Uchwała nr 67/2017
Zarządu Stowarzyszenia Wielkie Jeziora Mazurskie 2020
z dnia 06.07.2017
w sprawie wprowadzenia Polityki Bezpieczeństwa

Na podstawie § 21 ust. 1 pkt. 15 Statutu Stowarzyszenia Wielkie Jeziora Mazurskie 2020 Zarząd Stowarzyszenia uchwala co następuje:

§ 1

Wprowadza się, jako obowiązującą w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 Politykę Bezpieczeństwa stanowiącą załącznik nr 1 do uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Zarządu Stowarzyszenia
Piotr Jakubowski

STOWARZYSZENIE
Wielkie Jeziora Mazurskie 2020
11-730 Mikołajki, ul. Kolejowa 6
NIP 845-198-57-00 REGON 361222985

Stowarzyszenie WIELKIE JEZIORA MAZURSKIE 2020

POLITYKA BEZPIECZEŃSTWA

Kod dokumentu:	ODO-PBI-01
Wersja:	01.
Data wersji:	2017/06/02
Utworzony przez:	Mirosław Górski
Zatwierdzony przez:	
Poziom poufności:	Użytek wewnętrzny

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany
2017-06-30	0.1	Mirosław Górski	Podstawowy szablon dokumentu

Spis treści

1. CEL, ZAKRES I UŻYTKOWNICY 4

2. DOKUMENTY REFERENCYJNE 4

3. OKREŚLENIA I SKRÓTY UŻYTE W POLITYCE BEZPIECZEŃSTWA 4

4. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH 6

4.1. WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE 6

4.2. WYKAZ ZBIORÓW DANYCH 6

4.3. OPIS STRUKTURY ZBIORÓW DANYCH 7

4.4. PRZEPŁYW DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI 7

4.5. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH 7

4.5.1. Zabezpieczenia organizacyjne 7

4.5.2. Zabezpieczenia ochrony fizycznej danych osobowych 8

4.5.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej 8

4.5.4. Zabezpieczenia narzędzi programowych i baz danych 8

5. ZARZĄDZANIE PRZETWARZANIEM DANYCH OSOBOWYCH ORAZ CZUWANIE NAD ICH BEZPIECZEŃSTWEM 8

5.1. UPRAWNIENIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI 8

5.2. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH 8

6. GROMADZENIE DANYCH OSOBOWYCH 9

6.1. WYKORZYSTYWANIE DANYCH 9

7. PRZETWARZANIE DANYCH OSOBOWYCH 9

8. OBOWIĄZEK INFORMACYJNY 9

9. UDOSTĘPNIENIE DANYCH OSOBOWYCH 10

9.1. ODMOWA UDOSTĘPNIENIA DANYCH 11

10. OCHRONA PRZETWARZANIA DANYCH OSOBOWYCH 11

10.1. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH 11

10.2. OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE 11

11. POSTĘPOWANIE W PRZYPADKACH NARUSZENIA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH 12

11.1. PRZYPADKI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH 12

11.2. POSTĘPOWANIE W RAZIE WYKRYCIA NARUSZEŃ 12

12. ZAŁĄCZNIKI 13

13. WAŻNOŚĆ ORAZ ZARZĄDZANIE NINIEJSZYM DOKUMENTEM 13

1. Cel, zakres i użytkownicy

Niniejsza Polityka Bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych.

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z 29 sierpnia 1997r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niemniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w organizacji w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

Użytkownikami niniejszego dokumentu są pracownicy Stowarzyszenia Wielkie Jeziora Mazurskie 2020, jak również odnośne podmioty zewnętrzne.

2. Dokumenty referencyjne

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
- Instrukcja Zarządzania Systemem Informatycznym w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;

3. Określenia i skróty użyte w Polityce Bezpieczeństwa

Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych.

Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób.

Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna.

Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji.

Polityka - rozumie się przez to Politykę Bezpieczeństwa Informacji w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;

Instrukcja - rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;

Administrator Danych Osobowych – Zarząd Stowarzyszenia Wielkie Jeziora Mazurskie 2020, decydujący o celach i środkach przetwarzania danych osobowych;

Administrator Bezpieczeństwa Informacji (ABI) - osobę powołaną przez ADO w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020, wpisaną do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych rejestru administratorów bezpieczeństwa informacji, zwaną dalej „ABI";

Ustawa - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922);

Rozporządzenie - Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);

Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;

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

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

Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;

Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;

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

Użytkownik - pracownik Stowarzyszenia Wielkie Jeziora Mazurskie 2020 posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

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

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

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

Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie.

4. Obszary przetwarzania danych osobowych

4.1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe

Obszar przetwarzania danych osobowych w Stowarzyszeniu WJM 2020 obejmuje pomieszczenie w którym przetwarzane są dane osobowe (miejsce, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsce, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji.

Obszar przetwarzania danych osobowych określony jest w rejestrze „**Wykazie pomieszczeń, w których przetwarzane są dane osobowe**", stanowiącym **załącznik nr 1** do Polityki Bezpieczeństwa. Wykaz ten zawiera następujące informacje:

1) lokalizację budynku,
2) numer pomieszczenia i jego przeznaczenie,
3) wskazanie piętra budynku,
4) określenie komórki użytkującej dane pomieszczenie,
5) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
6) określenie zabezpieczenia pomieszczenia.

Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w **załączniku nr 2** do Polityki Bezpieczeństwa - „**Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe**".

4.2. Wykaz zbiorów danych

Wykaz zbiorów danych przetwarzanych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 określony został w **załączniku nr 3** do Polityki Bezpieczeństwa – „**Wykaz zasobów danych osobowych i systemów ich przetwarzania**". Wykaz ten zawiera następujące informacje:

1) nazwę zbioru danych,
2) określenie systemu przetwarzania danych osobowych,
3) lokalizację miejsca przetwarzania danych osobowych,
4) stosowane przy przetwarzaniu danych osobowych oprogramowanie,
5) określenie sposobu przepływu danych pomiędzy systemami,

Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania danego systemu informatycznego są zawarte w instrukcji zarządzania systemem informatycznym.

4.3. Opis struktury zbiorów danych

Elektroniczne przetwarzanie danych osobowych odbywa się na stacjach roboczych użytkowników. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi określony został w **załączniku nr 4** do Polityki Bezpieczeństwa – **„Opis struktury zbiorów danych"**

4.4. Przepływ danych pomiędzy systemami informatycznymi

W ramach procesów przetwarzania danych ma miejsce przepływ danych w ramach systemu informatycznego SL2014 i RAKS. Informacje na temat przepływu danych w ramach systemu informatycznego znajdują się w **załączniku nr 3** do Polityki Bezpieczeństwa - **„Wykazie zasobów danych osobowych i systemów ich przetwarzania"**

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

4.5.1. Zabezpieczenia organizacyjne

1) Został wyznaczony i zgłoszony do GIODO administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych, określenie systemu przetwarzania danych osobowych,
2) Została opracowana i wdrożona polityka bezpieczeństwa,
3) Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
4) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
5) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
6) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
7) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
8) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
9) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
10) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe,
11) Dochowuje się staranności zabezpieczenia danych przy ich gromadzeniu oraz udostępnianiu,
12) Określono postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych.

4.5.2. Zabezpieczenia ochrony fizycznej danych osobowych

Zabezpieczenia fizyczne ochrony danych osobowych określone zostały w **załączniku nr 2** do Polityki Bezpieczeństwa - „**Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe**".

4.5.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

4.5.4. Zabezpieczenia narzędzi programowych i baz danych

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

5. Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

5.1. Uprawnienia Administratora Bezpieczeństwa Informacji

W celu realizacji powierzonych zadań ABI w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 ma prawo:

1) Kontrolować Stowarzyszenie Wielkie Jeziora Mazurskie 2020 w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia pracownikom Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w zakresie bezpieczeństwa danych osobowych;
3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich członków Stowarzyszenia Wielkie Jeziora Mazurskie 2020 wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

5.2. Obowiązki Administratora Danych Osobowych

ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

1) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych; wzór formularza oświadczenia stanowi **załącznik nr 5** do Polityki Bezpieczeństwa;
2) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi **załącznik nr 5a** do Polityki Bezpieczeństwa;
3) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej; wzór formularza porozumienia stanowi **załącznik nr 6** do Polityki Bezpieczeństwa.

6. Gromadzenie danych osobowych

Dane osobowe przetwarzane w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

6.1. Wykorzystywanie danych

Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Jeżeli dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

7. Przetwarzanie danych osobowych

Właściciel zasobów danych osobowych obowiązany jest zgłaszać Administratorowi Bezpieczeństwa Informacji zamiar utworzenia nowego zbioru danych osobowych. Administrator Bezpieczeństwa Informacji przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru zgłoszenia.

Administrator Bezpieczeństwa Informacji, w uzgodnieniu z Administratorem Danych Osobowych, określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.

Administrator Bezpieczeństwa Informacji przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru. Przepisy ust. 2–7 stosuje się odpowiednio.

8. Obowiązek informacyjny

Stowarzyszenie Wielkie Jeziora Mazurskie 2020 w którym są zbieranie i przetwarzane dane osobowe, jest odpowiedzialne za poinformowanie osób, których dane osobowe przetwarzają, o:

1) adresie siedziby organizacji, pod którym dane są zbierane i przetwarzane;
2) celu zbierania danych;
3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 Ustawy.

Wzór formularza stosowanego dla spełnienia obowiązków, stanowi **załącznik nr 7** do Polityki Bezpieczeństwa.

Materiały dotyczące innej niż ustawowa/podstawowa działalności organizacji mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

Kandydaci do pracy w Stowarzyszeniu, w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.

Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.

9. Udostępnienie danych osobowych

ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
2) na podstawie umowy z innym podmiotem, w ramach, której istnieje konieczność udostępnienia danych;
3) na podstawie wniosku osoby, której dane dotyczą.

Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi **załącznik nr 8** do Polityki Bezpieczeństwa.

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

W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.

Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu, i informuje o tym ABI.

ABI jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

9.1. Odmowa udostępnienia danych

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

10.Ochrona przetwarzania danych osobowych

Do przetwarzania danych mogą być dopuszczeni pracownicy organizacji posiadający upoważnienie nadane przez ABI. Wzór upoważnienia określa **załącznik nr 9** do Polityki Bezpieczeństwa.

Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi **załącznik nr 10** do Polityki Bezpieczeństwa.

10.1. Powierzenie przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 31 Ustawy na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

Właściciel zasobów danych osobowych informuje Administratora Bezpieczeństwa Informacji o zamiarze powierzenia danych osobowych do przetwarzania.

Administrator Bezpieczeństwa Informacji przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.

W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.

Zaparafowany projekt umowy jest przedkładany przez Administratora Bezpieczeństwa Informacji do akceptacji i podpisu Administratora Danych Osobowych. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 11** do Polityki Bezpieczeństwa Informacji.

10.2. Obowiązki podmiotu przetwarzającego dane osobowe

Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

Podmiot, o którym mowa wyżej, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.

11. Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;
2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

11.1. Przypadki naruszenia bezpieczeństwa danych osobowych

Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

11.2. Postępowanie w razie wykrycia naruszeń

W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji a następnie postępować stosownie do podjętej przez niego decyzji.

Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;
4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

Administrator Danych osobowych podejmuje działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia;
2) wyjaśnienie okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia,

4) umożliwienie dalszego bezpiecznego przetwarzania danych.

2. Dla realizacji celów określonych w ust. 1 Administrator Bezpieczeństwa Informacji ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:

1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji traktowana będzie, jako naruszenie obowiązków pracowniczych.

Administrator Bezpieczeństwa Informacji po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi **załącznik nr 12** do Polityki Bezpieczeństwa Informacji.

12.Załączniki

- Załącznik 1: Wykaz pomieszczeń, w których przetwarzane są dane osobowe
- Załącznik 2: Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe
- Załącznik 3: Wykaz zbiorów
- Załącznik 4: Opis struktury zbiorów
- Załącznik 5: Oświadczenie osoby upoważnionej do przetwarzania danych
- Załącznik 5a: Oświadczenie
- Załącznik 6: Przekazanie sprzętu
- Załącznik 7: Oświadczenie o spełnieniu obowiązku informacyjnego
- Załącznik 8: Wniosek o udostępnienie danych osobowych
- Załącznik 9: Upoważnienie do przetwarzania danych osobowych
- Załącznik 10: Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik 11: Umowa powierzenie danych osobowych
- Załącznik 12: Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych

13.Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 2017/06/02.

Właścicielem niniejszego dokumentu jest Administrator Bezpieczeństwa Informacji, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu, co najmniej raz w roku.

W ocenie efektywności i właściwości niniejszego dokumentu należy wziąć pod uwagę następujące kryteria:

- liczbę pracowników i podmiotów zewnętrznych, których dotyczy proces przetwarzania danych osobowych, a którzy nie zapoznali się z niniejszym dokumentem

- niezgodność dokumentacji przetwarzania danych osobowych z przepisami prawa, obowiązkami branżowymi, zobowiązaniami umownymi oraz innymi dokumentami wewnętrznymi organizacji;
- nieefektywność wdrożenia i obsługi procesu danych osobowych
- niejasny podział odpowiedzialności za wdrożenie dokumentacji przetwarzania danych osobowych

Załącznik nr 1 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Wykaz pomieszczeń siedziby Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w Mikołajkach,

w których przetwarzane są dane osobowe

	Lokalizacja Adres i numer budynku	Numer i przeznaczenie pomieszczenia*	Piętro	Nazwa referatu użytkującego pomieszczenie	Osoby pracujące w pomieszczeniu**	Zabezpieczenie pomieszczenia***
1.	2.	3.	4.	5.	6.	7.
1	ul. Kolejowa 6 11-730 Mikołajki	Pomieszczenie biurowe	1	Biuro Stowarzyszenia WJM 2020	Dyrektor Biura Stowarzyszenia WJM 2020 Specjalista ds. realizacji i koordynacji projektów, Stowarzyszenie WJM 2020	Drzwi zabezpieczone zamkiem

*Należy podać numer pomieszczenia i jego przeznaczenie np. pokój biurowy, archiwum, kancelaria, serwerownia, biuro przepustek.
** Należy podać same stanowiska i liczbę osób bez imion i nazwisk.
*** Należy podać sposób zabezpieczenia pomieszczenia np. drzwi zamykane na klucz, kraty w oknach, pomieszczenie monitorowane, kontrola dostępu itp.

Załącznik nr 2 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

§ 1. Ochrona pomieszczeń

1. Zarząd Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w Mikołajkach odpowiada za należyte zabezpieczenie fizyczne zasobów danych osobowych.

2. ABI zobowiązany jest przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłaszać Prezesowi Zarządu Stowarzyszenia WJM 2020 w Mikołajkach uwagi lub propozycje kontroli.

3. Obszarem, w którym przetwarzane są dane osobowe, jest siedziba Stowarzyszenia Wielkie Jeziora Mazurskie 2020 przy ulicy Kolejowej 6, 11-730 Mikołajki.

4. ABI jest odpowiedzialny za prowadzenie i uaktualnianie wykazu pomieszczeń, w których przetwarzane są dane osobowe.

5. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach, o których mowa w pkt 4, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą właściciela zasobów danych osobowych.

6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych, o którym mowa w ust. 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.

7. Przewodniczący Zarządu może zezwolić na przebywanie w pomieszczeniach, o których mowa w pkt 4, osobom sprzątającym te pomieszczenia poza godzinami pracy Stowarzyszenia bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby sprzątające podpisują oświadczenie o zachowaniu poufności.

8. Pomieszczenie, w których przetwarzane są dane osobowe, powinno być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

11. Budynek i pomieszczenie Stowarzyszenia Wielkie Jeziora Mazurskie w Mikołajkach posiadają następujące zabezpieczenia:

1) drzwi zewnętrzne (2 szt.) zaopatrzone są w zamki patentowe;
2) dostęp (klucze) do drzwi głównych wejściowych posiadają: pracownicy biura Stowarzyszenia Wielkie Jeziora Mazurskie 2020 i wskazany pracownik gospodarczy;
3) drzwi do pomieszczenia biurowego posiadają zamek patentowy,
4) dokumenty z danymi osobowymi przechowywane są w szafach na akta wyposażonych w zamki patentowe.

§ 2. Ochrona danych osobowych przetwarzanych poza obszarem przetwarzania

1. W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 1 pkt 3 należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.
2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 w Mikołajkach

§ 3. Monitorowanie ochrony zasobów danych osobowych

1. Administrator Bezpieczeństwa Informacji prowadzi:
   1) aktualny wykaz zasobów danych osobowych przetwarzanych w Stowarzyszeniu,
   2) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,
   3) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych i ich zabezpieczeń.

Załącznik nr 3 do Polityki Bezpieczeństwa

Mikołajki, dnia 02/06/2017r.

PROJEKT

Wykaz zasobów danych osobowych i systemów ich przetwarzania

Lp.	Nazwa zbioru/zasobu danych osobowych	Rodzaj przetwarzania	Lokalizacja miejsca przetwarzania	Zastosowane oprogramowanie	Rejestr ABI	Rejestr GIODO	Sposób przepływu danych pomiędzy systemami
1.	Księgowość	Papierowo, elektronicznie	Biuro Stowarzyszenia WJM 2020 ul. Kolejowa 6 11-730 Mikołajki	RAKS	Tak	Nie	brak
2.	Przedsiębiorcy, realizatorzy i beneficjenci projektów unijnych	Papierowo, elektronicznie	Biuro Stowarzyszenia WJM 2020 ul. Kolejowa 6 11-730 Mikołajki	Programy pakietu Microsoft Office	Tak	Nie	brak
3.	Wykaz zawartych umów z kontrahentami	papierowo	Biuro Stowarzyszenia WJM 2020 ul. Kolejowa 6 11-730 Mikołajki	-	Tak	Nie	brak

4	Rejestr korespondencji	papierowo	Biuro Stowarzyszenia WJM 2020 ul. Kolejowa 6 11-730 Mikołajki	-	Tak	Nie	brak
5	Rejestr uczestników projektu unijnego (nazwa projektu)	Papierowo, elektronicznie	Biuro Stowarzyszenia WJM 2020 ul. Kolejowa 6 11-730 Mikołajki	SL2014	Tak	Nie	brak

Załącznik nr 4 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

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

Do każdego programu oddzielny dokument:

1. Program SL2014
2. Program płacowy RAKS

Załącznik nr 5 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Oświadczenie osoby upoważnionej do przetwarzania danych osobowych

Oświadczam, że zapoznałem/zapoznałam się z treścią :

1) ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922),
2) rozporządzenia MSWiA z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024),
3) Polityki Bezpieczeństwa Danych Osobowych obowiązującej w Stowarzyszeniu,
4) Instrukcji Zarządzania Systemem Informatycznym obowiązującym w Stowarzyszeniu,
5) Procedur postępowania związanych z przetwarzaniem danych osobowych w Stowarzyszeniu.

Zobowiązuje się do nieujawniania informacji, z którymi zapoznałem/am się przy okazji wykonywanej pracy. W szczególności zobowiązuję się nie ujawniać:

1) danych osobowych zawartych w systemach informatycznych,
2) szczegółów technologicznych używanych w systemach informatycznych eksploatowanych Stowarzyszeniu,
3) używanego oprogramowania przeznaczonego do przetwarzania danych osobowych w Stowarzyszeniu,
4) haseł i loginów do systemów w których przetwarzane są dane osobowe,

a także nie przetwarzać danych osobowych gromadzonych w Stowarzyszeniu w sposób inny, niż dopuszczają to przepisy o ochronie danych osobowych oraz dokumentacja Stowarzyszenia.

.....	.....
(podpis pracownika)	*(podpis przełożonego)*
.....	.....
(pieczęć organizacji)	*(miejscowość i data)*

Załącznik nr 7 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

OŚWIADCZENIE

Ja niżej podpisany(a) ..... oświadczam, iż zostałem(am) poinformowana przez Stowarzyszenia Wielkie Jeziora Mazurskie 2020 o:

1) adresie siedziby stowarzyszenia, pod którym dane są zbierane i przetwarzane;
2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
4) możliwości wniesienia żądania zaprzestania przetwarzania moich danych osobowych;
5) możliwości wniesienia sprzeciwu.

.....	.....	.....
(Miejsce złożenia oświadczenia)	(Data złożenia oświadczenia)	(Numer PESEL)

.....

(Podpis osoby składającej)

Załącznik nr 6 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Porozumienie zawierane pomiędzy Zarządem Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w Mikołajkach a pracownikiem zatrudnionym przy przetwarzaniu danych osobowych, w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej

§ 1

Przewodniczący Zarządu Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w Mikołajkach zwany dalej „Administratorem Danych Osobowych", oraz ..... (*wskazać imię i nazwisko pracownika*), zwany dalej „pracownikiem", zawierają na czas trwania zatrudnienia pracownika w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 w Mikołajkach porozumienie w sprawie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej.

§ 2

Przewodniczący Zarządu Stowarzyszenia zobowiązuje się do:

1) zaznajomienia pracownika z obowiązującymi przy realizacji powierzonych mu zadań i obowiązków przepisami prawa i regulacjami wewnętrznymi, w szczególności związanymi z przetwarzaniem danych osobowych, przy wykorzystaniu sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej;
2) zapewnienia pracownikowi niezbędnego sprzętu informatycznego, w tym komputera, drukarki i urządzeń, umożliwiających komunikację dla prawidłowego i terminowego wykonywania zadań i obowiązków;
3) zapewnienia pracownikowi legalnego oprogramowania wspierającego realizację powierzonych mu zadań i obowiązków;
4) braku konsekwencji służbowych w przypadku niewywiązania się pracownika z zadań i obowiązków spowodowanego niedziałaniem lub wadliwym działaniem sprzętu informatycznego, oprogramowania lub udostępnionych zasobów, chyba że działanie takie będzie wynikiem działania pracownika;

5) akceptowania wykorzystywania w miejscu pracy przez pracownika powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych dla celów służących samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z wykonywanymi zadaniami i pełnionymi obowiązkami, pod warunkiem wcześniejszego prawidłowego i terminowego wykonania powierzonych mu zadań i obowiązków.

§ 3

Pracownik zobowiązuje się do:

1) przestrzegania obowiązujących przepisów prawa i regulacji wewnętrznych w zakresie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej podczas wykonywania swoich zadań i obowiązków, w tym w szczególności podczas przetwarzania danych osobowych;
2) wykorzystywania powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych wyłącznie dla realizacji powierzonych mu zadań i obowiązków lub dla celów służących samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z pełnionymi obowiązkami;
3) dbania o powierzony mu sprzęt informatyczny, oprogramowanie i zasoby sieciowe;
4) powstrzymania się od działań mogących mieć wpływ na bezpieczeństwo danych, w tym w szczególności od dokonywania jakichkolwiek zmian w konfiguracji powierzonego mu sprzętu informatycznego, od instalowania lub odinstalowania oprogramowania na powierzonym mu sprzęcie informatycznym oraz od wykorzystywania sprzętu lub oprogramowania do celów prywatnych, niezwiązanych w żaden sposób z wykonywanymi zadaniami i obowiązkami lub samokształceniem.

§ 4

Przewodniczący Zarządu Stowarzyszenia informuje, a pracownik przyjmuje do wiadomości, że praca sieci informatycznej, sprzętu informatycznego, łączy teleinformatycznych i telekomunikacyjnych, działanie oprogramowania, przepływ danych i informacji oraz działania wszystkich pracowników związane z tymi elementami podlegają stałemu monitoringowi w celu zapewnienia bezpieczeństwa danych.

....

(podpis ADO) *(podpis pracownika)*

Załącznik nr 8 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Wniosek do:

1) .....
.....;
2) .....
.....

(dokładna nazwa administratora danych)

2. Wnioskodawca

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

(nazwa firmy, adres, NIP, REGON, dane do korespondencji)

3. Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych jako odbiorcy danych, zgodnie z art. 7 ust. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.);

1) .....
.....;
2) .....
.....;
3) .....
.....;
4) .....
.....

4. Cel przetwarzania danych:

1) .....
.....;
2) .....
.....;
3) .....
.....

5. Nazwa zbioru, z którego mają być udostępnione dane osobowe lub informacje umożliwiające zidentyfikowanie dokumentów, w których występowały dane osobowe (*np. sygnatura akt, rok złożonych dokumentów, symbol wydziału itp.*):

1) .....
.....;
2) .....
.....;
3) .....
.....

6. Zakres wymaganych danych, jakie mają być udostępnione:

1) .....
.....;
2) .....
.....;
3) .....
.....;
4) .....
.....

7. Inne informacje umożliwiające wyszukiwanie danych w zbiorze:

1) .....
.....;
2) .....
.....;
3) .....
.....

8. Forma doręczenia udostępnianych danych osobowych:

1) .....
.....;
2) .....
.....;
3) .....
.....

9. Lista załączników do wniosku:

1) .....;
2) .....;
3) .....

Załącznik nr 9 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Stowarzyszenie Wielkie Jeziora Mazurskie 2020

Upoważnienie nr..../....

do przetwarzania danych osobowych

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922)

Upoważniam Pana/Panią:

.....

do przetwarzania danych osobowych

w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 w zakresie niezbędnym do działania *Stowarzyszenia* określonym w *Statucie Stowarzyszenie Wielkie Jeziora Mazurskie 2020.*

Dane przetwarzane są w następujących zbiorach danych:

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

Upoważnienie jest ważne na czas zatrudnienia/członkostwa w Stowarzyszeniu

Upoważnienie jest ważne do dnia.....

Upoważnienie jest ważne przez okres wykonywania zadania (jakiego – do kiedy?)

* (*niepotrzebne skreślić*)

.....

(*pieczęć i podpis osoby nadającej upoważnienie*)

Załącznik nr 10 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko komórka/jednostka organizacyjna	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia (czynności)*	Identyfikator w danym systemie informatycznym**

* Należy podać zakres upoważnienia związany z czynnościami przy przetwarzaniu danych osobowych: zbieranie danych, wprowadzanie danych drukowanie, usuwanie/niszczenie.

** Należy podać identyfikator (id, login) dla każdego systemu, do którego dana osoba ma dostęp.

Załącznik nr 11 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

Umowa powierzenia przetwarzania danych osobowych

Umowa Nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

..... z siedzibą w .....
przy ul. ....., wpisaną do rejestru przedsiębiorców prowadzonego
przez Sąd Rejonowy dla ..... w .....,
..... Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS.....
....., NIP ....., wysokość kapitału zakładowego ..... zł,
reprezentowaną przez:
....., zwaną dalej **Zleceniodawcą,**
a
..... z siedzibą w ..... przy ul. ....., wpisaną do
rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla ..... –
..... w .....,Wydział Krajowego Rejestru Sądowego pod numerem KRS:
....., o kapitale zakładowym w wysokości ..... złotych
NIP: ..... Regon: .....

reprezentowaną przez:
....., zwaną dalej **Wykonawcą,**
zwanymi łącznie „Stronami" o następującej treści:

§ 1.

1. W związku z realizacją umowy nr ..... z dnia ..... r. o ..... Zleceniodawca powierza Wykonawcy trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.), zwanej dalej „ustawą", przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych osobowych, które powierza.
3. Powierzone dane zawierają informacje o osobach fizycznych/pracownikach pracodawców lub pracodawcach będących osobami fizycznymi.
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2.

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych:
   1) imię i nazwisko,
   2) numer ewidencyjny PESEL,
   3) seria i numer dowodu osobistego,
   4) .....

2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 1 ust. 1, i w sposób zgodny z niniejszą Umową.

§ 3.

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust. 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36–39a ustawy.
2. Wykonawca oświadcza, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024):
   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony, jako wysoki,
   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
   1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia;
   2) każdym nieupoważnionym dostępie do danych osobowych;
   3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

§ 4.

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie czego Zleceniodawca, jako administrator danych osobowych, zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5.

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia .....

§ 6.

Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:

1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności o niespełnianiu wymagań określonych w § 3.

§ 7.

Wykonawca, w przypadku wygaśnięcia niniejszej Umowy niezwłocznie, ale nie później niż w terminie 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§ 8.

Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

§ 9.

W sprawach nieuregulowanych w niniejszej Umowie mają zastosowanie przepisy Kodeksu Cywilnego oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§ 10.

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11.

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

(podpis Zleceniodawcy) (podpis Wykonawcy)

Załącznik nr 12 do Polityki Bezpieczeństwa

Mikołajki, dnia .....

...../.....

RAPORT

z naruszenia bezpieczeństwa zasad ochrony danych osobowych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020

1. Data: .... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika, jeśli występuje)

3. Lokalizacja zdarzenia:

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

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

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

5. Przyczyny wystąpienia zdarzenia:

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

6. Podjęte działania:

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

7. Skutki zdarzenia:

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

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

8. Postępowanie wyjaśniające:

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

.....
(data, podpis ABI)