Zał. nr 1

Stowarzyszenie WIELKIE JEZIORA MAZURSKIE 2020

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Wersja:	0.1
Data wersji:	15.08.2018r.
Utworzony przez:	Elit Partner Sp. z o.o.
Zatwierdzony przez:	
Poziom poufności:	UŻYTEK WEWNĘTRZNY

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany
2018-08-15	0.1	Mateusz Borowski	Pierwsza wersja dokumentu

Spis treści

1. Cel, zakres i użytkownicy

Realizując postanowienia:

- art. 24 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)

wprowadza się „Politykę bezpieczeństwa danych osobowych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020"

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

Polityka Bezpieczeństwa ma zastosowanie do ochrony danych osobowych przetwarzanych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy Stowarzyszenia Wielkie Jeziora Mazurskie 2020.

Stowarzyszenie Wielkie Jeziora Mazurskie 2020 realizując postanowienia niniejszej Polityki, dokłada najwyższej staranności w celu ochrony praw i wolności osób, których dane dotyczą, a w szczególności zapewnia:

- przetwarzanie danych zgodnie z prawem, rzetelnie i w sposób przejrzysty,
- zbieranie danych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie ich dalej w sposób niezgodny z tymi celami, dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami,
- minimalizację danych, poprzez przetwarzanie danych adekwatnych, stosownych oraz ograniczonych do niezbędnych celów przetwarzania,
- realizację zasady, zgodnie z którą dane powinny być prawidłowe i w razie potrzeby uaktualniane oraz podejmowanie wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
- przechowywanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne,
- integralność i poufność danych poprzez odpowiednie zapewnienie bezpieczeństwa,

- w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych,
- realizację zasady rozliczalności poprzez wdrożenie odpowiednich procedur i zasad, pozwalających na wykazanie przestrzegania przepisów Rozporządzenia, ze szczególnym uwzględnieniem udziału w tych działaniach inspektora ochrony danych.

Politykę stosuje się:

- do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania danych w sposób inny niż zautomatyzowany, danych osobowych stanowiących część zbioru lub mających stanowić część zbioru danych,
- w celu dopasowania obowiązków do wymogów odnoszących się do ryzyka naruszenia praw i wolności osób fizycznych,
- w celu ograniczania ryzyka naruszenia praw i wolności osób fizycznych, jakie może nieść przetwarzanie danych osobowych, poprzez zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem.

Niniejsza Polityka została opracowana w celu stworzenia i utrzymania wysokiego poziomu bezpieczeństwa zbiorów danych osobowych zgodnie z wymogami Rozporządzenia rozumianego, jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań.

Ze względu na zmieniający się charakter zagrożeń, a także pojawianie się nowych, Administrator traktuje zabezpieczenie danych osobowych nie jako stan, ale jako proces wymagający ciągłego doskonalenia, modyfikowania dostosowywania rozwiązań technicznych i organizacyjnych do możliwości pojawienia się nowych kategorii niebezpieczeństw i zagrożeń.

2. Dokumenty referencyjne

- Instrukcja Zarządzania Systemami Informatycznymi w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;
- Instrukcja przechowywania archiwizacji dokumentów w ramach projektów UE

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 - Polityka Bezpieczeństwa Danych Osobowych w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;

Instrukcja – Instrukcja Zarządzania Systemami Informatycznymi w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020;

Administrator – Stowarzyszenie Wielkie Jeziora Mazurskie 2020 reprezentowane przez Zarząd, decydujący o celach i środkach przetwarzania danych osobowych;

Rozporządzenie - 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)

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

Zgoda osoby, której dane dotyczą - 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 - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

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

Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

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

Zabezpieczenie systemu informatycznego - 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, dyski 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.

Organ nadzorczy – Urząd Ochrony Danych Osobowych;

Odbiorca danych - osoba fizyczna, lub prawna, organ publiczny lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane w ramach konkretnego postępowania nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosowne do celów przetwarzania;

Właściciel aktywów – pracownik Stowarzyszenia Wielkie Jeziora Mazurskie 2020, który w ramach swoich kompetencji podejmuje decyzję o sposobie wykorzystania aktywów informacyjnych. Osoba ta jest odpowiedzialna za właściwą klasyfikację aktywów informacyjnych;

Zagrożenie - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji;

Podatność - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie;

Aktywa - wszystko, co ma wartość dla organizacji;

Właściciel ryzyka – konkretna osoba, której przypisano własność poszczególnych ryzyk, osoba odpowiedzialna za plany działań, ograniczenie prawdopodobieństwa wystąpienia ryzyka lub naprawę zmaterializowanego ryzyka. Osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zaradczych w stosunku do obszaru, którym zarządza;

Stowarzyszenie - Stowarzyszenie Wielkie Jeziora Mazurskie 2020.

4. Obszary przetwarzania danych osobowych

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

Administrator przy ustalaniu środków bezpieczeństwa wdraża odpowiednie środki bezpieczeństwa w szczególności minimalizację przetwarzanych danych osobowych, ochronę danych w fazie projektowania oraz domyślną ochronę danych osobowych. Ustalanie środków bezpieczeństwa jest ściśle związane z przeprowadzanym regularnie procesem oceny skutków dla ochrony danych

osobowych. Poszczególne formy zabezpieczeń są przedmiotem regularnych audytów w celu oceny ich skuteczności i mierzenia stopnia ich realizacji.

4.1.1. Zabezpieczenia organizacyjne

1) Została opracowana i wdrożona polityka bezpieczeństwa,
2) Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
3) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
4) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
5) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
6) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
7) 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,
8) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe,
9) Dochowuje się staranności zabezpieczenia danych przy ich gromadzeniu oraz udostępnianiu,
10) Określono postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych.

Pracownikom Stowarzyszenia zabrania się:

1) Ujawniania hasła i loginu współpracownikom oraz osobom trzecim,
2) Przechowywania haseł w miejscu widocznym bądź łatwo dostępnym dla innych osób,
3) Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
4) Udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
5) Używania programów w innym zakresie niż pozwala na to umowa licencyjna,
6) Przenoszenia oprogramowania z jednego stanowiska na inne bez wiedzy i zgody Administratora lub osoby przez niego upoważnionej,
7) Wymontowania bądź przenoszenia dysków twardych z jednego stanowiska na inne,
8) Tworzenia kopii danych na zewnętrznych nośnikach w celu wyniesienia ich poza obszar Stowarzyszenia bez zgody Administratora lub osoby przez niego upoważnionej,
9) Instalowania i używania jakichkolwiek programów komputerowych (w tym również programów do użytku prywatnego) bez wiedzy i zgody Administratora lub osoby przez niego upoważnionej,
10) Używania zewnętrznych nośników danych bez wcześniejszego sprawdzania programem antywirusowym.
11) Pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady dostępu,

12) Pozostawiania dokumentów bądź kopii dokumentów zawierających dane osobowe w drukarkach bądź kserokopiarkach,
13) Wyrzucania dokumentów zawierających dane osobowe bez uprzedniego trwałego zniszczenia,
14) Pozostawiania osób trzecich bez nadzoru w pomieszczeniach Stowarzyszenia, w których przetwarzane są dane osobowe,
15) Przekazywania danych osobowych osobom nieupoważnionym,
16) Ignorowania zapisów Polityk Ochrony.

Wymagane jest:

1) Posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2) Tworzenie haseł trudnych do odgadnięcia dla innych użytkowników oraz osób nieupoważnionych,
3) Traktowanie konta pocztowego Stowarzyszenia jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
4) Zabezpieczenie sprzętu komputerowego w tym komputerów przenośnych przed kradzieżą lub nieuprawnionym dostępem do danych.
5) Osoby przetwarzające informacje zawierające dane osobowe zobowiązane są do zachowania tajemnicy służbowej.
6) Informacji zawierających dane osobowe nie można wynosić poza teren Stowarzyszenia bez zgody Administratora.
7) Osoby przetwarzające informacje zawierające dane osobowe zobowiązane są do niezwłocznego poinformowania Administratora o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

4.1.2. Zabezpieczenia ochrony fizycznej danych osobowych

Określono obszar przetwarzania danych osobowych wraz z opisem stosowanych środków ochrony fizycznej w **załączniku nr 1 – „Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe"**.

4.1.3. 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.

4.1.4. 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. Obowiązki Zastępcy Dyrektora Biura Stowarzyszenia

1) Wydawanie, zbieranie i ewidencjonowanie oświadczeń osób zatrudnianych na podstawie, umowy o prac, umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi **załącznik nr 2 – „Oświadczenie o zachowaniu poufności"** do Polityki Bezpieczeństwa Danych Osobowych;
2) Przygotowywanie i przekazywanie do podpisu Administratorowi upoważnień do przetwarzania danych osobowych stanowiących **załącznik nr 3 – „Upoważnienie do przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych;
3) Prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, wzór ewidencji stanowi **załącznik nr 4 – „Ewidencja osób upoważnionych do przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych.
4) Zapoznawanie pracowników mających dostęp do danych osobowych z zasadami bezpieczeństwa danych osobowych podczas szkolenia stanowiskowego.
5)

6. Gromadzenie danych osobowych

Dane osobowe przetwarzane w Stowarzyszeniu 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, w stosownych przypadkach należy dokonać anonimizacji tych danych osobowych.

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

7. Obowiązek informacyjny

Pracownicy komórek organizacyjnych Stowarzyszenia, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:

1) tożsamości i danych kontaktowych Administratora;
2) celach przetwarzania danych osobowych lub prawnie uzasadnionych interesach realizowanych przez administratora;

3) informacjach o odbiorcach i kategoriach odbiorców , jeżeli istnieją;
4) okresie bądź kryteriach ustalania okresu przechowywania danych osobowych
5) prawie wglądu do treści swoich danych oraz możliwości ich sprostowania, usunięcia, ograniczenia przetwarzania lub prawie do wniesienia sprzeciwu wobec przetwarzania danych oraz o prawie do przenoszenia danych;
6) w przypadku wyrażenia zgody na przetwarzanie danych osobowych o możliwości jej cofnięcia;
7) prawie do wniesienia skargi do organu nadzorczego;
8) dobrowolności bądź wymogu ustawowym podania danych osobowych oraz o konsekwencjach niepodania danych.

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. 14 Rozporządzenia. W celu realizacji obowiązku informacyjnego stosuje się klauzule informacyjne określone w **załączniku nr 5 – „Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych.

8. Zgody na przetwarzanie danych osobowych

Jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanej danych osobowych, o której mowa w artykule 6 ust. 1 pkt a) rozporządzenia. Stowarzyszenie dba, aby zgody były wyrażane dobrowolnie oraz żeby były zrozumiałe. Stosowane oświadczenia woli w Stowarzyszeniu zostały określone w **załączniku nr 5 – „Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych.

W przypadku zbierania zgód należy poinformować osobę o możliwości jej wycofania, Stowarzyszenie nie ogranicza form wycofania zgód na przetwarzanie danych osobowych.

9. Udostępnienie danych osobowych

Administrator udostępnia dane osobowe 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.

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 bez zbędnej zwłoki w każdym razie w terminie miesiąca od otrzymania żądania .

9.1. Odmowa udostępnienia danych

Odmowa udostępnienia danych osobowych następuje na podstawie obowiązków wynikających z art. 32 dotyczących bezpieczeństwa przetwarzania danych osobowych. 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

10.1. Domyślna ochrona danych i zabezpieczenie informacji w fazie projektowania

Stowarzyszenie zarządza zmianami mającymi wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i nowych czynności przetwarzania przez Stowarzyszenie odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny skutków dla ochrony danych osobowych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub nowej czynności przetwarzania.

10.2. Obowiązki podmiotu przetwarzającego i powierzenie danych

Powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu odbywa się zgodnie z art. 28 Rozporządzenia na podstawie umowy zawartej na piśmie pomiędzy Administratorem a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

Zastępca Dyrektora Biura Stowarzyszenia przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.

W projekcie umowy należy wyspecyfikować prawa i obowiązki administratora oraz podmiotu przetwarzającego w szczególności:

1) Stosowanych środków bezpieczeństwa w szczególności zasady uwzględniania ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych
2) Działanie tylko i wyłącznie zgodnie z poleceniami administratora;
3) Zapewnienie o zachowaniu poufności i zachowania w tajemnicy danych osobowych;
4) Udzielanego wsparcia w zakresie przestrzegania przepisów o prawach osób, których dane dotyczą;
5) Kwestie usunięcia lub zwrócenia danych osobowych po zakończeniu świadczenia usługi;
6) Udostępnianie i przekazywanie informacji dla właściwej ochrony danych osobowych;
7) Reguluje kwestie podpowierzenia danych osobowych i dalszego ich przekazywania.
8) Obowiązku zgłaszania naruszeń do Administratora.

Projekt umowy jest przedkładany przez Zastępcę Dyrektora Biura Stowarzyszenia do akceptacji i podpisu Administratora. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 6 – „Umowa powierzenia przetwarzania danych osobowych – wzorzec”** do Polityki Bezpieczeństwa Danych osobowych.

11. Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia 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 oraz Zastępcę Dyrektora Biura Stowarzyszenia (ewentualnie osobę przez niego upoważnioną), 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.

Zastępca Biura Stowarzyszenia podejmuje działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia;

2) wyjaśnienie okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia,
4) umożliwienie dalszego bezpiecznego przetwarzania danych.

Dla realizacji celów określonych powyżej Zastępca Dyrektora Biura Stowarzyszenai 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 Zastępcą Dyrektora Biura Stowarzyszenia traktowana będzie, jako naruszenie obowiązków pracowniczych.

Zgodnie z art. 33 Rozporządzenia po przeprowadzonej analizie przypadku naruszenia oraz możliwych konsekwencji wystąpienia naruszenia dla praw i wolności osób fizycznych Zastępca Dyrektora Biura Stowarzyszenia 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 7 – „Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych. Zastępca Dyrektora Biura Stowarzyszenia przekazuje raport do Administratora.

11.3. Analiza przypadków naruszeń

Na podstawie raportu Administrator podejmuje decyzje czy:

1) Należy zgłosić naruszenie ochrony danych osobowych organowi nadzorczemu;
2) Należy zawiadomić osoby, których dane zostały naruszone.

Zgłoszenia oraz zawiadomienia, o których mowa powyżej winny być zrealizowane niezwłocznie nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.

Zgłoszenie do Urzędu Ochrony Danych Osobowych powinno zawierać, co najmniej:

a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wykazów danych osobowych, których dotyczy naruszenie;
b) imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) możliwe konsekwencje naruszenia ochrony danych osobowych;
d) środki zastosowane lub proponowane przez administratora w celu naprawy naruszenia ochrony danych osobowych, w tym w stosownym przypadku zminimalizowania jego ewentualnych negatywnych skutków.

12.Rejestr czynności przetwarzania

Administrator zgodnie z obowiązkiem wynikającym z art. 30 ust. 1 Rozporządzenia prowadzi wewnętrzny rejestr czynności przetwarzania stanowiący **załącznik nr 8 – „Rejestr czynności przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych. Rejestr jest udostępniany na żądanie organu nadzorczego.

13.Rejestr wszystkich kategorii czynności przetwarzania

W sytuacji gdy Stowarzyszenie staje się podmiotem przetwarzającym na polecenie innych administratorów danych, sytuacja ta jest odnotowywana w prowadzonym wewnętrznie rejestrze wszystkich kategorii czynności przetwarzania stanowiący **załącznik nr 9 – „Rejestr wszystkich kategorii czynności przetwarzania"** do Polityki Bezpieczeństwa Danych Osobowych. Rejestr prowadzony jest zgodnie z obowiązkiem wynikającym z art. 30 rozporządzenia, rejestr jest udostępniany na żądanie organu nadzorczego.

14.Ocena skutków dla ochrony danych

Celem niniejszej procedury jest zdefiniowanie metodyki oceny skutków dla ochrony danych osobowych związanymi z przetwarzaniem informacji oraz określenie akceptowalnych poziomów ryzyk, zgodnie z normą PN-ISO/IEC 27001:2014-12.

14.1. Proces

Ocena skutków dla ochrony danych osobowych wykonywane jest z użyciem Tabeli szacowania ryzyka oraz rejestru czynności przetwarzania. Identyfikacja zagrożeń i podatności jest wykonywana przez właścicieli aktywów, natomiast szacowanie konsekwencji oraz prawdopodobieństwa jest wykonywane przez właścicieli ryzyka.

14.1.1. Aktywa, podatności i zagrożenia

Pierwszym krokiem w ocenie skutków dla ochrony jest zidentyfikowanie wszystkich czynności przetwarzania będących w zakresie ochrony danych osobowych – oznacza to wszystkie operacje, które mogą wpływać na poufność, integralność i dostępność informacji w Stowarzyszeniu. Podczas identyfikacji operacji, konieczne jest także określenie ich właścicieli – osób lub jednostek organizacyjnych odpowiedzialnych za poszczególne aktywa.

Kolejnym krokiem jest identyfikacja wszystkich zagrożeń i podatności związanych z poszczególnymi aktywami. Identyfikacji zagrożeń i podatności dokonuje się z użyciem katalogów znajdujących się w Tabeli szacowania ryzyka. Poszczególne aktywa mogą być związane z więcej niż jednym zagrożeniem, a każde zagrożenie może być związane z więcej niż jedną podatnością.

14.1.2. Określanie właścicieli ryzyka

Dla każdego ryzyka należy określić właściciela ryzyka, czyli osobę lub jednostkę organizacyjną odpowiedzialną za to ryzyko. Osoba ta może być jednocześnie właścicielem aktywu.

14.1.3. Konsekwencje i prawdopodobieństwo

Gdy właściciele ryzyk zostali już określeni, należy dla każdego aktywu oraz każdej kombinacji zagrożenie-podatność oszacować liczbowo znaczenie skutków zdarzenia, w którym dana podatność została wykorzystana przez dane zagrożenie:

Skutki niewielkie	0	Utrata poufności, dostępności lub integralności nie wpływa na, zobowiązania umowne lub prawne lub jej reputację.
Skutki średnie	1	Utrata poufności, dostępności lub integralności powoduje konsekwencje oraz ma niski lub średni wpływ na zobowiązania prawne, umowne lub reputację Stowarzyszenia
Skutki znaczące	2	Utrata poufności, dostępności lub integralności ma znaczący i/lub natychmiastowy wpływ na Stowarzyszenie, jego działanie, zobowiązania prawne lub umowne i/lub jego reputację.

Po oszacowaniu skutków konieczne jest określenie prawdopodobieństwa zdarzenia, tj. prawdopodobieństwa, że dane zagrożenie wykorzysta podatność danego aktywu:

Prawdopodobieństwo niskie	0	Istniejące zabezpieczenia są silne i zapewniały dotychczas odpowiedni poziom ochrony. Nie oczekuje się w przyszłości nowych incydentów.
Prawdopodobieństwo średnie	1	Istniejące zabezpieczenia w większości przypadków zapewniały odpowiedni poziom ochrony. Nowe incydenty są możliwe, ale nie są wysoce prawdopodobne.
Prawdopodobieństwo wysokie	2	Istniejące zabezpieczenia są nieefektywne. Prawdopodobieństwo incydentów w przyszłości jest wysokie.

Po wprowadzeniu wartości skutków oraz prawdopodobieństwa do Tabeli szacowania ryzyka, poziom ryzyka jest obliczany automatycznie. Istniejące zabezpieczenia wpisuje się w ostatniej kolumnie Tabeli szacowania ryzyka.

14.2. Kryteria akceptacji ryzyka

Wynikowe wartości ryzyka 0, 1 i 2 są ryzykami akceptowalnymi, podczas gdy wartości 3 i 4 są ryzykami nieakceptowalnymi. Należy zaplanować postępowanie z ryzykami nieakceptowalnymi.

14.3. Postępowanie z ryzykiem

Postępowanie z ryzykiem planuje się z użyciem Tabeli szacowania ryzyka wzór tabeli stanowi **załącznik nr 10 – „Tabela szacowania ryzyka"** do Polityki Bezpieczeństwa Danych Osobowych. Za postępowanie z ryzykiem odpowiada Administrator

Dla każdego ryzyka oszacowanego na poziomie 3 lub 4 należy wybrać jedną lub więcej opcji postepowania z ryzykiem:

1. Wybranie zabezpieczenia;

2. Transfer ryzyka do strony trzeciej – np. poprzez ubezpieczenie ryzyka lub podpisanie innych umów (z dostawcą, partnerem)
3. Uniknięcie ryzyka poprzez zaprzestanie działań, które mogą to ryzyko powodować
4. Akceptacja ryzyka – ta opcja dopuszczalna jest jedynie wtedy, gdy wybór innej opcji postępowania z ryzykiem wiązałby się z kosztami wyższymi niż skutki finansowe incydentu związanego z tym ryzykiem.

Wyboru opcji dokonuje się w Tabeli szacowania ryzyka. Zwykle jest to opcja nr 1 – wybór jednego lub więcej zabezpieczeń. Jeśli dla danego ryzyka wybiera się więcej niż jedno zabezpieczenie, to zabezpieczenia te wymienia się kolejnych wierszach tabeli bezpośrednio pod wierszem zawierającym dane ryzyko.

14.4. Regularne przeglądy dotyczące szacowania ryzyka i postępowania z ryzykiem

Właściciele ryzyka muszą dokonywać przeglądów istniejących ryzyk, określać nowe ryzyka oraz odpowiednio aktualizować Tabelę szacowania ryzyka. Przeglądu takiego należy dokonywać co najmniej raz w roku – lub częściej w przypadku znaczących zmian organizacyjnych, zmian w stosowanych technologiach, celach przetwarzania danych osobowych.

15.Załączniki

- Załącznik 1: Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe
- Załącznik 2: Oświadczenie o zachowaniu poufności
- Załącznik 3: Upoważnienie do przetwarzania danych osobowych
- Załącznik 4: Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik 5: Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych
- Załącznik 6: Umowa powierzenia przetwarzania danych osobowych – wzorzec
- Załącznik 7: Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych
- Załącznik 8: Rejestr czynności przetwarzania danych osobowych
- Załącznik 9: Rejestr wszystkich kategorii czynności przetwarzania
- Załącznik 10: Tabela szacowania ryzyka

16.Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 15.08.2018r.

Właścicielem niniejszego dokumentu jest Administrator, 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

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 pok. 22	1	Biuro Stowarzyszenia WJM 2020	Dyrektor Biura Stowarzyszenia WJM 2020 Specjalista ds. realizacji i koordynacji projektów, Stowarzyszenie WJM 2020	Drzwi zabezpieczone zamkiem, monitoring wizyjny w Budynku

*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.

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	Właściwe zaznaczyć
Zadań i obowiązków wynikających z umowy o pracę zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu	
Zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	
Zadań wynikających z umowy praktyki zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	

*Właściwe zaznaczyć.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów [nazwa organizacji].

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 zasadach dotyczących przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa Danych Osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami rozporządzenia 2016/679 w sprawie ochrony osób fizycznych.

....

(*miejsce złożenia oświadczenia*) (*data złożenia oświadczenia*)

.....

(*podpis osoby składającej oświadczenie*)

Data wydania: XX/XX/XXXX

Upoważnienie nr XX/XX/XXXX

do przetwarzania danych osobowych

Zgodnie z przyjętymi zapisami Polityki Bezpieczeństwa Danych Osobowych oraz art. 32 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)

Upoważniam Panią/Pana:

.....

Zatrudnioną/zatrudnionego w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020

do przetwarzania danych osobowych

w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 w celach i zakresie związanym z wykonywaniem obowiązków na stanowisku:

.....

(zajmowane stanowisko)

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp. i elektronicznej, jak również w zakresie związanym z objętymi zastępstwami przez pracownika określonymi w komórce organizacyjnej.

Upoważnienie traci ważność z chwilą jego cofnięcia lub ustania stosunku umownego wiążącego upoważnionego z administratorem danych.

.....

(pieczęć i podpis osoby nadającej upoważnienie)

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

Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych

Rekrutacja (treść dodana do ogłoszeń o naborze)

Zgoda na przetwarzanie danych osobowych:

Wyrażam zgodę na przetwarzanie swoich danych osobowych (imię, nazwisko, telefon, data urodzenia, umiejętności, zainteresowania, staż pracy, wizerunek) dla potrzeb niezbędnych do realizacji procesu rekrutacji/ przyszłych rekrutacji w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020. Niniejsze oświadczenie jest zgodą w rozumieniu art. 4 pkt 11 ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Obowiązek informacyjny:
Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.
3. Twoje dane (imię, nazwisko, telefon, data urodzenia, umiejętności, zainteresowania, staż pracy, wizerunek) **będą przetwarzane** wyłącznie dla potrzeb niezbędnych do realizacji procesu rekrutacji.
4. Podstawą przetwarzania przez nas Twoich danych jest **zgoda na przetwarzanie danych osobowych**. W każdej chwili możesz wycofać udzieloną zgodę prostu pisząc do nas wiadomość lub osobiście informując osoby koordynujące proces rekrutacji.
5. Twoje dane nie będą **przekazywane** innym odbiorcom.
6. Twoje dane będziemy **przetwarzać**, nie dłużej niż przez rok czasu od momentu zakończenia procesu rekrutacji.
7. W każdej chwili **masz prawo dostępu** udzielenia informacji co do swoich danych i ich przetwarzania, ich sprostowania, usunięcia, uzyskania kopii danych.
8. Przysługuje Ci **prawo wniesienia skargi** do organu nadzorczego Urzędu Ochrony Danych Osobowych, co do przetwarzania Twoich danych osobowych
9. Podanie Twoich danych osobowych **jest nieobowiązkowe**, jednak niezbędne do właściwej oceny przy naborze na stanowisko.

Promocja i wizerunek (zgody zbierane poprzez wykorzystanie papierowych formularzy)

Zgoda na wykorzystanie wizerunku

W związku z udziałem w akcji promocyjnej prowadzonej przez Stowarzyszenie Wielkie Jeziora Mazurskie 2020, wyrażam zgodę na przetwarzanie mojego wizerunku do celów związanych z promocją ochrony środowiska.

Z komentarzem [MB1]: Jeżeli wizerunki będą zbierane dla celów w ramach prowadzonych projektów zmienić na Wojewodę

Niniejsze oświadczenie jest zezwoleniem w rozumieniu art. 81 ustawy o prawie autorskim i prawach pokrewnych (Dz.U. z 1994r. Nr 24, poz. 83).

Czytelny podpis i data: _____

Zgoda na przetwarzanie danych osobowych

Imię:

Nazwisko:

Wyrażam zgodę na przetwarzanie danych osobowych (wizerunek, imię i nazwisko) do celów związanych z promocją Stowarzyszenie Wielkie Jeziora Mazurskie 2020. Niniejsze oświadczenie jest zgodą w rozumieniu art. 4 pkt 11 ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Z komentarzem [MB2]: Jeżeli wizerunki będą zbierane dla celów w ramach prowadzonych projektów zmienić na Wojewodę

Czytelny podpis i data: _____

Obowiązek informacyjny:

Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.

Z komentarzem [MB3]: Jeżeli wizerunki będą zbierane dla celów w ramach prowadzonych projektów zmienić na Wojewodę

3. Podstawą przetwarzania przez nas Twoich danych jest **Twoja zgoda** wyrażona w sposób papierowy. W każdej chwili możesz cofnąć tę zgodę pisząc do nas wiadomość bądź przekazać tą informacje osobiście.
4. Twoje dane **będą** upublicznione co wiąże się z dostępem wielu odbiorców.
5. Twoje dane będziemy **przetwarzać tak długo**, jak długo będziesz uczestniczyć w akcjach promocyjnych, przekazanie danych wiąże się z ich upublicznieniem.
6. W każdej chwili **masz prawo dostępu** udzielenia informacji co do swoich danych i ich przetwarzania, ich sprostowania, usunięcia, uzyskania kopii danych.
7. Przysługuje Ci prawo wniesienia skargi do organu nadzorczego Urzędu Ochrony Danych Osobowych, co do przetwarzania Twoich danych osobowych.
8. Podanie Twoich danych osobowych jest **dobrowolne** .

Szkolenia i wydarzenia (treść dodana do ogłoszeń o naborze)

Obowiązek informacyjny:
Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.
3. Podstawą przetwarzania przez nas Twoich danych jest **prawnie uzasadniony interes** Stowarzyszenia Wielkie Jeziora Mazurskie 2020.
4. Twoje dane będą **przekazywane** innym odbiorcom uczestniczącym w organizacji szkolenia.
5. Twoje dane będziemy **przetwarzać** nie dłużej niż przez okres 5 lat od zakończenia ostatniego szkolenia bądź wydarzenia, w którym bierzesz udział.
6. W każdej chwili **masz prawo dostępu** udzielenia informacji co do swoich danych i ich przetwarzania, ich sprostowania, usunięcia, uzyskania kopii danych.
7. Przysługuje Ci prawo wniesienia skargi do organu nadzorczego Urzędu Ochrony Danych Osobowych, co do przetwarzania Twoich danych osobowych
8. Podanie Twoich danych osobowych jest **obowiązkowe**, dla udziału w wydarzeniu.

Z komentarzem [MB4]: Jeżeli szkolenia realizowane są dla celów w ramach prowadzonych projektów zmienić na Wojewodę

Umowy o dzieło, umowy zlecenie (treść dodana do kwestionariuszy osobowych)

Obowiązek informacyjny:
Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.
3. Podstawą przetwarzania przez nas Twoich danych jest **umowa** zawarta z Stowarzyszeniem Wielkie Jeziora Mazurskie 2020.
4. Twoje dane **będą przekazywane** bankom.
5. Twoje dane będziemy **przetwarzać** nie dłużej niż przez okres 5 lat.
6. W każdej chwili **masz prawo dostępu** udzielenia informacji co do swoich danych i ich przetwarzania, ich sprostowania, uzyskania kopii danych.
7. Przysługuje Ci prawo wniesienia skargi do organu nadzorczego Urzędu Ochrony Danych Osobowych, co do przetwarzania Twoich danych osobowych
8. Podanie Twoich danych osobowych jest **obowiązkowe**, dla celów realizacji umowy.

Umowy o prace (treść dodana do kwestionariuszy osobowych)

Obowiązek informacyjny:
Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.
3. Podstawą przetwarzania przez nas Twoich danych jest **przepis prawa**: ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.
4. Twoje dane **będą** przekazywane firmom ubezpieczeniowym, bankom.
5. Twoje dane będziemy **przetwarzać** nie dłużej niż przez okres 50 lat.
6. W każdej chwili masz **prawo do uzyskania kopii danych lub dostępu** do swoich danych, ich sprostowania, ograniczenia lub do wniesienia sprzeciwu wobec przetwarzania.

7. Przysługuje Ci prawo wniesienia skargi do organu nadzorczego Urzędu Ochrony Danych Osobowych, co do przetwarzania Twoich danych osobowych
8. Podanie Twoich danych osobowych jest **obowiązkowe**, dla celów dopełnienia obowiązków wynikających z przepisów prawa.

SIWZ (treść dodana do zamówień i zapytań ofertowych)

Obowiązek informacyjny:
Stosownie do art. 13 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 (RODO) informujemy, że:

1. **Administratorem** podanych przez Ciebie danych będzie Stowarzyszenie Wielkie Jeziora Mazurskie 2020, z siedzibą przy ul. Kolejowa 6, 11-730 Mikołajki.
2. W sprawie danych osobowych możesz **kontaktować się** z nami pod numerem fax: 087 421 61 46 lub osobiście.
3. Twoje dane **będą przetwarzane** wyłącznie dla potrzeb niezbędnych do realizacji procesu udzielenia realizacji zamówienia publicznego/zapytania ofertowego.
4. Podstawą przetwarzania przez nas Twoich danych jest **przepis prawa**: ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych.
5. Twoje dane **będą przekazywane** firmom specjalizującym się w doradztwie w zakresie zamówień publicznych.
6. Twoje dane będziemy **przetwarzać** nie dłużej niż przez cztery lata od dnia zakończenia postępowania o udzielenie zamówienia.,
7. W każdej chwili masz **prawo do uzyskania kopii danych lub dostępu** do swoich danych, ich sprostowania, ograniczenia lub do wniesienia sprzeciwu wobec przetwarzania.
8. Przysługuje Ci prawo wniesienia skargi do organu nadzorczego, co do przetwarzania Twoich danych osobowych
9. Podanie Twoich danych osobowych jest **obowiązkowe**, dla celów dopełnienia obowiązków wynikających z przepisów prawa.

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu ..... w ..... pomiędzy:
..... z siedzibą w ....., przy ul. ....., NIP .....,
reprezentowaną przez:

1. ..... - .....,

zwaną dalej **Zleceniodawcą**

a

..... z siedzibą w ....., przy ul. ....., NIP .....,
reprezentowaną przez:

2. ..... - .....,

zwaną dalej **Zleceniobiorcą,**

zwanymi dalej również łącznie "**Stronami**" lub każda z osobna "**Stroną**".

§ 1

1. Zleceniodawca oświadcza, że jest administratorem danych osobowych w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. 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 "Rozporządzenie" lub "RODO") w stosunku do danych powierzonych Zleceniobiorcy.
2. Zleceniobiorca oświadcza, że może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Zleceniodawcy, co dotyczy również przekazywania danych do państwa trzeciego lub organizacji międzynarodowej.
3. Ust. 2 nie stosuje się, jeżeli obowiązek przetwarzania danych osobowych nakładają na Zleceniobiorcę przepisy prawa. W takiej sytuacji informuje on Zleceniodawcę przed rozpoczęciem przetwarzania o tym obowiązku, chyba że przepisy te zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 2

1. Zleceniobiorca może przetwarzać dane osobowe wyłącznie w celu [UZUPELNIĆ], a także wykonania pozostałych operacji przetwarzania danych osobowych wskazanych w niniejszej Umowie, nieobjętych wprost przedmiotem usług.
2. Zleceniobiorca może przetwarzać dane osobowe następujących kategorii osób: [UZUPELNIĆ], które Zleceniodawca przetwarza jako administrator.
3. Zleceniobiorca może przetwarzać następujące kategorie danych osobowych: [UZUPELNIĆ],

§ 3

1. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy przez Zleceniobiorcę odnośnie zobowiązań, o których mowa w niniejszej Umowie. Warunkiem

przeprowadzenia kontroli jest zawiadomienie Zleceniobiorcy w terminie nie krótszym niż 7 dni przed planowanym terminem jej przeprowadzenia.

2. Zleceniobiorca udostępni Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia nałożonych na niego niniejszą Umową zobowiązań.
3. Zleceniobiorca umożliwia Zleceniodawcy lub audytorowi przez niego upoważnionemu przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
4. Uprawnienia określone w powyższych ustępach niniejszego paragrafu przysługują Zleceniodawcy odpowiednio w stosunku do Podwykonawców, o których mowa w § 7 ust. 1 niniejszej Umowy, w przypadku powierzenia przez Zleceniobiorcę przetwarzania danych Podwykonawcom, zgodnie z § 7 Umowy.
5. W związku z obowiązkiem określonym w ustępach powyżej, Zleceniobiorca niezwłocznie informuje Zleceniodawcę, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów powszechnie obowiązujących, które dotyczą ochrony danych osobowych.

§ 4

1. Zleceniobiorca zobowiązuje się do wdrożenia ze skutkiem na dzień 25 maja 2018 r. odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa przetwarzania danych uwzględniający stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
2. Środki, o których mowa w ustępie poprzednim, to między innymi w stosownych przypadkach:
   a) pseudonimizacja i szyfrowanie danych osobowych;
   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;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 5

1. Biorąc pod uwagę charakter przetwarzania danych, Zleceniobiorca zobowiązuje się od dnia stosowania Rozporządzenia do pomocy Zleceniodawcy, poprzez odpowiednie środki techniczne i organizacyjne, w wywiązaniu się z obowiązku odpowiedzi na żądania osoby, której dane dotyczą, w szczególności w zakresie wykonywania jej praw określonych w Rozdziale III Rozporządzenia.
2. Biorąc pod uwagę charakter przetwarzania danych oraz posiadane informacje, Zleceniobiorca zobowiązuje się do pomocy Zleceniodawcy w zakresie wywiązywania się z obowiązków wymienionych w art. 32-34 w Sekcji 2 i art. 35-36 Sekcji 3 Rozdziału IV Rozporządzenia, tj. w szczególności dotyczących wdrażania odpowiednich środków technicznych i organizacyjnych, zgłaszania naruszenia ochrony danych osobowych przez Zleceniodawcę organowi nadzorczemu oraz osobie, której dane dotyczą, co oznacza udzielenie Zleceniodawcy na każde jego żądanie i we wskazanym przez niego terminie, wszelkich wyjaśnień i innych form wsparcia, w tym informacji o stanie faktycznym, które pomogą Zleceniodawcy w spełnieniu jego obowiązków wynikających z RODO, o których mowa.

§ 6

1. Zleceniobiorca zobowiązuje się do prowadzenia rejestru wszystkich kategorii czynności przetwarzania danych osobowych (dalej "Rejestr") dokonywanych w imieniu Zleceniodawcy.
2. Rejestr zawiera następujące informacje:
   a) imię i nazwisko / nazwa i dane kontaktowe Zleceniobiorcy oraz Zleceniodawcy, a także ich przedstawicieli, jeżeli ma to zastosowanie zgodnie z RODO oraz inspektora ochrony danych, jeśli został wyznaczony;
   b) kategorie przetwarzań dokonywanych w imieniu Zleceniodawcy;
   c) ogólny opis środków technicznych i organizacyjnych mających na celu zabezpieczenie powierzonych danych osobowych;
   d) informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz nazwy tych państw lub podmiotów, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń.

§ 7

1. Zleceniodawca wyraża zgodę, aby Zleceniobiorca powierzył dalej przetwarzanie danych osobowych (dalej "Podpowierzenie") i wykonywanie zadań wynikających z Umowy podmiotowi trzeciemu (dalej "Podwykonawca"), pod warunkiem, że:
   a) Zleceniobiorca powiadomi uprzednio Zleceniodawcę, mailem lub w formie pisemnej, o swoim zamiarze Podpowierzenia;
   b) Zleceniodawca zachowuje prawo sprzeciwu wobec zamiaru Podpowierzenia lub zmiany jego warunków przez Zleceniobiorcę;
   c) zakres i cel Podpowierzenia nie będzie szerszy niż wynikający z Umowy;
   d) przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Zleceniodawcy zostaną zachowane w umowie Podpowierzenia odpowiednio do warunków, opisanych w niniejszej Umowie;
   e) Podpowierzenie będzie niezbędne dla realizacji celów związanych z procesami lub projektami wynikającymi z Umowy;
   f) Podpowierzenie nie naruszy interesów Zleceniodawcy;
   g) umowa Podpowierzenia zostanie zawarta z Podwykonawcą na piśmie, zgodnie z obowiązującymi przepisami dotyczącymi powierzania przetwarzania danych osobowych z

zastrzeżeniem, że wszelkie obowiązki Zleceniobiorcy, wynikające z niniejszej Umowy, Zleceniobiorca zastosuje odpowiednio do Podwykonawcy w umowie Podpowierzenia;

h) Podwykonawca spełnia obowiązki wynikające z Rozporządzenia, nakładane bezpośrednio na podmiot przetwarzający w rozumieniu Rozporządzenia, w tym w szczególności obowiązek prowadzenia rejestru czynności przetwarzania oraz wdrożenia środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych, o których mowa w Rozporządzeniu.

2. Zleceniobiorca w umowie Podpowierzenia zobowiąże Podwykonawców do przestrzegania przy przetwarzaniu powierzonych danych obowiązków dotyczących ochrony danych na poziomie, co najmniej określonym w niniejszej Umowie oraz Rozporządzeniu.
3. Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków określonych w niniejszej Umowie lub RODO, pełna odpowiedzialność wobec Zleceniodawcy za wypełnienie tych obowiązków spoczywa na Zleceniobiorcy.

§ 8

1. Zleceniobiorca oświadcza, że każda osoba (np. pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych, inne osoby pracujące na rzecz Zleceniobiorcy), która zostanie dopuszczona do przetwarzania powierzonych przez Zleceniodawcę danych osobowych zostanie zobowiązana do zachowania tych danych w tajemnicy. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych. Do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia zobowiązany jest także Zleceniobiorca, a samo zobowiązanie obejmuje podmioty, wymienione w niniejszym ustępie bezterminowo, tj. także po zakończeniu obowiązywania niniejszej Umowy. Postanowienia dotyczące zachowania tajemnicy, o której mowa w niniejszym ustępie, Zleceniobiorca ma obowiązek stosować odpowiednio także wobec swoich Podwykonawców i osób dopuszczonych przez Podwykonawców do przetwarzania danych osobowych.
2. Zleceniobiorca oświadcza, że każda osoba mająca dostęp do danych osobowych będzie je przetwarzała wyłącznie na polecenie Zleceniodawcy, chyba że obowiązek taki wynika z przepisów prawa.
3. Zleceniobiorca po zakończeniu realizacji usług, o których mowa w §2 ust. 1 Umowy zobowiązany jest do niezwłocznego zwrotu powierzonych mu danych oraz do usunięcia wszystkich ich istniejących kopii, sporządzonych na potrzeby bieżącej pracy, bądź na wyraźne żądanie Zleceniobiorcy - dokonać usunięcia powierzonych danych osobowych, zamiast ich zwrotu, chyba, że przepisy prawa nakazują przechowywanie danych osobowych. Na każde życzenie Zleceniodawcy, Zleceniobiorca ma obowiązek przedstawić w terminie 14 dni pisemny protokół potwierdzający fakt zniszczenia danych osobowych. Sposób zakończenia przetwarzania danych osobowych po sfinalizowaniu realizacji usług na rzecz Zleceniodawcy, opisany w niniejszym ustępie, Zleceniobiorca powinien wskazać odpowiednio swoim Podwykonawcom, w przypadku Podpowierzenia. Czas trwania przetwarzania danych osobowych w imieniu Zleceniodawcy przez Zleceniobiorcę (oraz odpowiednio - Podwykonawców) trwa do dnia zrealizowania obowiązku zwrotu lub usunięcia danych, o którym mowa w zdaniu pierwszym.

§ 9

1. Zleceniobiorca oświadcza, że w razie stwierdzenia naruszenia ochrony danych osobowych niezwłocznie, jednak nie później niż w terminie 48 godzin od wykrycia naruszenia, poinformuje o tym Zleceniodawcę.
2. Zgłoszenie, o którym mowa w ust. 1 musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez Zleceniobiorcę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. W celu realizacji obowiązków, o których mowa w ust. 1 i 2 powyżej, Zleceniobiorca jest zobowiązany do dokumentowania wszelkich okoliczności i zebrania wszelkich dowodów, które pomogą Zleceniodawcy wyjaśnić szczegóły naruszenia, w tym jego charakter, skalę, skutki, czas zdarzenia, osoby odpowiedzialne, osoby poszkodowane.

§ 10

1. Zleceniobiorca odpowiada za szkody majątkowe lub niemajątkowe jakie powstały wobec Zleceniodawcy lub osób trzecich w wyniku przetwarzania danych osobowych niezgodnego z Umową lub obowiązkami nałożonymi przez Rozporządzenie, a także inne powszechnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych bezpośrednio na Zleceniobiorcę oraz w wyniku działania poza zgodnymi z prawem instrukcjami Zleceniodawcy lub wbrew tym instrukcjom.
2. Zleceniodawca odpowiada za szkody majątkowe lub niemajątkowe, jakie powstały wobec osób trzecich w wyniku przetwarzania danych naruszającego Rozporządzenie lub inne przepisy dotyczące ochrony danych osobowych.
3. Strony są zwolnione z odpowiedzialności wynikającej z ust. 1 i 2, jeżeli udowodnią, że zdarzenie, które doprowadziło do powstania szkody, jest przez nie niezawinione.
4. Jeżeli w tym samym przetwarzaniu biorą udział obie Strony i są odpowiedzialne za szkodę spowodowaną przetwarzaniem zgodnie z ust. 1 i ust. 2, ponoszą one odpowiedzialność solidarną.
5. Strona, która zapłaciła odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od drugiej Strony, która uczestniczyła w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi odpowiedzialność, zgodnie z warunkami określonymi w ust. 1 i ust. 2.
6. Zleceniobiorca ponosi odpowiedzialność za działania lub zaniechania Podwykonawcy, dotyczące przetwarzania powierzonych danych osobowych, jak za działania lub zaniechania własne, przez co postanowienia dotyczące odpowiedzialności Zleceniobiorcy na warunkach opisanych powyżej obejmują także odpowiedzialność Zleceniobiorcy za działania lub zaniechania jego Podwykonawców.

§ 11

1. Strony oświadczają, że zawierają niniejszą Umowę na czas ..... *(wskazać czy na czas określony - wówczas od ... do ... albo na czas nieokreślony)*, przy czym termin jej wypowiedzenia wynosi ..... *(wskazać właściwy)*
2. Zleceniodawca ma prawo wypowiedzieć Umowę w trybie natychmiastowym, gdy Zleceniobiorca:

a) wykorzystuje dane osobowe w sposób niezgodny z Umową, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonych przez Zleceniodawcę terminie nie usunie wskazanych naruszeń,
b) nie zaprzestanie niewłaściwego przetwarzania danych osobowych, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonych przez Zleceniodawcę terminie nie usunie wskazanych naruszeń.

§ 12

1. Na wniosek Zleceniodawcy, treść umowy powierzenia podlega zmianom wynikającym z aktualnych przepisów o ochronie danych osobowych, przy czym wszelkie zmiany i uzupełnienia postanowień Umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy kodeksu cywilnego, a od oraz Rozporządzenia.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
4. Umowa wchodzi w życie z dniem podpisania.
5. Zgodną wolą Stron jest uregulowanie aktualnych warunków powierzenia przetwarzania danych osobowych. W momencie wejścia w życie niniejszej Umowy jej postanowienia zastępują wszelkie dotychczasowe ustalenia Stron, zawarte w umowie lub umowach powierzenia, sporządzonych w oparciu o art. 31 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych, dotyczące powierzenia przetwarzania danych osobowych, o których mowa w niniejszej Umowie.

Zleceniodawca **Zleceniobiorca**

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych

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 Z-cy Dyrektora Biura)

Rejestr czynności przetwarzania danych wymagany na podstawie art. 30 ust. 1 RODO

LP.	1 Nazwa czynności przetwarzania	3 Cel czynności	4 Kategoria osób	5 Kategorie danych	6 Podstawa prawna	7 Źródło danych	8 Planowany termin usunięcia danych	9 Planowane zabezpieczenia	10 Odbiorcy lub kategorie odbiorców	11 Odbiorcy w państwie trzecim lub organizacji międzynarodowej	12 Nazwa systemu lub oprogramowania	13 Opisy wdrożonych technicznych i organizacyjnych środków bezpieczeństwa	14 DPIA (jeśli tak, lokalizacja raportu)	15 Transfer do kraju trzeciego lub organizacji międzynarodowej	16 Inne informacje
1.	Rekrutacja pracowników	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Zgoda osób, których dane dotyczą	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Nie dotyczy	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
2.	Prowadzenie rejestru pracowników, akt pracowniczych (w tym stażystów) i ewidencji czasu ich pracy	Prowadzenie ewidencji pracowników zgodnie z Kodeksem pracy	Pracownicy pomocniczy (recepcjonści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz lekarze	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), orzeczenia o stanie zdrowia, orzeczenia o niekaralności, dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy	• Umowa o pracę • Przepis prawa Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 z ind. 1 w związku z art. 94 pkt 9a i 9b	Pracownik	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe, AGA	Płatnik (system ZUS), e-Puap - transfer danych do Urzędu Skarbowego,interfejs bankowy dla płatności elektronicznych,	Zamykane szafy w pomieszczenniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
3.	Zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach	Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Pracownicy pomocniczy (recepcjonści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz lekarze	Dane identyfikacyjne, dane adresowe, dane o Oddziale Kasy Chorych oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15b - zgłoszenie opieki nad innym członkiem rodziny	• Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Płatnik (system ZUS), e-Puap - transfer danych do Urzędu Skarbowego,interfejs bankowy dla płatności elektronicznych, m	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
4.	Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Pracownicy pomocniczy (recepcjonści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz lekarze	Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.), numery kont dla przelewów bankowych pracownika	Umowa o pracę. Przepis prawa. • Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) Dział III Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	Bankl, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Płatnik (system ZUS), e-Puap - transfer danych do Urzędu Skarbowego,interfejs bankowy dla płatności elektronicznych,	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
5.	Księgowość i rachunkowość	Prowadzenie księgowości i rachunkowości	Pracownicy, kontrahenci, klienci	Dane identyfikacyjne, dane teleadresowe, dane finansowe	Przepisy prawa: Ustawa z dnia 29.09.1994 r. o rachunkowości	Pracownik, kontrahent, klient	5 lat dla dowodów księgowych	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	RAKS	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
6.	Zamówienia publiczne i zapytania ofertowe	zawarcie umowy na realizację zamówienia publicznego na zlecenie wnioskodawcy	strona umowy, oferent	Imię, nazwisko, nazwa, adres zamieszkania, adres siedziby, nr telefonu, email	ustawa z dnia 29 stycznia 2004 r. Prawo zamowień publicznych, inne akty wykonawcze wydane na podstawie ustawy Pzp,	Bezpośrednio od osób, których dane dotyczą	dokumenty przechowywane w przedziale czasowym od 5 do 10 lat	nie dotyczy	nie dotyczy	Dane nie są przekazywane innym podmiotom	nie dotyczy	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	nie dotyczy
7.	Ewidencja pism przychodzących i wychodzących	opracowywanie dokumentów przychodzących i wychodzących	kontrahenci	dane osobowe pochodzące z dokumentów przychodzących i wychodzących	Usprawiedliwiony interes administratora	Bezpośrednio od osób, których dane dotyczą	5 lat od zakończenia sprawy	nie dotyczy	nie dotyczy	Dane nie są przekazywane innym podmiotom	nie dotyczy	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	nie dotyczy

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	Stowarzyszenie Wielkie Jeziora Mazurskie 2020
Adres	ul. Kolejowa 6, 11-730 Mikołajki
Email	
Fax	087 421 61 46

Inspektor Ochrony Danych (jeśli powołano)	
Imię i Nazwisko	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 2 RODO

	1	2	3	4	5	6	7	8	9	10	11
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1 2 3 4	Beneficjent Regionanlego Programu Operacyjnego Województwa Warmińsko-Mazurkisego na lata 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Społecznego - aplikowanie o środki unijne i realizacji Projektu, w szczególności potwierdzania kwalifikowalności wydatków, udzielania wsparcia uczestnikom Projektu, zarzadzania, ewaluacji, monitoringu, kontroli, audytu, audytu, sprawozdawczości oraz działan informacyjno-promocyjnych (podniesienie jakości ofert edukacyjnej ukierunkowanej na rozwój kompetencji klcuzowych uczniów z obszaru Krainy Wielkich Jezior Mazurskich: Powiat Giżycki - II LO)	• Środki zabezpieczające zgodnie z art. 32 RODO; • Wydawanie upoważnień do przetwarzania danych osobowych zgodnie z zał 5 do Umowy. • Prowadzenie i przekazywanie wykazu podmiotów, którym powierzono przetwarzanie danych osobowych (szczegółowe procedury znajdują się w polityce bezpieczeństwa)	Województwo Warmińsko-Mazurskie reprezentokwane przez Zarząd Województwa Warmińsko-Mazurskiego z siedzibą w Olsztynie przy ul. Emilii Plater 1, 10-562 Olsztyn	Nie dotyczy	Nie dotyczy	Inspektor Ochrony Danych: Paweł Żywicki 10-447 Olsztyn, ul. Głowackiego 17, pok. nr 8 tel. (89) 521 94 39	5 lat od daty płatności końcowej na rzecz Beneficjenta	Nie dotyczy	Nie dotyczy		

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	Stowarzyszenie Wielkie Jeziora Mazurskie 2020
Adres	ul. Kolejowa 6, 11-730 Mikołajki
Email	
Fax	087 421 61 46

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

Zał. 10 Tabela szacowania ryzyka

szacowanie przeprowadzono od [data rozpoczecia] do [data zakończenia]

Lp.	Nazwa czynności przetwarzania (operacje zawarte w rejestrze czynności "Tak")	Właściciel czynności	Zagrożenie	Podatność	Właściciel ryzyka	Skutek	Prawdopodobieństwo	Ryzyko	Istniejące zabezpieczenia
									-
									-
									-
									-
