

POLITYKA OCHRONY DANYCH

**Stowarzyszenia
Przyjaciół Młodzieżowego Domu Kultury w Jaśle
FAMILIARIS**



FAMILIARIS

Stowarzyszenie Przyjaciół MDK w Jaśle

**Stowarzyszenie Przyjaciół
Młodzieżowego Domu Kultury w Jaśle
FAMILIARIS
38-200 Jasło, ul. Jana Pawła II 8A
tel. 13 446 59 25
NIP 6852337785, REGON 383187600**

JASŁO 2019

OLYMPIA POLITICA

Family
Political History and Family
History



FAMILIARIS

Family History and Political History



FAMILIARIS

SPIS TREŚCI

Podstawa prawna.....	4
Podstawowe pojęcia, skróty i definicje.....	5
Rozdział I ZAŁOŻENIA POLITYKI OCHRONY DANYCH	
I.1 Przedmiot regulacji	7
I.2 Cele wdrożenia polityki	7
I.3 Zakres obowiązywania	7
Rozdział II SYSTEM PRZETWARZANI DANYCH OSOBOWYCH	
II.1 Uczestnicy procesu przetwarzania danych i ich zadania	9
II.2 Przesłanki legalności przetwarzania danych osobowych.....	9
II.3 Zasady dotyczące przetwarzania danych osobowych	10
II.4 Prawa osób, których dane są przetwarzane	11
Rozdział III BEZPIECZEŃSTWO DANYCH OSOBOWYCH	
III.1 Istota bezpieczeństwa danych osobowych	13
III.2 Podstawowe zasady ochrony danych	13
III.3 Standardy bezpieczeństwa danych przetwarzanych w formie tradycyjnej	14
III.4 Standardy bezpieczeństwa danych przetwarzanych w systemie informatycznym	15
III.5 Sankcje karne	16
Rozdział IV PROCEDURY SŁUŻĄCE ZABEZPIECZENIU DANYCH	
IV.1 Udzielanie dostępu do danych osobowych	17
IV.2 Zabezpieczenia urządzeń sieciowych i serwerowych	22
IV.3 Zabezpieczenia systemu informatycznego	23
IV.4 Przetwarzanie danych na urządzeniach mobilnych.....	23
IV.5 Postępowanie z nośnikami danych.....	25
IV.6 Udostępnianie danych	26
IV.7 Analiza ryzyka.....	27
IV.8 Zasady zgłaszania naruszeń	29

Podstawa prawna

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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000 ze zmianami)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247)

Podstawowe pojęcia, skróty i definicje

Na użytek niniejszego dokumentu:

- 1) **administrator danych osobowych** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w niniejszym dokumencie oznacza Stowarzyszenie Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS reprezentowaną przez Zarząd;
- 2) **dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
- 3) **możliwa do zidentyfikowania osoba fizyczna** oznacza osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- 4) **dane wrażliwe** oznaczają dane szczególnej kategorii, dotyczą one pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, stanu zdrowia, seksualności lub orientacji seksualnej, obejmują też dane genetyczne i biometryczne;
- 5) **zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- 6) **przetwarzanie danych** oznacza 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;
- 7) **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
- 8) **podatności** oznacza słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie;
- 9) **zagrożenie** oznacza potencjalną przyczynę niepożądanego zdarzenia, które może powodować szkodę w przetwarzanych zbiorach danych;

- 10) **zabezpieczenie** oznacza środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko wystąpienia niepożądanych zdarzeń;
- 11) **pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
- 12) **incydent** oznacza naruszenie bezpieczeństwa danych osobowych, czyli zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 13) **państwo trzecie** oznacza państwo nienależące do Europejskiego Obszaru Gospodarczego;
- 14) **ustawa** oznacza ustawę o ochronie danych osobowych z dnia 10 maja 2018 r.;
- 15) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- 16) **KRI** oznacza Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- 17) **UODO** oznacza Urząd Ochrony Danych Osobowych, który jest organem nadzorczym w kwestiach związanych z ochroną danych osobowych.

Rozdział I

ZAŁOŻENIA POLITYKI OCHRONY DANYCH

I.1 Przedmiot regulacji

Polityka Ochrony Danych Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS określa:

- 1) normy i zasady dotyczące przetwarzania danych osobowych,
- 2) obowiązki osób uczestniczących w procesach przetwarzania danych,
- 3) podstawowe środki techniczne i organizacyjne służące zabezpieczeniu przetwarzanych danych,
- 4) częstotliwość i metodologię przeprowadzania analizy ryzyka,
- 5) procedury postępowania w przypadku wystąpienia naruszeń.

I.2 Cele wdrożenia polityki

Wdrożenie niniejszej Polityki Ochrony Danych ma na celu:

- 1) utrzymanie bezpieczeństwa przetwarzanych danych osobowych, czyli zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie,
- 2) realizację obowiązku nałożonego na Administratora Danych Osobowych (Art. 24 ust. 2 RODO),
- 3) zwiększenie świadomości osób zaangażowanych w procesy przetwarzania danych osobowych,
- 4) zredukowanie prawdopodobieństwa wystąpienia negatywnych konsekwencji naruszeń tj.:
 - naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Stowarzyszeniu Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS,
 - naruszeń przepisów prawa oraz innych regulacji,
 - strat finansowych ponoszonych w wyniku nałożonych kar,
 - strat finansowych ponoszonych w wyniku wypłaty odszkodowań osobom pokrzywdzonym,
 - zakłóceń w funkcjonowaniu organizacji spowodowanych nieprawidłowym działaniem systemów,
 - utraty lub obniżenia reputacji Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS.

I.3 Zakres obowiązywania

1. Polityka Ochrony Danych ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez Stowarzyszenie Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS.

2. Polityka ma zastosowanie do wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.
3. Polityka ma zastosowanie do wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
4. Do stosowania zasad określonych w Polityce Ochrony Danych zobowiązani są wszyscy członkowie Stowarzyszenia, zleceniobiorcy, wolontariusze oraz inne osoby, mające dostęp do informacji podlegających ochronie.

Rozdział II

SYSTEM PRZETWARZANIA DANYCH OSOBOWYCH

II.1 Uczestnicy procesu przetwarzania danych i ich zadania

1. **Administrator Danych Osobowych (ADO)** czyli Zarząd Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS:
 - 1) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
 - 2) odpowiada za zgodne z prawem przetwarzanie danych osobowych w Stowarzyszeniu Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS,
 - 3) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
 - 4) nadaje uprawnienia do dostępu do danych.
2. **Osoba przetwarzająca dane** czyli członek stowarzyszenia, zleceniobiorca, wolontariusz lub osoba upoważniona przez Zarząd do przetwarzania danych osobowych:
 - 1) chroni prawo do prywatności osób, których dane przetwarza,
 - 2) zna normy prawne dotyczącymi ochrony danych osobowych oraz zasady określone w Polityce danych osobowych Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS i wykonuje powierzone jej zadania z uwzględnieniem tych przepisów,
 - 3) niezwłocznie informuje Administratora Danych Osobowych lub o wszelkich nieprawidłowościach dotyczących przetwarzania danych osobowych,
 - 4) stosuje środki techniczne i organizacyjne służące zabezpieczeniu danych, które przetwarza w związku z realizacją obowiązków służbowych.
3. **Podmiot przetwarzający** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który na podstawie umowy powierzenia, przetwarza dane osobowe w imieniu administratora.
4. **Odbiorca** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe.
5. **Strona trzecia** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

II.2 Przesłanki legalności przetwarzania danych osobowych

1. W Stowarzyszeniu Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS przetwarza się dane osobowe zwykle.
2. Dane osobowe przetwarzane są wyłącznie w następujących przypadkach:
 - 1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

- 2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - 3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - 4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
 - 5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
 - 6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
3. Dane wrażliwe mogą być przetwarzane wyłącznie w sytuacjach określonych w art. 9 RODO i podlegają one szczególnej ochronie.
4. Przetwarzanie danych na podstawie zgody wymaga aby:
- 1) zgoda na przetwarzanie danych osobowych była jednoznaczna - wyrażona w formie pisemnej lub inny sposób, umożliwiając wykazanie posiadania zgody;
 - 2) jeżeli zgoda wyrażana jest w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę było przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
 - 3) zgoda mogła być w dowolnym momencie wycofana i było to równie łatwe jak jej wyrażenie;
 - 4) wycofanie zgody nie wpływało na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
 - 5) osoba, której dane dotyczą, była poinformowana o warunkach wyrażenia zgody przed jej wyrażeniem;
 - 6) wykonanie umowy nie było uzależnione od wyrażenia zgody na przetwarzanie danych, w tym świadczenie usługi, jeśli nie jest niezbędne do wykonania tej umowy.

II.3 Zasady dotyczące przetwarzania danych osobowych

1. Dane mogą być przetwarzane wyłącznie w taki sposób, aby zapewnione były:
 - 1) zgodność z prawem, rzetelność i przejrzystość, czyli przetwarzanie danych zgodnie z obowiązującymi przepisami oraz w sposób czytelny i zrozumiały dla osoby, której dane dotyczą;
 - 2) ograniczenie celu, czyli zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami (przetwarzanie do celów archiwalnych, naukowych, historycznych lub statystycznych

- jest uznawane za zgodne z pierwotnymi celami, przy czym powinno odbywać się na podstawie odrębnych przepisów);
- 3) minimalizacja danych, czyli określenie zakresu przetwarzanych danych w sposób adekwatny dla celu, do realizacji którego zostały zebrane;
 - 4) prawidłowość, czyli dbanie o merytoryczną wartość przetwarzanych informacji (dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania należy niezwłocznie usunąć lub sprostować);
 - 5) ograniczenie przechowywania, czyli przechowywanie danych w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne dla realizacji celów, do których dane te zostały zebrane (dane osobowe można przechowywać przez okres dłuższy, wyłącznie w celach określonych przepisami, przy zastosowaniu odpowiednich środków technicznych i organizacyjnych);
 - 6) integralność i poufność, czyli przetwarzanie danych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym, niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
2. W przypadku zbierania danych od osoby, której one dotyczą należy poinformować ją o:
- tożsamości i danych kontaktowych Administratora,
 - celu oraz podstawie prawnej przetwarzania,
 - odbiorcach danych lub kategoriach odbiorców – jeżeli istnieją,
 - zamiarze przekazywania danych do państw trzecich (w razie przekazywania danych - informacje o stopniu ochrony, zabezpieczeniach, możliwościach uzyskania kopii danych lub miejscu udostępnienia),
 - okresie przechowywania lub kryteriach ustalania tego okresu,
 - prawach przysługujących osobie, której dane są przetwarzane,
 - możliwości wniesienia skargi do organu nadzorczego,
 - dobrowolności lub obowiązku podania danych i ewentualnych konsekwencjach ich niepodania,
 - zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu.

II.4 Prawa osób, których dane są przetwarzane

1. Osobie, której dane są przetwarzane przysługują następujące uprawnienia:
 - prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
 - prawo do żądania sprostowania (poprawiania) danych osobowych, w przypadku stwierdzenia, że dane są nieprawidłowe lub niekompletne;
 - prawo do bycia zapomnianym tj. prawo do żądania usunięcia danych osobowych, w przypadku gdy:
 - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
 - wniesiono sprzeciw wobec przetwarzania danych osobowych,
 - wycofano zgodę na przetwarzanie danych osobowych, na podstawie której przetwarzano dane i nie ma innej podstawy prawnej ich przetwarzania,
 - dane osobowe przetwarzane są niezgodnie z prawem,
 - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;

- prawo do żądania ograniczenia przetwarzania danych osobowych, w przypadku, gdy:
 - kwestionuje się prawidłowość danych osobowych,
 - przetwarzanie danych jest niezgodne z prawem, a osoba, której dotyczą sprzeciwia się ich usunięciu, żądając w zamian ograniczenia przetwarzania,
 - placówka nie potrzebuje już danych dla swoich celów, ale osoba, której dotyczą potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
 - wniesiono sprzeciw wobec przetwarzania danych, do czasu ustalenia czy prawnie uzasadnione podstawy po stronie placówki są nadrzędne wobec podstawy sprzeciwu;
 - prawo do przenoszenia danych, w przypadku gdy łącznie spełnione są następujące przesłanki:
 - przetwarzanie danych odbywa się na podstawie zawartej umowy lub na podstawie zgody,
 - przetwarzanie odbywa się w sposób zautomatyzowany.
2. W przypadku stwierdzenia, że dane przetwarzane są niezgodnie z prawem, osobie, której dane są przetwarzane, przysługuje prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych tj. Urzędu Ochrony Danych.

Rozdział III

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

III.1 Istota bezpieczeństwa danych osobowych

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych polega na zapewnieniu ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
2. Ochrona danych osobowych realizowana jest poprzez stosowanie środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych, których celem jest zabezpieczenie zarówno zbiorów przetwarzanych w formie tradycyjnej jak i systemu informatycznego.

III.2 Podstawowe zasady ochrony danych

1. Stosowane zabezpieczenia poddawane są okresowej inwentaryzacji i modyfikowane adekwatnie do pojawiających się zagrożeń.
2. Czynności przetwarzania danych są ewidencjonowane w rejestrze czynności przetwarzania (na podstawie art. 30 ust. 1 RODO), który zawiera następujące elementy:
 - nazwa czynności przetwarzania,
 - cel przetwarzania,
 - kategorie osób,
 - kategorie danych,
 - podstawa przetwarzania danych,
 - źródło danych,
 - planowany termin usunięcia kategorii danych,
 - nazwa współadministratora i dane kontaktowe,
 - kategorie odbiorców,
 - nazwa systemu lub oprogramowania,
 - ogólny opis techniczny i organizacyjny środków bezpieczeństwa,
 - transfer do kraju trzeciego lub organizacji międzynarodowej (w przypadku transferu nazwa kraju i podmiotu oraz dokumentacja odpowiednich zabezpieczeń),
 - osoba odpowiedzialna za zawartość rejestru.
3. W razie przetwarzania danych w imieniu innego Administratora danych (na podstawie umowy powierzenia, która powinna zawierać elementy określone w artykule 28 RODO) rejestrowane są kategorie czynności przetwarzania (na podstawie art. 30 ust. 2 RODO), który zawiera następujące elementy:
 - kategorie przetworzeń,
 - administrator,
 - ogólny opis techniczny i organizacyjny środków bezpieczeństwa,
 - czas trwania przetwarzania,
 - transfer do kraju trzeciego lub organizacji międzynarodowej (w przypadku transferu nazwa kraju i podmiotu oraz dokumentacja odpowiednich zabezpieczeń),
 - osoba odpowiedzialna za zawartość rejestru.
4. Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania prowadzi Administrator Danych Osobowych.

5. Za treść wpisów zamieszczonych w rejestrach odpowiedzialność ponoszą członkowie stowarzyszenia, którzy daną czynność realizują.
6. Kontrolę nad zawartością rejestrów sprawuje Zarząd Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS, który zatwierdza wszystkie wpisy do rejestrów.
7. Członkowie stowarzyszenia zobowiązani są do realizacji poszczególnych czynności przetwarzania zgodnie z zatwierdzonymi rejestrami, a wszelkie zmiany wpisów w rejestrach wymagają pisemnej zgody Zarządu stowarzyszenia.
8. W razie przetwarzania danych na podstawie zgody członek stowarzyszenia pozyskujący dane od osoby, której dotyczą zobowiązany jest uzyskać jej zgodę i spełnić wobec niej obowiązek informacyjny w imieniu Administratora.
9. W razie pozyskiwania danych od osoby, której dotyczą zobowiązany jest spełnić wobec niej obowiązek informacyjny w imieniu Administratora.
10. Administrator, uwzględniając ochronę danych w fazie projektowania, dokonuje analizy ryzyka przed rozpoczęciem przetwarzania (zgodnie z art.25 RODO).
11. Nie rzadziej niż raz w roku przeprowadzana jest analiza ryzyka utraty integralności, dostępności lub poufności informacji (na podstawie § 20 ust. 2 pkt 3 KRI w oparciu o podrozdział IV.13). Analiza ryzyka dotyczy czynności przetwarzania, które są opisane w Rejestrze czynności przetwarzania. Jeżeli Administrator przetwarza dane osobowe innego administratora, a umowa powierzenia nie stanowi inaczej analiza obejmuje również kategorie czynności przetwarzania.
12. Analiza ryzyka może być przeprowadzana po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).
13. W razie stwierdzenia ryzyka mogącego mieć wpływ na bezpieczeństwo danych należy podjąć działania minimalizujące ryzyko.
14. W razie wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych przeprowadzana jest ocena skutków dla ochrony danych (na podstawie art. 35 RODO).

III.3 Standardy bezpieczeństwa danych przetwarzanych w formie tradycyjnej

1. Zadania wymagające przetwarzania danych osobowych realizują wyłącznie osoby upoważnione przez Zarząd stowarzyszenia.
2. Dokumenty zawierające dane osobowe muszą być przechowywane w szafach zamykanych na klucz, a dostęp do nich mogą mieć wyłącznie osoby do tego uprawnione.
3. Klucze do szaf i pomieszczeń, gdzie przetwarza się dane osobowe są ewidencjonowane i mają do nich dostęp tylko uprawnione osoby.
4. Duplikaty kluczy do szaf i pomieszczeń, gdzie przechowywane są dane osobowe dorabia się wyłącznie na polecenie lub za zgodą Zarządu stowarzyszenia.
5. Członek stowarzyszenia w czasie pracy powinien mieć na biurku tylko te dokumenty, które są mu potrzebne do realizacji określonego zadania.
6. W przypadku chwilowego opuszczenia stanowiska pracy dokumenty zawierające dane osobowe muszą być zabezpieczone przed dostępem osób nieuprawnionych.

7. Po zakończeniu pracy dokumenty muszą zabezpieczane w szafie zamykanej na klucz („zasada czystego biurka”).
8. Kopie robocze pism oraz inne przeznaczone do brakowania dokumenty, które zawierają dane osobowe, muszą być zniszczone w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w spełniającej ten wymóg niszczarce.
9. Dokumentacja zawierająca dane osobowe powinna być przechowywana w siedzibie administratora.
10. Przenoszenie dokumentacji poza siedzibę administratora dopuszczalne jest wyłącznie za wiedzą i zgodą Administratora lub gdy konieczność taka wynika z wewnętrznych procedur bądź obowiązujących przepisów.

III.4 Standardy bezpieczeństwa danych przetwarzanych w systemie informatycznym

1. Oprogramowanie musi być aktualizowane na bieżąco.
2. Systemy operacyjne muszą być chronione przez programy antywirusowe.
3. Konto administracyjne musi być oddzielone od kont użytkowników - należy zapewnić ochronę plików systemowych (na podstawie § 20 ust. 2 pkt 12 e KRI).
4. Przed przystąpieniem do pracy członek stowarzyszenia zobowiązany jest sprawdzić czy stacja robocza, na której przetwarzane są dane osobowe nie ma śladów ingerencji osób trzecich.
5. Dane przetwarzane w systemie informatycznym chronione są przed nieuprawnionym dostępem. Członek stowarzyszenia zobligowany jest do przestrzegania następujących zasad:
 - w czasie pracy należy mieć otwarte tylko te programy i aplikacje, które są potrzebne do realizacji określonego zadania,
 - w przypadku chwilowego opuszczenia stanowiska pracy należy wylogować się z systemu lub uruchomić wygaszacz ekranu zabezpieczony hasłem,
 - w razie przesyłania dokumentów z danymi osobowymi pocztą elektroniczną należy stosować mechanizmy kryptograficzne (hasła należy przekazać oddzielnym kanałem),
 - po zakończeniu pracy należy wylogować się z systemu,
 - po zakończeniu pracy wszelkie nośniki danych (dyski zewnętrzne, pendrivy, płyty CD) należy usunąć ze stacji roboczej i zabezpieczyć.
6. Należy stosować środki techniczne i organizacyjne oraz podejmować działania służące redukcji ryzyk, wynikających ze stwierdzonych podatności systemów informatycznych.
7. W razie dostrzeżenia nieujawnionych podatności systemów informatycznych mogących mieć wpływ na bezpieczeństwo danych należy niezwłocznie zgłosić to Administratorowi danych osobowych.
8. Nie rzadziej niż raz na pół roku należy przeprowadzić kontrolę zgodności systemów informatycznych z obowiązującymi normami prawnymi i regulacjami wewnętrznymi.

III.5 Sankcje karne

1. Osoba, która przetwarza dane osobowe, których przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli niedozwolone przetwarzanie dotyczy danych wrażliwych osoba, która dane przetwarza podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.
3. Osobie, która udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Rozdział IV

PROCEDURY SŁUŻĄCE ZABEZPIECZENIU DANYCH

IV.1

UDZIELANIA DOSTĘPU DO DANYCH OSOBOWYCH

Podstawa prawna: § 20 ust. 2 pkt 4 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 29 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

Cel: Określenie zasad dotyczących udzielania dostępu do danych osobowych.

Opis norm postępowania:

1. Osoba, która w związku z wykonywaniem obowiązków, przetwarza dane osobowe w imieniu administratora posiada pisemne upoważnienie (wzór upoważnienie określa załącznik nr 1).
2. Osoba, która nie jest upoważniona do przetwarzania danych, ale w związku z wykonywaniem obowiązków przebywa w pomieszczeniach, gdzie przetwarzane są dane osobowe posiada pisemne upoważnienie (wzór upoważnienie określa załącznik nr 2).
3. Upoważnienia wydaje Zarząd Stowarzyszenia.
4. Upoważnienia są ewidencjonowane (wzór rejestru osób upoważnionych do przetwarzania danych osobowych określa załącznik nr 3, wzór rejestru osób upoważnionych do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe określa załącznik nr 4).
5. Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznania się z przepisami RODO, Ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w szkole Polityce ochrony danych.

Jasło, dnia r.

.....
(pieczęć Stowarzyszenia)

UPOWAŻNIENIE nr/20... do przetwarzania danych osobowych

Upoważniam Panią/Pana członka Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jasle FAMILIARIS do przetwarzania danych osobowych w zakresie określonym w obowiązках.

Niniejszym zobowiązuje Panią/Pana do zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji o sposobie ich zabezpieczenia.

Upoważnienie obowiązuje od dnia..... 20.... r. i traci moc z chwilą odwołania z funkcji Członka stowarzyszenia.

.....
(pieczęć i podpisy Administratora Danych Osobowych)

OŚWIADCZENIE o zachowaniu poufności i zapoznaniu się z przepisami

Oświadczam, że zostałem/am poinformowany/a o obowiązujących przepisach dotyczących przetwarzania danych osobowych i zobowiązuje się ich przestrzegać.

Oświadczam, iż zobowiązuje się do zachowania w tajemnicy danych osobowych oraz informacji o sposobie ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków.

Jasło, dnia

.....
(podpis Członka stowarzyszenia)

Jasło, dnia r.

.....
(pieczęć Stowarzyszenia)

UPOWAŻNIENIE nr/20...
do przebywania w pomieszczeniach,
gdzie przetwarzane są dane osobowe

Upoważniam Panią/Pana członka Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jasle FAMILIARIS do przebywania w siedzibie stowarzyszenia czyli w pokoju 22 budynku Młodzieżowego Domu Kultury w Jasle - w którym przetwarzane są dane osobowe.

Niniejszym zobowiązuje Panią/Pana do zachowania w tajemnicy danych osobowych, do których może mieć Pani/Pan dostęp w związku z wykonywaniem obowiązków oraz informacji o sposobie ich zabezpieczenia.

Upoważnienie obowiązuje od dnia..... 20.... r. i traci moc z chwilą odwołania z funkcji Członka stowarzyszenia.

.....
(pieczęć i podpisy Administratora Danych Osobowych)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Oświadczam, że zostałem/am poinformowany/a o obowiązujących przepisach dotyczących przetwarzania danych osobowych i zobowiązuje się ich przestrzegać.

Oświadczam, iż zobowiązuje się do zachowania w tajemnicy danych osobowych oraz informacji o sposobie ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków.

Jasło, dnia

.....
(podpis Członka stowarzyszenia)

IV.2

ZABEZPIECZENIA URZĄDZEŃ SIECIOWYCH I SERWEROWYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Cel: Zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych przed utratą lub nieuprawnionym dostępem.

Informacja:

Stowarzyszenie korzysta z urządzeń sieciowych i serwerowych Młodzieżowego Domu Kultury w Jaśle, w którym ma siedzibę.

Opis norm postępowania:

1. Urządzenia serwerowe zainstalowane są w szafie teleinformatycznej w pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione przez Dyrektora Placówki.
2. W pomieszczeniu zapewnione muszą być zapewnione warunki (wilgotność, temperatura) zgodne z zaleceniami producenta poszczególnych urządzeń.
3. Urządzenia instalowane są w taki sposób, aby był zapewniony do nich swobodny dostęp fizyczny, w razie ich serwisowania bądź napraw.
4. Routery powinny być instalowane w takich miejscach, aby dostęp do nich miały tylko upoważnione osoby.
5. Urządzenia na których przetwarzane są dane powinny być podłączone pod system zasilania awaryjnego np. UPS, umożliwiającego podtrzymanie zasilania na czas konieczny do bezpiecznego wyłączenia urządzeń.
6. Okablowanie powinno być poprowadzone torami bezpiecznymi tj. podtynkowo, torem ziemnym lub w na ścianie w odpowiednich osłonach montażowych, zapewniających ochronę przed uszkodzeniem.
7. Okablowanie powinno być uporządkowane i oznakowane w sposób umożliwiający szybkość identyfikację.

IV.3

ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

Podstawa prawna: § 21 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Cel: Zapewnienie ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem.

Opis norm postępowania:

1. System informatyczny musi posiadać ochronę antywirusową oraz zaporę sieciową, która obejmuje wszystkie stacje robocze oraz serwery.
2. Oprogramowanie powinno być skonfigurowane w sposób aby:
 - zapewnić automatyczne usuwanie wirusów, a w sytuacji kiedy nie jest to możliwe objęcie ich kwarantanną,
 - zapewnić okresowe skanowanie wszystkich dysków lokalnych oraz powiadamianie o wykrytym oprogramowaniu złośliwym.

IV.4

PRZETWARZANIE DANYCH NA URZĄDZENIACH MOBILNYCH

Podstawa prawna: § 20 ust. 2 pkt 8 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Cel: Zapewnienie bezpieczeństwa danych przetwarzanych na urządzeniach mobilnych.

Opis norm postępowania:

1. Dopuszczalne jest stosowanie usług chmurowych, co oznacza, że dane przechowywane są na serwerze podmiotu oferującego usługę, który odpowiada za dostępność do danych i zabezpieczenie serwera. Zawsze w takiej sytuacji wymagana jest umowa powierzenia danych, zawierająca przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki i prawa podmiotu przetwarzającego (zgodnie z art. 28 RODO).
2. Korzystanie z urządzeń mobilnych (w tym prywatnych) w celu przetwarzania danych osobowych jest dopuszczalne, ale wymaga stosowania wszystkich zabezpieczeń określonych w niniejszej polityce m.in.:
 - stosowanie programów antywirusowych,
 - stosowania haseł,
 - ochronę haseł przed dostępem osób nieuprawnionych (w tym niestosowanie autologowania),
 - zabezpieczenia dostępu do danych w razie utraty urządzenia (np. w wyniku kradzieży),
 - zapewnienie ochrony urządzenia przed nieuprawnionym dostępem (np. stosowanie wygaszaczy ekranu zabezpieczonych hasłem) lub jego utratą (stosowanie zasad dotyczących nośników danych).
3. Za właściwe zabezpieczenie służbowych urządzeń mobilnych odpowiedzialność ponosi Administrator danych.
4. Za właściwe zabezpieczenie prywatnych urządzeń mobilnych wykorzystywanych do przetwarzania danych odpowiedzialność ponosi pracownik.

IV.5

POSTĘPOWANIE Z NOŚNIKAMI DANYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Cel: Zapewnienie ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem.

Opis norm postępowania:

1. Nośniki danych należy przechowywać w miejscu niedostępnym dla osób nieuprawnionych (np. w szafie pancernej).
2. Warunki środowiskowe przechowywania nośników danych muszą być zgodne z zaleceniami producentów tych urządzeń.
3. Przenoszenie nośników danych wymaga zabezpieczenia ich przed nieuprawnionym dostępem poprzez szyfrowanie lub pakowanie w programie Zip oraz zabezpieczenie kodem. Kod musi być chroniony i zawierać minimum 8 znaków, w tym małe i duże litery, przynajmniej jedną cyfrę oraz znak specjalny.
4. Przenoszenie nośników danych powinno odbywać się z zachowaniem szczególnej uwagi i ostrożności. W przypadku zlecenia transportu nośników należy korzystać z usług sprawdzonych firm i kurierów.
5. Przenoszenie danych osobowych poza siedzibę Stowarzyszenia Przyjaciół Młodzieżowego Domu Kultury w Jaśle FAMILIARIS jest dopuszczalne jest wyłącznie za wiedzą i zgodą Prezesa.
6. Naprawa nośników danych powinna być przeprowadzona po trwałym usunięciu zapisanych na nim informacji lub jeżeli nie jest to możliwe zlecona podmiotowi, spełniającemu wymogi bezpieczeństwa, z którym zawarta została umowa powierzenia danych.
7. W celu odzyskania utraconych danych dopuszczalne jest za zgodą Prezesa Stowarzyszenia przekazanie nośnika danych specjalistycznemu podmiotowi, spełniającemu wymogi bezpieczeństwa, z którym zawarta została umowa powierzenia danych.
8. Z nośników danych przeznaczonych do likwidacji należy trwale usunąć zapisane wcześniej dane lub uszkodzić je w taki sposób, aby odczyt danych stał się niemożliwy.

IV.6

UDOSTĘPNIANIE DANYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Cel: Określenie warunków udostępniania danych.

Opis norm postępowania:

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
2. Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
 - adresat wniosku (administrator danych),
 - wnioskodawca,
 - podstawa prawna (wskazanie potrzeby),
 - wskazanie przeznaczenia,
 - zakres informacji.
3. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

IV.7 Analiza ryzyka

ANALIZA RYZYKA

Podstawa prawna: § 20 ust. 2 pkt 3 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Cel: Ocena ryzyka związanego z procesami przetwarzania danych i podjęcie działań adekwatnych do jego poziomu.

Opis norm postępowania:

Powołanie zespołu

1. Analizę ryzyka przeprowadza Administrator danych we współpracy z powołanym w tym celu zespołem zadaniowym.
2. W skład zespołu wchodzi członkowie stowarzyszenia bezpośrednio zaangażowani w przetwarzanie danych.

Określenie zagrożeń

3. Zespół określa wykaz zagrożeń dla poszczególnych czynności i kategorii czynności. Uwzględniane są zagrożenia, których materializacja może spowodować naruszenie poufności, dostępności lub integralności przetwarzanych danych osobowych.
4. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych czynności przetwarzania i kategorii czynności przetwarzania.

Wyznaczenie wartości ryzyka

5. Zespół szacuje prawdopodobieństwo (P) zmaterializowania zagrożenia dla poszczególnych czynności przetwarzania i kategorii czynności, według następujących kryteriów:

PRAWDOPODOBIENSTWO	CZĘSTOTLIWOŚĆ	SKALA (WAGA)
niskie	nie występuje lub występuje rzadziej niż raz w roku	P = 1
średnie	występuje kilka razy w roku	P = 2
wysokie	występuje co najmniej raz w tygodniu	P = 3

6. Zespół określa skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne, według następujących kryteriów:

POZIOM	SKUTKI WYSTĄPIENIA	SKALA (WAGA)
małe	nie powoduje naruszenia ochrony danych osobowych	S = 1
średnie	naruszenie, którego nie trzeba zgłaszać do Generalnego Inspektora Ochrony Danych Osobowych	S = 2
duże	naruszenie danych szczególnych (wrażliwych) lub naruszenie dotyczące dużej ilości osób, naruszenie podlegające zgłoszeniu do Generalnego Inspektora Ochrony Danych Osobowych	S = 3

7. Korzystając z macierzy ryzyka, określa się wartość ryzyka dla poszczególnych zagrożeń jako:

N (niską), **Ś** (średnią) lub **W** (wysoką)

	S=1	S=2	S=3
P=1	N	N	Ś
P=2	N	Ś	W
P=3	Ś	W	W

Postępowanie z ryzykiem

8. Na podstawie uzyskanych wyników Administrator decyduje o postępowaniu z ryzykiem. Reakcje na wartości ryzyka mogą być następujące:
- **dla wartości N - akceptacja ryzyka**, czyli uznaje się, że zabezpieczenia są właściwe i nie ma potrzeby stosowania dodatkowych zabezpieczeń),
 - **dla wartości Ś - akceptacja ryzyka i monitorowanie**, czyli zakłada się, że zabezpieczenia są właściwe, ale wskazane jest stosowanie dodatkowych zabezpieczeń lub ich modyfikacja w miarę możliwości i dostępnych środków,
 - **dla wartości W - ryzyko nieakceptowalne**, oznacza, że zabezpieczenia są niewystarczające i należy podjąć działanie zmniejszające wartość ryzyka. Może to być:
 - przeniesienie, czyli przerzucenie ryzyka np. outsourcing, ubezpieczenie,
 - unikanie, czyli eliminacja działań powodujących ryzyko,
 - redukcja, czyli zastosowanie zabezpieczeń w celu obniżenia ryzyka.

Zawsze gdy Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

IV.8

ZASADY ZGŁASZANIA NARUSZEŃ

Podstawa prawna: Art. 33 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

Cel: Określenie zasad postępowania w razie zaistnienia naruszenia bezpieczeństwa danych.

Opis norm postępowania:

1. Każdy członek stowarzyszenia, który stwierdzi podatność, fakt naruszenia bezpieczeństwa danych, bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Prezesowi stowarzyszenia.
2. W przypadku stwierdzenia naruszenia danych członek stowarzyszenia ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.
3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych nie należy podejmować działań mogących utrudnić określenie przyczyn wystąpienia incydentu i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Prezesa.
4. Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
 - a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki (może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem),
 - b) inicjuje ewentualne działania dyscyplinarne,
 - c) działa na rzecz przywrócenia działania jednostki po wystąpieniu incydentu,
 - d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (wzór rejestru naruszeń określa załącznik nr 1, wzór raportu z naruszenia określa załącznik nr 2).
6. W przypadku przetwarzania danych na podstawie umowy powierzenia o stwierdzeniu naruszenia zawiadamia się niezwłocznie Administratora danych.

7. W przypadku stwierdzenia, że naruszenie mogło skutkować naruszeniem praw i wolności osób fizycznych administrator zgłasza naruszenie do Urzędu Ochrony Danych nie później niż 72 godzin od stwierdzenia naruszenia (zgodnie z art.33 RODO).
8. W przypadku stwierdzenia, że incydent może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, Prezes Stowarzyszenia bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o zaistniałym zdarzeniu (wzór zawiadomienia określa załącznik nr 2).

UWAGA! Przykłady naruszeń:

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

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Lp.	Data incydentu	Rodzaj naruszenia bezpieczeństwa	Stwierdzony poziom ryzyka	Data zgłoszenia naruszenia do UODO
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

11.				
-----	--	--	--	--

Załącznik Nr 2

Jasło, dnia r.

.....
(pieczęć)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Data incydentu: r. Godzina incydentu:
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia:
.....
(np. nr pokoju, nazwa pomieszczenia, opis lokalizacji)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....
5. Przyczyny wystąpienia zdarzenia:
.....
.....
6. Podjęte działania:
.....
.....
7. Postępowanie wyjaśniające:
.....
.....
.....
.....
.....

.....
(podpis Administratora Danych Osobowych)

Załącznik Nr 3

Jasło, dnia r.

.....
(pieczęć)

Szanowna/y Pani/Pan

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH

Na podstawie art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

informuję o naruszeniu ochrony Pani/Pana danych osobowych

przetwarzanych przez

Charakter naruszenia	
Możliwe konsekwencje naruszenia	
Zastosowane/proponowane środki w celu zminimalizowania skutków naruszenia	

W razie pytań proszę o kontakt z Administratorem Danych Osobowych (Zarząd Stowarzyszenia w składzie:

Prezes

Wiceprezes

Sekretarz

Skarbnik

tel. 13 446 59 25

.....
(podpis Administratora Danych Osobowych)