofanie z eksploatacji urządzenia mobilnego i/lub nośników danych, przekazanie do naprawy lub ponownego użycia jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.
2. Uszkodzone urządzenia mobilne i/lub nośniki danych zawierające informacje, w tym dane osobowe są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.
3. Wycofane urządzenia mobilne i/lub nośniki danych, które były wykorzystywane do przetwarzania informacji, w tym danych osobowych, nie mogą być wynoszone poza siedzibę Administratora, bez wcześniejszego skutecznego usunięcia danych.
4. Uszkodzone urządzenia mobilne i/lub nośniki danych, zawierające informacje, w tym dane osobowe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji, w szczególności poprzez zgniatanie, łamanie, działanie silnym polem magnetycznym. Niszczenia urządzeń mobilnych i/lub nośników danych dokonuje komisja wyznaczona przez ADO lub wybrana przez ADO firma zewnętrzna.

Załącznik nr 1 do Instrukcji zarządzania urządzeniami mobilnymi i nośnikami danych

Protokół zdawczo-odbiorczy

Dane osoby odbierającej urządzenie mobilne/nośnik danych:

Imię: .....

Nazwisko: .....

Ja niżej podpisany .....

potwierdzam odbiór w dniu ..... godz. ..... następującego urządzenia mobilnego/nośnika danych*:

*niewłaściwe skreślić

Rodzaj urządzenia (np. laptop, pendrive)*	
Numer seryjny *	
Czy zastosowano zabezpieczenie kryptograficzne*	TAK/NIE
***Uzupełnia ADO**	

Oświadczam, że ponoszę materialną odpowiedzialność za urządzenie w czasie jego użytkowania.

....

Administrator Odbierający

Protokół zdawczo-odbiorczy spisano w dwóch egzemplarzach po jednym dla każdej ze stron.

Załącznik Nr 13
do Polityki Ochrony Danych Osobowych

REGULAMIN KORZYSTANIA Z URZĄDZEŃ MOBILNYCH I NOŚNIKÓW DANYCH

§ 1

Niniejszy Regulamin określa zasady użytkowania służbowych urządzeń mobilnych i nośników danych przez pracowników/współpracowników Administratora.

§ 2

1. Pracownik/współpracownik ma obowiązek należytej pieczy nad powierzonym mu mieniem. Pracownik/współpracownik zobowiązany jest do przechowywania i zabezpieczenia mienia w sposób utrudniający jego uszkodzenie lub kradzież, w szczególności dotyczy to urządzeń zawierających dane osobowe. Mienie powierzone winno być używane wyłącznie do celów związanych z prawidłowym wykonaniem obowiązków pracowniczych oraz zgodnie z jego przeznaczeniem.
2. Zabrania się korzystania ze służbowych urządzeń mobilnych i nośników danych w celach innych niż służbowe.
3. Niedopuszczalne jest podczas wykonywania obowiązków pracowniczych korzystanie z prywatnych urządzeń mobilnych i nośników danych.
4. W urządzeniach mobilnych i nośnikach danych, w których istnieje techniczna możliwość stosuje się zabezpieczenia kryptograficzne przy pomocy stworzonych do tego narzędzi np. BitLocker. Za zapewnienie wdrożenia zabezpieczeń kryptograficznych odpowiada ADO.

§ 3

1. Pracownik/współpracownik upoważniony do korzystania z urządzenia mobilnych i/lub nośników danych zobowiązany jest do ich zabezpieczenia w czasie transportu.
2. Gdy urządzenie mobilne jest pozostawione w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie go hasłem (blokada ekranu zgodnie z Zasadą czystego ekranu).
3. Pracując na urządzeniu mobilnym w miejscach publicznych i środkach transportu, pracownik/współpracownik zobowiązany jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
4. Każde urządzenie mobilne powinno być zablokowane hasłem/blokadą klawiatury w postaci cyfrowej, linii papilarnych lub interfejsu graficznego. Hasło dostępu do komputera przenośnego powinno się składać co najmniej z 8 znaków i zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Kod blokady klawiatury do pozostałych urządzeń mobilnych nie może być trywialny.
5. Pracownik/współpracownik nie może samodzielnie dokonywać napraw, modyfikacji urządzeń mobilnych i nośników danych pod rygorem obciążenia kosztami ewentualnych napraw na skutek w/w czynności. Za zapewnienie napraw i modyfikacji urządzeń mobilnych i nośników danych odpowiedzialny jest ADO.
6. Pracownik/współpracownik nie może przechowywać w pamięci urządzenia mobilnego i na nośnikach danych plików muzycznych, graficznych, video z nielegalnych źródeł oraz naruszających prawa autorskie.
7. Pracownik/współpracownik nie może samodzielnie instalować na urządzeniach mobilnych różnego rodzaju aplikacji. Za zapewnienie konfiguracji urządzeń mobilnych odpowiedzialny jest ADO.
8. Za szkody spowodowane instalacją obcego oprogramowania, o którym mowa w ust. 7, jak również za wszelkie szkody powstałe wskutek nieprawidłowego korzystania z powierzonego

mienia, w tym w szczególności w wyniku niezastosowania się do zasad określonych w niniejszym Regulaminie, odpowiada pracownik/współpracownik.

§ 4

W przypadku zagubienia, kradzieży lub uszkodzenia nośnika danych użytkownik jest zobowiązany niezwłocznie powiadomić o tym fakcie ADO.

§ 5

W sprawach nieuregulowanych niniejszym Regulaminem ostateczną decyzje podejmuje Administrator, a w przypadku powstania szkody zastosowanie znajdują przepisy Kodeksu pracy/Kodeksu cywilnego regulujące zasady odpowiedzialności pracownika/współpracownika za szkodę wyrządzoną w mieniu powierzonym.

Załącznik Nr 14
do Polityki Ochrony Danych Osobowych

Regulamin
korzystania z dostępu do Internetu oraz z poczty elektronicznej

§ 1
Postanowienia ogólne

1. Administrator udostępnia swoim pracownikom dostęp do systemu informatycznego. Dostęp ten odbywa się za pośrednictwem powierzonych użytkownikom komputerowych stanowisk w celu wykonywania czynności służbowych z indywidualną możliwością korzystania z niniejszych serwisów informacyjnych oraz wymiany danych dostępnych w sieci Internet:
   - serwis WWW,
   - pocztę elektroniczną.

2. Nadzór nad systemem informatycznym oraz nad pocztą elektroniczną sprawuje Dyrektor.

§ 2
Zasady korzystania z sieci Internet przy użyciu sprzętu służbowego

1. Wszelkie czynności prowadzące do uzyskania dostępu poza udzielonym, w tym usiłowania obejścia zabezpieczeń, instalowanie nakładek programowych umożliwiających dostęp do innych serwisów poprzez WWW, instalowanie wszelkiego oprogramowania na powierzonych komputerowych stanowiskach bez zgody Dyrektora będzie interpretowane jako naruszenie niniejszego Regulaminu oraz uznawane za zachowanie godzące w interesy majątkowe i dobre imię Administratora. W przypadku takich naruszeń będą one traktowane jako naruszenia obowiązków pracowniczych.
2. Użytkownicy podczas korzystania z udostępnionych serwisów internetowych w czasie pracy powinni korzystać z nich proporcjonalnie do czasu wykonywania powierzonych zadań przy użyciu Internetu.
3. Z serwisów internetowych należy korzystać wyłącznie do celów służbowych, co jest podyktowane koniecznością zachowania odpowiedniego poziomu bezpieczeństwa.
4. W związku z publicznym charakterem Internetu, należy podejmować niezbędne działania, aby nie ujawniać w nim informacji poufnych, a także nie uzyskiwać za jego pośrednictwem nielegalnych informacji.
5. Jest zabronione oraz jest ścigane przez prawo uzyskiwanie dostępu, przechowywanie lub rozprowadzanie przez Internet lub za pomocą poczty elektronicznej:
   1) materiałów pornograficznych lub obscenicznych,
   2) informacji i instrukcji, zastosowanie których może powodować uszczerbek w zdrowiu, utratę życia lub zagrożenie zbiorowe,
   3) wirusów komputerowych, koni trojańskich,
   4) nielegalnych kopii oprogramowania lub utworów.
6. Korzystając z Internetu należy pamiętać, iż każda wysłana wiadomość może z łatwością zostać przechwycona, wydrukowana, zmodyfikowana i rozpowszechniona szkodząc wizerunkowi Administratora, a także wizerunkowi jego pracowników lub współpracowników.
7. Pracownik, poruszając się w sieci Internet, gromadząc lub rozsyłając w niej informacje, może naruszyć obowiązujące prawo, w tym w szczególności:
   - 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),

- ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,
- ustawę z dnia 6 czerwca 1997 r. - Kodeks karny

§ 3

Zakładanie kont poczty elektronicznej

1. Konta pocztowe są zakładane na czas świadczenia pracy na rzecz Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28.
2. Konta służbowe poczty elektronicznej w Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28 są zakładane przez Dyrektora.
3. Imienne adresy poczty mailowej mają postać: pierwszaliteranazwiskanazwisko@rewal.pl
4. Dostęp do kont poczty elektronicznej chroniony jest hasłem utworzonym przez Dyrektora.
5. Hasło dostępowe, o którym mowa w ust. 4 przekazywane jest użytkownikowi konta poczty elektronicznej z zachowaniem poufności.
6. Dyrektor raz w roku dokonuje zmiany haseł i przekazuje je użytkownikom kont poczty elektronicznej.
7. Hasło dostępu do poczty powinno się składać co najmniej z 8 znaków i zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

§ 4

Dostęp do kont poczty elektronicznej

1. Dostęp do konta poczty elektronicznej odbywa się za pośrednictwem powierzonych użytkownikom komputerowych stanowisk i wyłącznie przy użyciu sprzętu służbowego.
2. Dostęp do konta poczty elektronicznej jest możliwy za pomocą przeglądarki internetowej.
3. Po zakończeniu pracy przy użyciu konta poczty elektronicznej pracownik zobowiązany jest się z niego wylogować.
4. Informacje o adresach e-mail pracowników są jawne.
5. W toku toczących się postępowań oraz na stronie internetowej są podawane wyłącznie służbowe adresy poczty mailowej pracowników.

§ 5

Prawa i obowiązki użytkowników poczty elektronicznej

1. Ze służbowego konta poczty elektronicznej może korzystać wyłącznie osoba lub grupa osób, dla której konto zostało założone. Zabronione jest udostępnianie hasła dostępu do konta osobom nieuprawnionym.
2. Konto poczty elektronicznej jest przeznaczone wyłącznie do użytku służbowego. Niedozwolone jest wykorzystywanie konta w sposób godzący w dobre imię Administratora.
3. Użytkownicy służbowej poczty elektronicznej są zobowiązani do systematycznego przeglądania poczty przychodzącej.
4. Użytkownicy mają obowiązek szyfrowania 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;
5. W przypadku wysyłania korespondencji do większej liczby osób należy dbać o to, aby osoba, do której skierowana jest tego typu korespondencja, nie miała możliwości zapoznawania się z danymi pozostałych adresatów wiadomości, nie tylko ich imionami i nazwiskami, ale również adresami e-mail.
6. Przy wysyłce maila do większej ilości adresatów należy skorzystać z opcji „kopii ukrytej" (BCC, UDW).

7. Pracownicy wysyłający pliki, które zawierają dane osobowe drogą mailową zobowiązane są do używania programu szyfrującego (np. WinRAR) w celu zabezpieczenia przesyłanego pliku hasłem oraz przesłania hasła do odbiorcy drogą alternatywną (sms lub przekazanie hasła telefonicznie).
8. Pracownikom nie wolno korzystać z poczty elektronicznej w celu uzyskania korzyści osobistych i majątkowych, reklamowania się, ubiegania się o środki finansowe, wysyłania listów rozsyłanych systemem lawinowym (łańcuszkowym), rozsyłania tzw. spamu lub wysyłania dowolnych innych wiadomości, które mogłyby szkodzić reputacji lub narazić Szpital na koszty lub straty.
9. Problemy techniczne związane z użytkowaniem konta powinny być zgłaszane Dyrektorowi. Próby wyłudzenia danych poprzez konto służbowej poczty elektronicznej lub nieuprawnionego dostępu do niego powinny być zgłaszane Inspektorowi Ochrony Danych (IOD).
10. W przypadkach otrzymywania nieoczekiwanych wiadomości od nieznanych nadawców, użytkownicy nie powinni ich otwierać, nie otwierać ich załączników, poza tym nie wolno im rozsyłać ich do innych użytkowników. Jeśli wiadomość nie dotyczy Administratora, należy ją wykasować. Jeśli może dotyczyć Administratora, należy skonsultować jej zawartość z innymi użytkownikami wysyłając do nich odrębną wiadomość. Zabrania się rozsyłania otrzymanej wiadomości w formie zapytania do innych poszczególnych użytkowników, w szczególności do dużych grup użytkowników ze względu na możliwość powiększenia istniejącego zagrożenia wirusami komputerowymi.
11. Wiadomości wysyłane przez pracowników z konta służbowej poczty elektronicznej powinny być opatrzone klauzulą poufności o treści:

„Niniejsza wiadomość zawiera dane wrażliwe i jest przeznaczona wyłącznie do użytku osób, do których wiadomość została adresowana. Jeśli nie są Państwo zamierzonym odbiorcą tej wiadomości, informujemy, że jej ujawnianie, kopiowanie, przesyłanie lub podejmowanie jakichkolwiek działań w związku z treścią tej wiadomości jest surowo wzbronione.
Prosimy o natychmiastowe powiadomienie nadawcy, za pośrednictwem poczty elektronicznej, o pomyłkowym otrzymaniu tej wiadomości i usunięcie jej z Państwa komputera."

§ 6
Blokowanie kont poczty elektronicznej

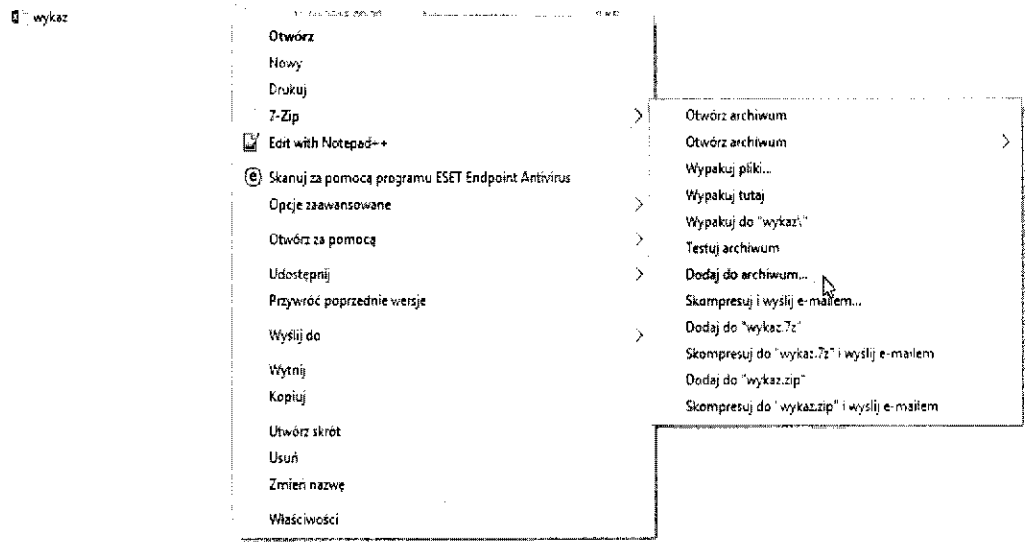
1. Administrator ma prawo zablokowania konta pocztowego w przypadkach jego wykorzystania w sposób niezgodny z niniejszym Regulaminem.
2. Blokady konta dokonuje Dyrektor.
3. Konto pocztowe pracownika może być zablokowane w przypadku planowanej nieobecności pracownika trwającej dłużej niż miesiąc.
4. Konto pocztowe pracownika może być odblokowane po usunięciu przyczyny jego zablokowania.

§ 7
Zamykanie kont poczty elektronicznej

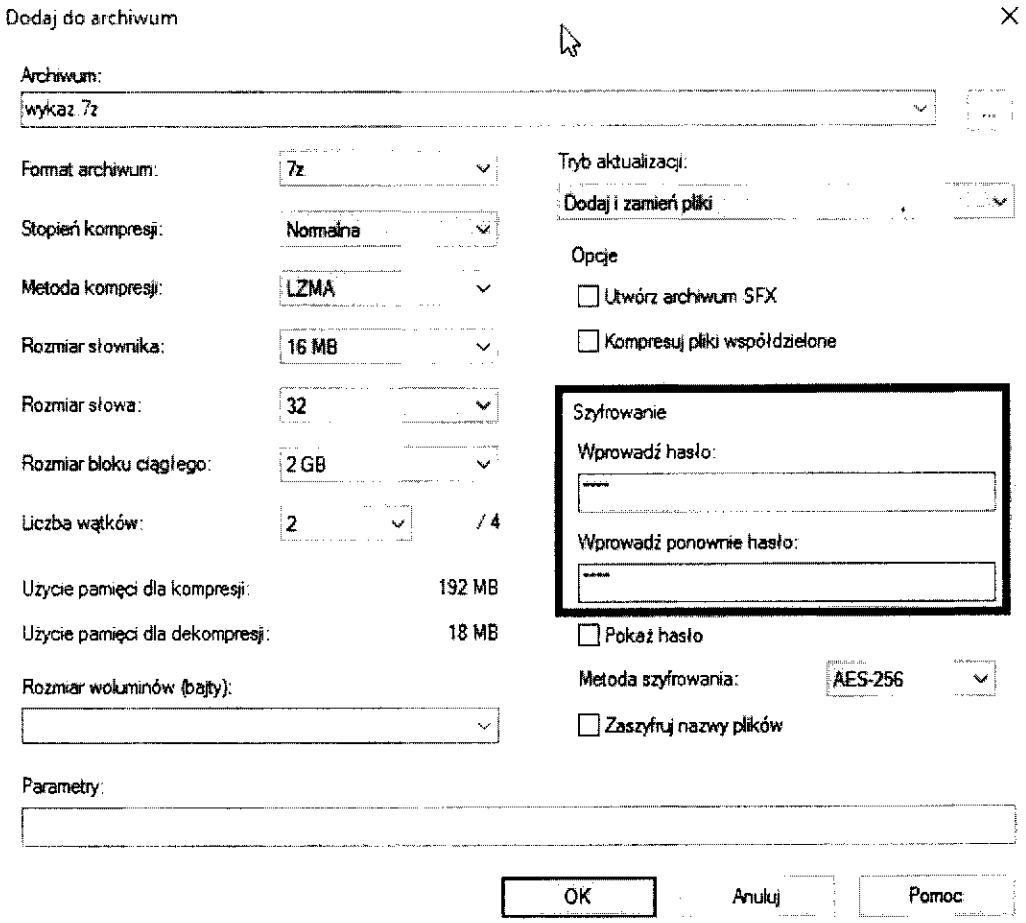
1. W przypadku rozwiązania lub wygaśnięcia stosunku pracy/zakończenia współpracy z Administratorem, konto użytkownika jest niezwłocznie blokowane przez Dyrektora.
2. Trwałe usunięcie konta wraz z jego zawartością następuje po upływie 5 lat od dnia jego zablokowania.
3. Dyrektor może zdecydować o zarchiwizowaniu wiadomości znajdujących się na koncie pocztowym.

I. INTRUKCJA SZYFROWANIA PLIKU/KATALOGU PROGRAMEM 7-ZIP

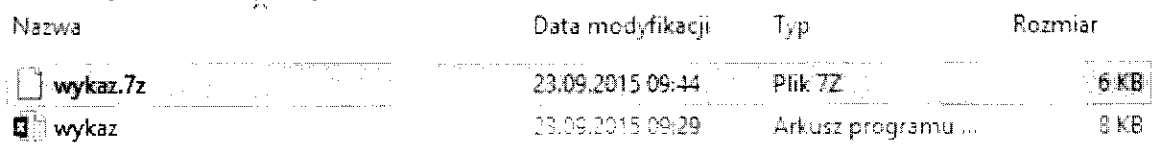
1. Należy kliknąć prawym przyciskiem myszy na plik lub katalog i wybrać opcję 7-zip -> Dodaj do archiwum. Przykład na poniższym rysunku:



2. Następnie w okienku „Dodaj do archiwum" w polu „Wprowadź hasło:" wpisujemy hasło, którym chcemy zaszyfrować plik lub katalog. W polu „Wprowadź ponownie hasło:" ponownie wpisujemy hasło w celu weryfikacji poprawności wpisanego hasła. Przykład na poniższym rysunku:

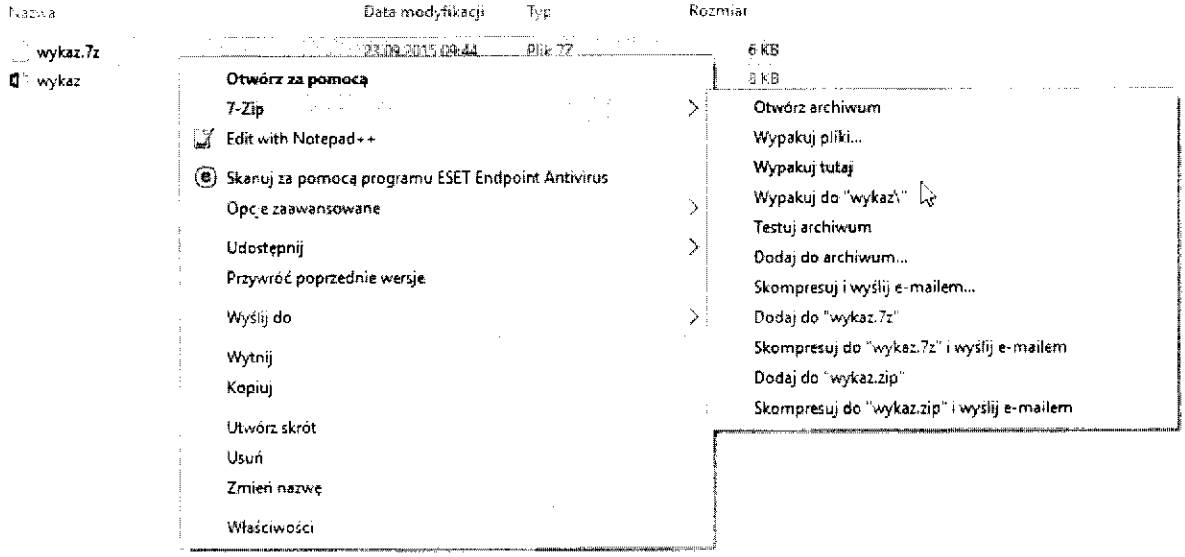


3. W wyniku szyfrowania otrzymujemy plik o rozszerzeniu .7z, który można bezpiecznie przesłać e-mailem jak normalny załącznik.

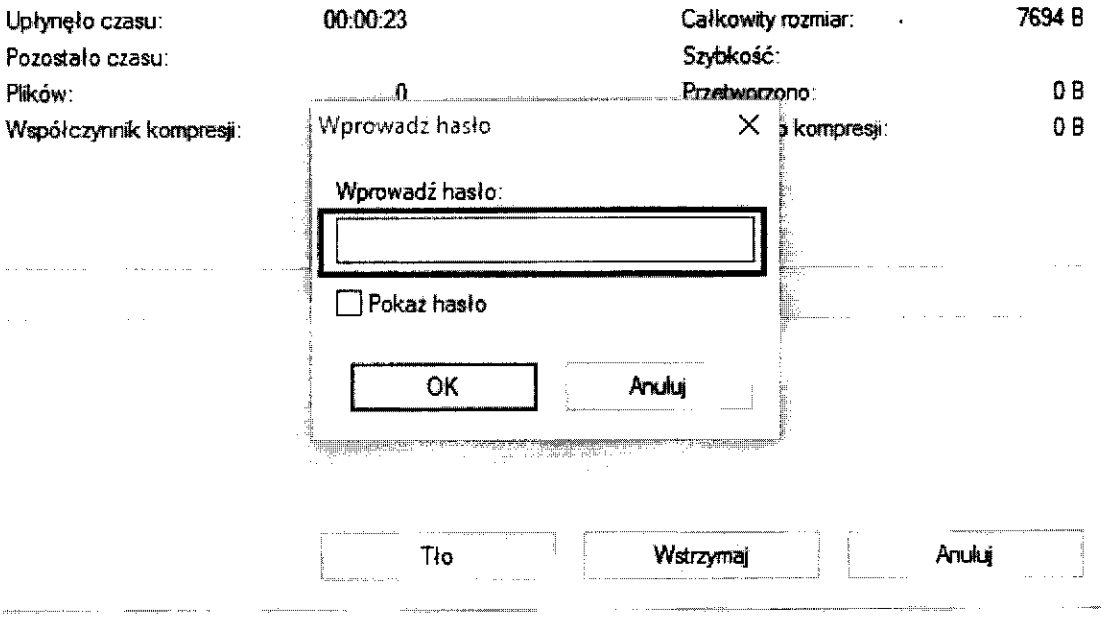


II. INTRUKCJA ODSZYFROWANIA PLIKU/KATALOGU PROGRAMEM 7-ZIP

1. Zaszyfrowany załącznik w wiadomości e-mail należy zapisać na komputerze.
2. Na zaszyfrowanym pliku należy kliknąć prawym przyciskiem myszy i wybrać opcję 7 zip -> wypakuj tutaj. Przykład na poniższym obrazku:



3. Następnie w okienku wpisujemy hasło do archiwum. Przykład na poniższym obrazku:



Załącznik Nr 16
do Polityki Ochrony Danych Osobowych

INSTRUKCJA USUWANIA DANYCH OSOBOWYCH Z KOPII ZAPASOWYCH I SPROSTOWANIA DANYCH OSOBOWYCH W KOPIACH ZAPASOWYCH

Niniejsza instrukcja zawiera opis zasad usuwania danych osobowych z kopii zapasowych i zasad sprostowania danych w kopiach zapasowych.

§1
Usuwanie danych osobowych z kopii zapasowych

1. W celu realizacji praw osób, których dane osobowe przetwarza ADO, wynikających z art. 17 RODO (prawo do usunięcia danych) po stronie ADO istnieje obowiązek usunięcia danych osobowych w następujących przypadkach:

   - wygaśnięcie przesłanki do przetwarzania danych osobowych określonej w art. 6 i 9 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) – dalej RODO,
   - skorzystanie przez osobę z prawa do usunięcia danych osobowych.

2. W przypadku wpłynięcia wniosku o usunięcie danych osobowych lub w przypadku wygaśnięcia przesłanki do przetwarzania danych osobowych należy przede wszystkim usunąć dane osobowe ze środowiska produkcyjnego (środowisko, w którym uruchamiane są programy, a konfiguracje sprzętowe są instalowane i polegają na codziennych działaniach organizacji).
3. Zasady postępowania z danymi osobowymi wynikające z RODO mają zastosowanie do danych osobowych przetwarzanych w kopiach zapasowych. W związku z tym, w przypadku skorzystania przez osobę z prawa do usunięcia danych osobowych, na ADO spoczywa obowiązek ich usunięcia z kopii zapasowych, o ile jest to technicznie możliwe (np. kopia zapasowa nie jest w żaden sposób skompresowana, a więc usunięcie danych osobowych z kopii będzie równie łatwe jak usunięcie ze środowiska produkcyjnego).
4. W przypadku, gdy za przechowywanie kopii zapasowej odpowiedzialny jest podmiot zewnętrzny, Administrator każdorazowo ustala z nim zasady usuwania danych osobowych z kopii zapasowych.
5. W przypadku braku technicznej możliwości usunięcia takich danych osobowych z kopii zapasowych lub gdy koszty i wysiłek organizacyjny takiego selektywnego usunięcia danych osobowych będą zbyt duże w stosunku do ryzyka naruszenia praw i wolności podmiotu danych, usunięcie danych osobowych nastąpi w chwili ich nadpisania lub w przypadku konieczności przywrócenia danych osobowych z kopii zapasowej do środowiska produkcyjnego. Selektywne usunięcie danych osobowych z kopii zapasowych narusza ich integralność, a zatem może powodować ryzyko dla praw i wolności innych osób, których dane są przechowywane w ramach tej samej kopii zapasowej.
6. Żądanie usunięcia danych osobowych uważa się za spełnione, gdy dane osobowe zostały usunięte ze środowiska produkcyjnego i gdy kopie zapasowe zostały nadpisane kolejnymi kopiami.
7. Za ostateczną datę realizacji żądania uważa się datę trwałego usunięcia danych osobowych.
8. W sytuacji potrzeby odtworzenia kopii zapasowej do środowiska produkcyjnego, przed wyznaczoną datą jej nadpisania, ADO nadzoruje realizację usunięcia danych osobowych.
9. Należy również poinformować osobę wnioskującą o usunięcie danych osobowych o ich usunięciu ze środowiska produkcyjnego oraz podać datę usunięcia danych osobowych zawartych w kopiach zapasowych.

§2

Sprostowanie danych osobowych w kopiach zapasowych

1. W celu realizacji praw osób, których dane osobowe przetwarza ADO, wynikających z art. 16 RODO, po stronie ADO istnieje obowiązek sprostowania danych osoby składającej żądanie.
2. W przypadku wpłynięcia wniosku o sprostowanie danych należy przede wszystkim sprostować dane osobowe wnioskującej osoby w środowisku produkcyjnym.
3. Zasady postępowania z danymi osobowymi wynikające z RODO mają zastosowanie do danych osobowych przetwarzanych w kopiach zapasowych. W związku z tym, w przypadku skorzystania przez osobę z prawa do sprostowania danych, na ADO spoczywa obowiązek realizacji tego prawa również w zakresie kopii zapasowych, o ile jest to technicznie możliwe.
4. W przypadku, gdy za przechowywanie kopii zapasowej odpowiedzialny jest podmiot zewnętrzny, Administrator każdorazowo ustala z nim zasady sprostowania danych osobowych w kopiach zapasowych.
5. W przypadku braku technicznej możliwości sprostowania takich danych w kopiach zapasowych lub gdy koszty i wysiłek organizacyjny takiego sprostowania danych osobowych będą zbyt duże w stosunku do ryzyka naruszenia praw i wolności podmiotu danych, dane osobowe zostaną sprostowane tylko w przypadku konieczności przywrócenia danych osobowych z kopii zapasowej do środowiska produkcyjnego.
6. Żądanie sprostowania danych osobowych uważa się za spełnione, gdy dane osobowe zostaną sprostowane w środowisku produkcyjnym i gdy kopie zapasowe zostaną nadpisane kolejnymi kopiami.
7. Za ostateczną datę realizacji żądania uważa się datę ostatecznego sprostowania danych osobowych.
8. W sytuacji potrzeby odtworzenia kopii zapasowej do środowiska produkcyjnego, przed wyznaczoną datą jej nadpisania, ADO nadzoruje realizację sprostowania danych osobowych.
9. Należy również poinformować osobę wnioskującą o sprostowanie danych osobowych o ich sprostowaniu w środowisku produkcyjnym oraz podać datę nadpisania kopii zapasowych.

Załącznik Nr 17

do Polityki Ochrony Danych Osobowych

Ewidencja sprzętu informatycznego, aplikacji oraz użytkowników systemu informatycznego

LP	Numer ewidencyjny/numer seryjny	Nazwa modelu oraz rodzaj sprzętu	System operacyjny	Zainstalowane programy przetwarzające dane osobowe	Użytkownik oraz identyfikator użytkownika	Antywirus	Stosowane zabezpieczenia
1	Xxxx/xxx	Asus XXX	Windows 11 Pro	Thunderbird - Poczta/Program kadrowo płacowy - Librus - Etc.	Jan Kowalski Jan.kowalski	ESET Licencja ważna do.....	BitLocker
2							
3							
4							
5							
6							

Załącznik Nr 18
do Polityki Ochrony Danych Osobowych

Niechorze, dn. .....

Wniosek dot. wykorzystania sprzętu służbowego poza siedzibą Administratora

Imię	
Nazwisko	

Dyrektor Muzeum Rybołówstwa Morskiego w Niechorzu
72-350 Niechorze, Aleja Bursztynowa 28

Zwracam się z prośbą o udzielenie zgody na korzystanie w celach służbowych z niżej wymienionego urządzenia poza siedzibą Muzeum Rybołówstwa Morskiego w Niechorzu, 72-350 Niechorze, Aleja Bursztynowa 28. Szczegóły sprzętu:

Rodzaj urządzenia: _____ [laptop lub inne]
Numer seryjny: _____ [Numer seryjny]
Czy urządzenie zabezpieczono kryptograficznie: _____ [tak/nie]

Planowany okres użytkowania poza siedzibą Administratora:
Od: _____ [Data rozpoczęcia]
Do: _____ [Data zakończenia]

Zobowiązuję się do odpowiedzialnego i bezpiecznego korzystania z powierzonego sprzętu oraz do poniesienia pełnej odpowiedzialności materialnej za jego stan.

_____
Data i czytelny podpis pracownika

Wyrażam zgodę/nie wyrażam zgody na wykorzystywanie w/w sprzętu komputerowego poza siedzibą Administratora.

_____
Czytelny podpis Administratora