Zał. Nr 1

Stowarzyszenie WIELKIE JEZIORA MAZURSKIE 2020

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

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

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;

Za nadanie uprawnień w systemie informatycznym odpowiada właściwy Administrator Systemu. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.

W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, Administrator Systemu dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do ewidencji osób upoważnionych do przetwarzania danych osobowych.

Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.

Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.

Administrator Systemu przekazuje użytkownikowi identyfikator i hasło.

Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

5. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.

Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.

Nowe hasło jest przekazywane użytkownikowi przez Administratora Systemu.

Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.

Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:

1) posiadać długość co najmniej 8 znaków,
2) zawierać litery małe i duże,
3) zawierać cyfry lub znaki specjalne.

Hasło w systemach przetwarzających danych osobowych jest zmieniane przez użytkownika nie rzadziej, niż co 90 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.

Użytkownik zobowiązany jest do:

1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,

Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest właściwy Administrator Systemu.

Kopie zapasowe systemów przetwarzających dane osobowe są realizowane w formie pełnych kopii przetwarzanych baz danych na nośniki wbudowane w sprzęt na którym przetwarzane są dane. Kopie realizowane są co najmniej raz w tygodniu.

Utworzone kopie zapasowe podlegają okresowej weryfikacji ze względu na sprawdzenie możliwości odczytu danych.

Administrator Systemu określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.

8. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
2) przenośnych nośnikach elektronicznych.

Dane przechowywane są na nośnikach jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane.

Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.

Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych.

W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w Stowarzyszeniu. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada właściwy Administrator Systemu.

Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy określającej obowiązki podmiotu przetwarzającego, o których mowa w art. 28 Rozporządzenia,
2) zagwarantowania poufności danych przez usługodawcę,
3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez Administratora Systemu lub upoważnionego przez niego pracownika Stowarzyszenia,
4) udokumentowania faktu zniszczenia nośników protokołem.

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

11.Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 10.08.2018r.

Właścicielem niniejszego dokumentu jest Administrator, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu.

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

Katalog podatności

Poniżej znajduje się lista podatności.
Lista ta nie jest ostateczna. Każda organizacja może dodać podatności specyficzne dla jej funkcjonowania i otoczenia.

brak dezaktywacji kont użytkowników po zakończeniu stosunku pracy
brak dowodów wysłania lub odebrania wiadomości
brak kontroli danych wejściowych i wyjściowych
brak lub słaba kontrola wewnętrzna
brak ochrony systemów przed nieautoryzowanym dostępem
brak separacji środowiska testowego i produkcyjnego
brak walidacji przetwarzanych danych
brak zmian domyślnie generowanych kont i haseł użytkowników
dostęp do systemów po godzinach pracy
dostępność informacji dla nieautoryzowanych użytkowników
dostępność kluczy kryptograficznych dla nieautoryzowanych osób
lokalizacja wrażliwa na katastrofy naturalne
lokalizacja wrażliwa na wyciek wody
nadmierna zależność od jednego urządzenia/systemu
nadmierne uprawnienia
nieaktualne bazy danych oprogramowania zabezpieczającego przed złośliwym kodem (np. antywirusowego)
nieautoryzowane umieszczenie okablowania
niechronione połączenia z sieciami publicznymi
niekontrolowane kopiowanie
niekontrolowane pobieranie z internetu
niekontrolowane użycie systemów przetwarzania informacji
nieodpowiedni nadzór nad dostawcami zewnętrznymi
nieodpowiedni nadzór nad działaniami pracowników
nieodpowiedni podział odpowiedzialności
nieodpowiedni poziom wiedzy i/lub świadomości pracowników
nieodpowiednia obsługa
nieodpowiednie uprawnienia użytkowników
nieodpowiednie zarządzanie pojemnością/przepustowością
nieodpowiednie zarządzanie siecią
nieodpowiednie zarządzanie zmianami
nieprecyzyjnie zdefiniowane wymagania dla produkcji oprogramowania
nieprecyzyjnie zdefiniowane zasady kontroli dostępu
nieprecyzyjnie zdefiniowane zasady ochrony kryptograficznej
nieprecyzyjnie zdefiniowane zasady organizacyjne
nieprecyzyjnie zdefiniowane zasady pracy na zewnątrz
nieprecyzyjnie zdefiniowany poziom poufności
nieudokumentowane oprogramowanie
niezmotywowani lub niezadowoleni pracownicy
pozbycie się nośników informacji bez skasowania danych
sieci dostępne dla osób nieautoryzowanych
skomplikowany interfejs użytkownika
słabe hasła
słaby wybór danych testowych

Kategorie aktywów

Poniżej wymieniono przykłady aktywów informacyjnych, które mogą istnieć w organizacji.
Lista ta nie jest ostateczna. Każda organizacja musi stworzyć swoją własną listę aktywów istotnych dla bezpieczeństwa informacji.

Ludzie

- inni pracownicy
- kierownictwo średniego szczebla
- najwyższe kierownictwo (członkowie zarządu, członkowie rady nadzorczej, kierownicy jednostek)
- osoby z zewnątrz odwiedzające organizację
- pracownicy - eksperci (np. administratorzy systemów, projektanci, eksperci bezpieczeństwa itd.)
- zewnętrzni pracownicy niepełnoetatowi

Aplikacje i bazy danych

- bazy danych
- licencjonowane oprogramowanie aplikacyjne
- oprogramowanie darmowe (freeware, shareware)
- oprogramowanie systemowe
- różne oprogramowanie narzędziowe

Dokumentacja (w formie papierowej lub elektronicznej)

- decyzje
- dokumentacja sprzętu i wyposażenia
- dokumentacja szkoleniowa
- dokumenty i zapisy księgowe
- dokumenty pracownicze
- dokumenty wewnętrzne
- dzienniki
- kontrakty
- korespondencja z klientami i partnerami
- plany
- podręczniki
- potwierdzenia odbioru
- raporty
- rejestry
- standardy

IT, telekomunikacja oraz inny sprzęt i wyposażenie

- alarmy
- CD instalacyjne
- centrale telefoniczne
- drukarki
- faksy
- generatory prądu
- kable zasilające
- karty i czytniki kart
- klimatyzacja

Katalog zagrożeń

Poniżej znajduje się przykładowa lista zagrożeń. Lista ta nie jest kompletna. Każda organizacja może dodać tu zagrożenia specyficzne dla jej funkcjonowania.

atak bombowy
atak terrorystyczny
awaria łącz telekomunikacyjnych
awaria sprzętu
błąd użytkownika
błędy aplikacji
błędy obsługi
defraudacja
inne katastrofy naturalne
inne katastrofy spowodowane przez człowieka
inżynieria społeczna
kradzież
nadużycie narzędzi audytowych
nadużycie systemów przetwarzania informacji
nieautoryzowana instalacja oprogramowania
nieautoryzowana zmiana zapisów
nieautoryzowane użycie materiałów licencjonowanych
nieautoryzowane użycie oprogramowania
nieautoryzowany dostęp do sieci
nieautoryzowany dostęp do systemu przetwarzania informacji
nieautoryzowany dostęp fizyczny
oszustwo
piorun
podsłuch
podszycie się
powódź
pożar
przechwycenie informacji
przerwa w dostawie energii elektrycznej
przypadkowa zmiana danych w systemie przetwarzania informacji
sfałszowanie zapisów
strajk
szkody spowodowane działaniem strony trzeciej
szkody spowodowane testami penetracyjnymi
szpiegostwo przemysłowe
ujawnienie haseł
uruchomienie nieautoryzowanego lub nieprzetestowanego kodu
utrata usług wsparcia (np. technicznego)
wandalizm
wyciek/ujawnienie informacji
zagrożenie atakiem bombowym
zanieczyszczenie środowiska
złamanie kontraktu
złamanie prawa
złośliwy kod
zniszczenie zapisów
zużycie nośników informacji

Wykaz podmiotów przetwarzających, którym powierzono przetwarzanie danych osobowych

Lp.	Nazwa podmiotu przetwarzającego	Kategorie przetwarzań	Rodzaj i numer umowy	Komórka organizacyjna współpracująca z podmiotem	Uwagi
1.					

ElitPartner

Instrukcja Postępowania z Dokumentacją RODO

Dziękujemy za zaufanie i skorzystanie z naszych usług

Aby łatwiej było Ci zacząć pracę z wdrożeniem dokumentacji RODO, zapoznaj się z poniższymi instrukcjami i wskazówkami dalszego postępowania:

1) Dokumenty zostały przygotowane w **wersji edytowalnej**, oznacza to że w ramach udzielonej licencji można **zmieniać treści** i **poprawiać** przygotowane zapisy według uznania Klienta.
2) Należy sukcesywnie wydać **upoważnienia** do przetwarzania danych osobowych dla pracowników. Przy wydawaniu upoważnień pracownicy powinni podpisać **oświadczenia** o zachowaniu poufności i zapoznaniu się z wewnętrznymi procedurami. Po wydaniu upoważnień należy uzupełnić **ewidencję osób upoważnionych do przetwarzania danych.** Dokumenty te stanowią załącznik do Polityki Bezpieczeństwa Danych Osobowych.
3) Zrealizuj **obowiązek informacyjny** i zbieraj **zgody na przetwarzanie danych osobowych**, przygotowaliśmy wzorce klauzul do zastosowania znajdujące się w załączniku Oświadczenie ob. Informacyjny.
4) Zwracamy również uwagę na podpisywanie **umów powierzenia przetwarzania** danych osobowych z podmiotami działającymi na danych osobowych na zlecenie Klienta. Podpisywane umowy i zapisy dot. powierzenia przetwarzania danych osobowych w umowach głównych odnotuj w **rejestrze powierzeń**. Wzór umowy i rejestru zostały przygotowane jako załączniki do Polityki Bezpieczeństwa Danych Osobowych.
5) Jeżeli pojawia się sytuacja, że Twoja organizacja w roli **podmiotu przetwarzającego** podpisana została w tym zakresie umowa powierzenia wypełnij **rejestr wszystkich kategorii czynności przetwarzania**.
6) Przygotowaliśmy **rejestr czynności przetwarzania danych osobowych** prosimy o jego weryfikację i aktualizację w razie potrzeb, jeżeli pojawiły się pola w rejestrze podlegające weryfikacji oznaczyliśmy je kolorem żółtym.

7) Przyjmij **dokumenty obwieszczeniem wewnętrznym** (np. zarządzenie, uchwała) przygotowaliśmy również wzór takiego dokumentu.
8) W sytuacji pojawienia się nowych przepisów i obowiązków dotyczących przetwarzania danych osobowych lub realizowanych projektów, **oszacuj ryzyko** z wykorzystaniem **rejestru czynności przetwarzania** i **tabeli szacowania ryzyka**. Tabela szacowania ryzyka zawiera przykłady pojawiających się zagrożeń i podatności dla bezpieczeństwa danych osobowych.

WDROŻENIE DOKUMENTACJI RODO

Wskazówka Dostosuj listę zaleceń, aktualizuj status i priorytet

Nazwa projektu	Wdrożenie dokumentacji RODO	Nazwa Organizacji	Stowarzyszenie Wielkie Jeziora Mazurskie 2020
Opiekun projektu	Mateusz Borowski	Data	2018-08-15

OPIS PROJEKTU								WYKONANIE		ROBOCZOGODZINY		
STATUS	PRIORYTET	DATA ROZPOCZECIA	DATA ZAKOŃCZENIA	CZAS TRWANIA (DNI)	NAZWA ZADANIA	OPIEKUN	OPIS	WYKONANIE	% UKOŃCZENIA	USREDNIONY KOSZT	CZAS WYKONANIA	AKTUALNY CZAS
WDROŻENIE DOKUMENTACJI RODO									1%	0,00 zł	55	56
Zalecono	Wysoki	2018-09-09	2018-09-10	1	Upoważnienia projekty, pracownicy, prowadzenie ewidencji		Wydanie upoważnień dla pracowników, współpracowników (zarówno w ramach projektu, jak i upoważnień do wewnętrznych czynności). Prowadzenie ewidencji wydanych upoważnień		5%	0,00 zł	30	25
Zalecono	Wysoki	2018-09-10	2018-09-14	4	Wykazy podmiotów projekty UE		Prowadzenie wykazu podmiotów, którym powierzono przetwarzanie zgodnie z wymaganiem par. 20 ust 13 umowy o dofinansowanie		0%	0,00 zł	11	10
Zalecono	Wysoki	2018-09-11	2018-09-20	9	Zmiana skrzynek email		Audytor proponuje przejść na biznesowe skrzynki gmail - GSuite		0%	0,00 zł	12	18
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Wyłączenie zbierania plików cookies na stronie 7cudow, ustalenie administracji stroną www		Zwrócenie się do firmy IQ Connect Sp. z o.o. w sprawie wyłączenia plików cookie na stronie www 7 cudów, odzyskanie administracji stroną www		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Zakresy obowiązków		Przejrzenie i aktualizacja zakresów obowiązków z uwagi na wydawane upoważnienia do przetwarzania danych osobowych		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Antywirus		Wdrożenie oprogramowania antywirusowego		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Zmiany w instrukcji przechowywania archiwizacji dokumentów w ramach projektu		Uzupełnienie pomieszczeń w instrukcji - przechowywanie danych osobowych w Szkołach, uogólnienie instrukcji do wszystkich projektów		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Realizacja kopii zapasowych		Realizacja kopii zapasowych przez zewnętrzną księgową min. raz w tygodniu przenoszenie danych do niezależnego miejsca np. dysk biznesowy Google		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Powierzenie		Podpisanie umów powierzenia umowy z kancelarami, bhp, firmy eksperckie (zamówienia publiczne), organizatorzy wydarzeń		0%	0,00 zł	2	3
Zalecono	Wysoki	2018-09-12	2018-09-20	8	Niszczenie		Zakup niszczarek do dokumentów		0%	0,00 zł	2	3

STATUS
Zalecono
Nie rozporzęto
W trakcie
Ukończono

PRIORYTET
Niski
Średni
Wysoki