**POLITYKA**

**PRZETWARZANIA DANYCH OSOBOWYCH**

**PRZEZ**

**STOWARZYSZENIE „EURO-COUNTRY”**

***przyjęta uchwałą Zarządu Stowarzyszenia z dnia 28.06.2018 nr XXIV/65/2018/Z***

**Spis treści**

[**ROZDZIAŁ I POSTANOWIENIA OGÓLNE 3**](#_Toc514765133)

[**ROZDZIAŁ II ZASADY PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ LGD 6**](#_Toc514765134)

[**Zasady i wartości 6**](#_Toc514765135)

[**Rejestry czynności przetwarzania 7**](#_Toc514765136)

[**Prywatność w fazie projektowania i prywatność jako ustawienie domyślne oraz minimalizacja danych 8**](#_Toc514765137)

[**Przetwarzanie danych osobowych przez osoby upoważnione 9**](#_Toc514765138)

[**Powierzenie podmiotom trzecim danych, których administratorem jest LGD 11**](#_Toc514765139)

[**LGD jako podmiot przetwarzający 12**](#_Toc514765140)

[**ROZDZIAŁ III OSOBY ODPOWIEDZIALNE W STOWARZYSZENIU ZA NADZÓR NAD PRZETWARZANIEM DANYCH OSOBOWYCH 14**](#_Toc514765141)

[**Zadania Zarządu 14**](#_Toc514765142)

[**Pracownik ds. bezpieczeństwa informacji 14**](#_Toc514765143)

[**Przewodniczący Komisji Rewizyjnej LGD 15**](#_Toc514765144)

[**ROZDZIAŁ IV PRAWA OSÓB TRZECICH I SPOSÓB POSTĘPOWANIA PRZEZ STOWARZYSZENIE Z WNIOSKAMI TYCH OSOB 17**](#_Toc514765145)

[**Ogólne zasady 17**](#_Toc514765146)

[**Obowiązek informacyjny 18**](#_Toc514765147)

[**Prawo dostępu do danych osobowych 20**](#_Toc514765148)

[**Prawo do sprostowania danych 21**](#_Toc514765149)

[**Prawo do bycia zapomnianym 22**](#_Toc514765150)

[**Prawo do ograniczenia przetwarzania 23**](#_Toc514765151)

[**Prawo do przenoszenia danych 24**](#_Toc514765152)

[**Prawo do sprzeciwu 25**](#_Toc514765153)

[**Zautomatyzowane podejmowanie decyzji i profilowanie 25**](#_Toc514765154)

[**ROZDZIAŁ V STOSOWANE PRZEZ STOWARZYSZENIE ŚRODKI ZABEZPIECZENIA DANYCH 27**](#_Toc514765155)

[**Środki organizacyjne: 27**](#_Toc514765156)

[**Środki fizycznej ochrony 29**](#_Toc514765157)

[**Środki ochrony technicznej 30**](#_Toc514765158)

[**ROZDZIAŁ VI ZDARZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH i REAKCJA NA TAKIE ZDARZENIA 32**](#_Toc514765159)

[**Naruszenia ochrony danych – przykłady 32**](#_Toc514765160)

[**Procedura reagowania na naruszenia ochrony danych osobowych 34**](#_Toc514765161)

# ROZDZIAŁ I POSTANOWIENIA OGÓLNE

1. Niniejszy dokument, zwany dalej „**Polityką**”, reguluje zasady przetwarzania danych osobowych przez Stowarzyszenie „Euro-Country” zwane dalej „**Stowarzyszeniem**” lub „**LGD**”.

Celem Polityki jest:

* 1. ustalenie reguł postępowania, które gwarantują przestrzeganie przez LGD zasad domyślnej prywatności (*privacy by default*), prywatności od etapu projektowania (*privacy by default*) oraz minimalizacji danych;
  2. określenie, w jaki sposób LGD będzie realizować obowiązki wynikające z obowiązujących przepisów prawa powszechnie obowiązującego (procedur postępowania)   
     i kto w Stowarzyszeniu będzie odpowiedzialny za ich realizację;
  3. ustalenie procedur, zgodnie z którymi powinno się odbywać przetwarzanie danych osobowych przez LGD;
  4. określenie, w jaki sposób Stowarzyszenie będzie realizować uprawnienia osób trzecich, których dane przetwarza, wynikające z przepisów prawa i odnoszące się do tych danych osobowych;
  5. określenie środków zabezpieczenia danych osobowych, warunkujących ich przetwarzanie przez Stowarzyszenie w sposób bezpieczny, minimalizujący ryzyko naruszenia poufności, integralności i dostępności danych osobowych;
  6. określenie procedur reagowania na zdarzenia naruszenia bezpieczeństwa danych osobowych;
  7. opracowanie wzorów najważniejszych dokumentów, jakie stosować powinno Stowarzyszenie, w związku z przetwarzaniem danych osobowych (wzory zgód, formularzy informacyjnych, rejestrów, klauzul umownych).

**Polityka zastępuje obowiązujące dotychczas wewnętrzne dokumenty regulujące zasady przetwarzania danych osobowych przez LGD**, tj. Politykę bezpieczeństwa wraz z Instrukcją zarządzania systemem informatycznym, które zostały przyjęte uchwałą nr XXII/56/2017/Z .

1. Opracowanie Polityki zostało poprzedzone dokonaniem analizy procesów przetwarzania danych przez LGD, dotychczasowych doświadczeń na tym polu, posiadanych zasobów organizacyjnych, technicznych i osobowych. Kolejnym etapem przygotowania Polityki było wypełnienie przez Stowarzyszenie kwestionariusza dotyczącego przetwarzania danych osobowych. Na podstawie zabranych informacji została dokonana analiza ryzyka, w oparciu o którą Stowarzyszenie wdrożyło rozwiązania znajdujące odzwierciedlenie w treści Polityki.
2. Bezpośrednim powodem przyjęcia Polityki było rozpoczęcie okresu stosowania 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), które zasadniczo zmieniło podejście do zagadnień związanych z przetwarzaniem danych osobowych i ich ochroną.
3. W celu dostosowania sposobu postępowania do podejścia opartego na ryzyku (*risk based approach*), LGD, świadome, że zarówno regulacje prawne, jak i sposoby przetwarzania i zabezpieczania danych osobowych zmieniają się w czasie, a co za tym idzie zmienia się ryzyko związane z tymi procesami, będzie dokonywać **okresowej oceny Polityki w kontekście jej aktualności i adekwatności do procesów przetwarzania danych osobowych przez Stowarzyszenie w danym momencie.**

W tym celu **Stowarzyszenie przy okazji wdrażania nowych procesów związanych z przetwarzaniem danych osobowych, będzie przeprowadzało audyt** zagadnień związanych z przewarzaniem danych osobowych i ustali, czy istnieje potrzeba aktualizacji Polityki i sposobu postępowania z danymi osobowymi.

Przeprowadzenie audytu nie zwalnia Stowarzyszenia z obowiązku stosowania podejścia opartego na prywatności od etapu projektowania (*privacy by design*), polegającego na konieczności dokonania analizy każdego projektu z punktu widzenia ochrony danych osobowych przed rozpoczęciem realizacji tego projektu. Sposób stosowania podejścia *privacy by design* wyjaśnionow dalszej części Polityki.

1. Niektóre określenia, które mają swoje ustalone znaczenie w języku potocznym, na gruncie zagadnień związanych z przetwarzaniem danych osobowych, są zupełnie inaczej zdefiniowane. Dlatego poniżej podano definicje najważniejszych tego rodzaju terminów:
2. **Polityka** – niniejszy dokument;
3. **administrator** – podmiot decydujący o celach i warunkach przetwarzania danych osobowych (np. LGD jest administratorem danych osobowych swoich członków, bo decyduje o tym, w jaki sposób i w jakim celu je przetwarza, np. w celu powiadamiania ich o ważnych wydarzeniach dotyczących Stowarzyszenia komunikuje się z nimi za pośrednictwem poczty elektronicznej);
4. **Zarząd** – Zarząd LGD;
5. **RODO** –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);
6. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych;
7. **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować;
8. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany (maszynowy, komputerowy) lub niezautomatyzowany (ręczny, fizyczny), np.: zbieranie, organizowanie, porządkowanie, przechowywanie, przeglądanie, rozpowszechnianie, usuwanie, niszczenie danych osobowych;
9. **podmiot** – zarówno osoba fizyczna, jak i osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej, a także organ publiczny (organ administracji publicznej);
10. **osoba, której dane dotyczą** – konkretna osoba fizyczna, której dane przetwarza LGD i która zwraca się do Stowarzyszenia z określonym wnioskiem, z którą Stowarzyszenie się kontaktuje, wobec danych której LGD podejmuje określone działania;
11. **podmiot przetwarzający** – podmiot, który przetwarza dane osobowe w imieniu LGD (np. przechowuje, je, używa w celu wykonywania usług dla Stowarzyszenia) – podmiotem przetwarzającym jest np. księgowa, dostawca miejsca na serwerze, na którym Stowarzyszenie przechowuje swoje dane, dostawca aplikacji używanych do mailingu;
12. **strona (osoba) trzecia** – każdy podmiot, inny niż: (a) osoba, której dane dotyczą, (b) LGD, (c) podmiot przetwarzający (d) osoby, które z upoważnienia LGD lub podmiotu przetwarzającego mogą przetwarzać dane osobowe, których administratorem jest Stowarzyszenie;
13. **odbiorca** – podmiot, któremu LGD ujawnia dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania prowadzonego zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców (np. odbiorcami są podmioty przetwarzające, bo zazwyczaj administrator ujawnia mim dane osobowe);
14. **naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez LGD lub jego podmiot przetwarzający.

Jeżeli jakieś pojęcie ma swoiste znaczenie, ale jest rzadziej używane w Polityce, i nie zostało wymienione powyżej, jego definicja może znaleźć się w dalszej części tego dokumentu – zapisane ona będzie wówczas w nawiasie pogrubioną czcionką.

1. **Adresatem Polityki** (osobami zobowiązanymi do jej stosowania) są:
   1. członkowie organów Stowarzyszenia, w tym członkowie Stowarzyszenia, jeżeli przetwarzają dane osobowe, których LGD jest administratorem;
   2. pracownicy Stowarzyszenia (od momentu ich zatrudnienia);
   3. stali współpracownicy Stowarzyszenia mający dostęp do danych osobowych (w szczególności – jeżeli osoby takie się pojawią - osoby zatrudnione przez Stowarzyszenie na podstawie umów cywilnoprawnych do prac w biurze LGD);
   4. podmioty przetwarzające Stowarzyszenia – w ograniczonym zakresie: z tymi podmiotami LGD zawierać będzie umowy zawierające klauzulę umowną obligującą do przestrzegania głównych zasad wynikających z RODO oraz z Polityki. Wzór umowy powierzenia (który może zostać wykorzystany również jako klauzula w umowie o przedmiocie szerszym niż samo powierzenie danych osobowych) stanowi załącznik do Polityki.
2. Polityka jest dokumentem, z którym zapoznać się powinni wszyscy pracownicy i stali współpracownicy Stowarzyszenia oraz członkowie organów Stowarzyszenia.
3. Zarząd podejmuje stosowne działania, aby naruszenie zasad przetwarzania danych osobowych przez Adresatów Polityki wiązało się z surowymi konsekwencjami dla naruszyciela.

W szczególności naruszenie obowiązków zachowania w tajemnicy tych danych oraz o stosowanych sposobach zabezpieczeń danych osobowych, miejsc, urządzeń, systemów i programów, w których te dane są przechowywane może stanowić podstawę do:

* 1. odwołania członka organu Stowarzyszenia z pełnionej funkcji;
  2. wyciągnięcia wobec pracownika środków dyscyplinujących, a w szczególnie poważnych przypadkach zwolnienia dyscyplinarnego;
  3. naliczenia kary umownej, zerwania zawartej umowy z podmiotem przetwarzającym lub współpracownikiem Stowarzyszenia.

Niezależnie od tych konsekwencji, adresaci Polityki za naruszenie jej postanowień, mogą zostać obciążeni obowiązkiem odszkodowawczym (jeżeli naruszenie będzie wiązało się   
z wyrządzeniem szkody Stowarzyszeniu lub osobie trzeciej).

Zarząd podejmuje działania zmierzające do wprowadzenia do obowiązujących w Stowarzyszeniu regulaminów (np. Regulaminu Pracy Biura, Regulamin Rady), zawartych lub zawieranych umów, postanowień, które będą umożliwiały wyciąganie opisanych wyżej konsekwencji wobec naruszycieli Polityki

Zarząd podejmuje również działania zmierzające do rozpowszechnienia wśród adresatów Polityki wiedzy na temat tych konsekwencji.

# ROZDZIAŁ II ZASADY PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ LGD

## Zasady i wartości

1. LGD przetwarza dane osobowe zgodnie z poniższymi, **podstawowymi zasadami,** które znajdują swoje odzwierciedlenie w dalszej treści Polityki:
2. dane są **przetwarzane zgodnie z prawem**,
3. dane są **zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach** i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
4. Stowarzyszenie **przetwarza tylko takie dane osobowe** i **tylko w takim zakresie, jaki jest niezbędny** dla realizacji celu zgodnego z prawem**;**
5. przetwarzanie danych osobowych przez Stowarzyszenie jest **ograniczone w czasie**. przetwarza dane osobowe **nie dłużej niż jest to niezbędne do realizacji celów**, dla których zostały zebrane;
6. dane są przetwarzane w sposób **przejrzysty** dla osoby, której dane dotyczą;
7. Stowarzyszenie podejmuje rozsądne działania, aby przetwarzane dane osobowe były **zgodne z prawdą i aktualne**, a **nieprawidłowe dane zostały usunięte**;
8. Stowarzyszenie zapewnia **bezpieczeństwo (integralność i poufność) danych osobowych.**

Realizację tych zasad gwarantują dalsze postanowienia Polityki. Jeżeli pewne kwestie nie zostały wprost uregulowane w Polityce, adresaci Polityki podejmują czynności wiążące się z przetwarzaniem danych osobowych w ten sposób, by w jak najpełniejszym stopniu wypełnić powyższe zasady.

1. **Zgodność z prawem.**

**LGD przetwarza wyłącznie te dane osobowe, co do których, w świetle art. 6 ust. 1 RODO, ma uzasadnioną podstawę**. Jeżeli Administrator przetwarza dane osobowe (np. wyłącznie przechowuje), co do których nie ma uzasadnionej podstawy (np. zgody osoby, której dane dotyczą), albo jeżeli nie zna tej podstawy, zaprzestaje przetwarzania danych i niezwłocznie je usuwa.

Jeżeli – mimo braku podstaw do przetwarzania danych osobowych – wykonywanie operacji na tych danych (bądź choćby samo ich przechowywanie) ten jest z jakiegoś powodu ważne dla LGD – Stowarzyszenie podejmuje działania w celu uzyskania podstawy prawnej (np. zgody). Jeżeli działanie takie zakończy się niepowodzeniem LGD zaprzestaje przetwarzania danych i niezwłocznie je usuwa.

Ponieważ zgoda osoby zainteresowanej jest bardzo częstą podstawą przetwarzania danych osobowych, Stowarzyszenie opracowało wzór zgody, stanowiący **załącznik nr 1 do Polityki**.

Należy jednak pamiętać, że **zgoda nie jest jedyną podstawą uprawniającą administratora do przetwarzania danych.** Pozostałe podstawy przetwarzania zostały wymienione w art. 6 ust. 1 RODO. Każda z tych podstaw jest równoważna (nie ma lepszych i gorszych podstaw, każda tak samo „dobrze” legalizuje przetwarzanie danych). Każdy proces, który realizuje LGD, a który wiąże się z przetwarzaniem danych osobowych, powinien być w związku z tym przenalizowany pod kątem podstawy prawnej przetwarzania. Informacje na temat podstawy prawnej danego procesu zamieszczane są w Rejestrze czynności przetwarzania, stanowiącej załącznik do Polityki. Informację o konkretnej podstawie przetwarzania danych osobowych w ramach danego procesu należy przekazać osobie, której dane dotyczą w ramach realizacji tzw. obowiązku informacyjnego (por. pkt 34 Polityki)).

**Nie należy pobierać od osób, których dane dotyczą, zgód na przetwarzanie ich danych, jeżeli np. LGD może przetwarzać te dane na innej podstawie prawnej** (np. nie należy pozyskiwać zgody na przetwarzanie danych osobowych kontrahenta LGD będącego osobą fizyczną, jeżeli dane te są potrzebne wyłącznie do rozliczenia umowy, wystawienia faktury: samodzielną podstawą jest wówczas art. 6 ust. 1 lit. b RODO).

1. **Dane osobowe przetwarzane w Stowarzyszeniu podlegają ochronie.** Oznacza to, że na każdym etapie ich przetwarzania (począwszy od gromadzenia aż do usuwania) dane osobowe są traktowane przez LGD i adresatów Polityki jako dobro (zasób) stanowiący istotną wartość.

Adresaci Polityki, przetwarzając dane osobowe w Stowarzyszeniu, podejmują zatem niezbędne działania, nawet jeśli nie zostały one zapisane wyraźnie w Polityce, aby:

* 1. chronić dane osobowe przed ich utratą, modyfikacją, nieuprawnionym dostępem osób trzecich;
  2. przetwarzanie odbywało się w sposób minimalizujący ryzyko naruszenia ochrony danych osobowych;
  3. przetwarzanie odbywało się zgodnie z prawem, tj., aby każda czynność przetwarzania znajdowała oparcie w konkretnym przepisie prawa (odpowiednia podstawa przetwarzania);
  4. przetwarzanie danych osobowych odbywało się co do zasady w tym celu, dla którego dane zostały zebrane, chyba że Stowarzyszenie może zgodnie z prawem przetwarzać dane także w innym celu (np. dane zostały zebrane w celu zawarcia i wykonywania umowy, dopuszczalne jest późniejsze wykorzystywanie tych danych w sporze sądowym z kontrahentem – na postawie art. 6 ust. 1 lit. f RODO);
  5. minimalizować liczbę gromadzonych, używanych i ujawnianych danych osobowych do tyko tych danych, których przetworzenie jest w danej sytuacji konieczne do osiągnięcia zgodnego z prawem celu;
  6. chronić prywatność osób, których dane są przetwarzane,
  7. projektować takie mechanizmy i procedury, które domyślnie pozwalają na przetwarzanie jak najmniejszej liczby danych, a przetwarzanie ich w większym wymiarze wymaga świadomej decyzji osoby, której dane dotyczą (wyrażonej bezpośrednio w formie oświadczenia, zgody, jak również poprzez jej konkretne zachowanie, działania);
  8. niepotrzebne już dane osobowe były usuwane.

1. Przetwarzanie danych osobowych przez Stowarzyszenie **odbywa się zgodnie z zasadą rozliczalności:** LGD jest odpowiedzialna za dane osobowe, które przetwarza, za zapewnienie ich bezpieczeństwa, a jednocześnie panuje nad wszystkimi procesami przetwarzania danych osobowych w Stowarzyszeniu i je rozumie, nawet jeżeli sama ich nie wykonuje w jakimś zakresie (np. wprowadzanie danych osobowych do chmury).

Zarząd LGD odpowiada za to, by osoby, którym powierzono realizację zadań wiążących się z przetwarzaniem danych osobowych rozumiały ten proces, jego kontekst i funkcjonowanie rozwiązań, z których Stowarzyszenie korzysta przetwarzając dane. W tym celu Stowarzyszenie regularnie szkoli swoich pracowników oraz członków swoich organów, pierwszego dnia wykonywania przez nich swoich obowiązków zaznajamia ich z najważniejszymi regułami dotyczącymi przetwarzania danych osobowych w Stowarzyszeniu.

## Rejestry czynności przetwarzania

1. W celu zapewnienie kontroli nad procesem przetwarzania danych: nad tym jakie dane osobowe, w jakim celu i na jakiej podstawie są przetwarzane, **LGD prowadzi Rejestr czynności przetwarzania**, którego **wzór stanowi załącznik nr 2 do Polityki**. W Rejestrze tym zamieszcza się informacje o przetwarzaniu przez Stowarzyszenie danych osobowych, dla których LGD jest administratorem (tj. decyduje o sposobie i celach przetwarzania).

Prowadzenie tego Rejestru w sposób prawidłowy i jego regularne aktualizowanie jest niezbędne do tego, by w sposób prawidłowy realizować zasadę rozliczalności podaną w RODO.

**Aktualny Rejestr stanowić będzie podstawowe narzędzie, dzięki któremu LGD będzie miało możliwość np. wypełniać żądania osób, których dane przetwarza** (opisanych w dalszej części Polityki, np. prawo do bycia zapomnianym, prawo do sprzeciwu, prawo dostępu do danych), tylko bowiem mając świadomość gdzie (w których systemach, programach) znajdują się dane danej kategorii, LGD może np. usunąć dane określonej osoby fizycznej.

1. W sytuacji, w której LGD przetwarza dane osobowe dla kogoś innego (np. przechowuje takie dane dla innego podmiotu, gromadzi je na zlecenie lub wykonując obowiązek prawny po to, by następnie przekazać je innemu podmiotowi, który będzie decydował co i jak z tymi danymi zrobić, Stowarzyszenie uwzględnia ten fakt w **Rejestrze kategorii czynności przetwarzania dokonywanych w imieniu administratora,** którego **wzór stanowi załącznik nr 3 do Polityki.**
2. **Za prowadzenie Rejestrów, o których mowa w pkt 13 i 14 Polityki odpowiada Zarząd**.

Dokonuje on analizy tego czy aktualne procesy przetwarzania danych przez Stowarzyszenie znajdują odzwierciedlenie w treści Rejestrów, oraz przeprowadza ewentualna aktualizację informacji w tych Rejestrach. Zarząd powinien dokonać aktualizacji informacji zawartych w Rejestrach w każdym przypadku wdrożenia nowego produktu, realizacji nowego projektu itp. wiążącego się z przetwarzaniem nowych danych osobowych lub przetwarzaniu dotychczasowych danych ich w innym celu lub przy użyciu nowych mechanizmów, aplikacji itp.

## Prywatność w fazie projektowania i prywatność jako ustawienie domyślne oraz minimalizacja danych

1. Jeżeli rozpoczęcie lub zmiana określonego procesu (projektu) prowadzonego przez Stowarzyszenie wiąże się z przetwarzanym danych osobowych Zarząd dokonuje analizy tego **projektu pod kątem przestrzegania zasad opisanych w pkt 9 Polityki.**

***Security by design.***

W zależności od wyników, Zarząd analizy podejmuje następujące działania:

* 1. ustala:
     1. jakiego rodzaju dane osobowe będą przetwarzane w ramach procesu
     2. czy wszystkie kategorie danych osobowych, planowanych do pozyskania, są konieczne dla prawidłowego wdrożenia procesu;
     3. jaka jest podstawa prawna takiego przetworzenia;
     4. kiedy należy usunąć dane osobowe pozyskane w trakcie procesu**.**
  2. tak projektuje proces, by zbieranie danych osobowych dotyczyło wyłącznie kategorii danych niezbędnych (np., czy wzór formularza albo aplikacja służąca do gromadzenia danych o podmiotach, nie wymaga podania zbyt wielu informacji) i w razie potrzeby podejmuje działania zmierzające do minimalizacji danych modyfikuje projekt tak, by dane te nie były przetwarzane (np., jeżeli z przepisu prawa lub z charakteru procesu nie wynika obowiązek przetwarzania określonej kategorii danych lub danych określonych osób);
  3. wprowadza **mechanizmy zwiększające ochronę danych osobowych w ramach procesu** (projektu) – jeżeli analiza wskazuje na to, że w ramach projektu (procesu) przetwarzane będą duże ilości danych lub dane o dużym znaczeniu, albo gdy ryzyko naruszenia bezpieczeństwa danych jest znaczne;
  4. dokonuje **aktualizacji danych w Rejestrach**, o których mowa w pkt 13 i 14 Polityki – jeżeli projekt (proces) lub pewne jego cechy nie zostały uwzględnione w Rejestrach;
  5. **rezygnuje z realizacji projektu** (procesu), w zaplanowanym wcześniej zakresie, jeżeli stwierdzi, że przetwarzanie danych osobowych byłoby niezgodne z prawem (np. nie miałoby podstawy prawnej) lub dojdzie do wniosku, że przy pomocy dostępnych (finansowo, organizacyjnie, technicznie) narzędzi i rozwiązań nie jest w stanie zapewnić przestrzegania zasad opisanych w pkt 9 Polityki, a zwłaszcza zapewnić bezpieczeństwa danych.

W przypadku bardziej złożonych procesów/projektów, wynik tej analizy może zostać spisany w formie odrębnego, krótkiego dokumentu, zwłaszcza jeżeli przetwarzanie dotyczy szczególnych kategorii danych w rozumieniu art. 9 ust. 1 RODO, tzw. „**danych wrażliwych**” (dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej).

W celu dokonania takiej analizy LGD wykorzystuje szablon analizy ryzyka, który stanowi **załącznik nr 11 do Polityki**.

***Privacy by default:***

LGD przetwarzając dane osobowe, wprowadza rozwiązania zmierzające do tego, by chroniona byłą prywatność osób, których dane są lub mogłyby być przetwarzane przez Stowarzyszenie. W związku z tym:

1. w przypadku formularzy zawierających zgody na przetwarzanie danych osobowych **nie zaznacza „za składającego oświadczenie” pól potwierdzających zapoznanie się z informacjami lub wyrażenie zgody** (zakaz automatycznego, domyślnego wypełniania checkboxów) – dotyczy to zarówno drukowanych formularzy zgód i informacji, jak i zgód i informacji udzielanych elektronicznie – na stronie internetowej, w ramach aplikacji/programu)
2. jeżeli dana osoba, ma przekazać szereg danych osobowych do LGD na formularzu, który przygotowało Stowarzyszenie i który zawiera pytania na różne tematy, LGD wyraźnie odznacza kategorie danych, których podanie jest konieczne.

***Minimalizacja danych:***

Stowarzyszenie ogranicza zakres gromadzonych danych osobowych do minimum niezbędnego do realizacji celu, dla którego są one zbierane:

1. jeżeli wykorzystanie określonej kategorii danych osobowych nie jest konieczne dla wykonania przez LGD danego zadania, a jedynie ułatwi LGD wykonanie pewnych obowiązków związanych z usługą, Stowarzyszenie nie uzależnia wykonania tego zadania od podania tych „dodatkowych” danych (np. nie warunkuje się udziału w szkoleniu od podania daty i miejsca urodzenia lub numeru PESEL, ale można w formularzu zgłoszenia na szkolenie zostawić te pola wraz z informacją, że ich wypełnienie pozwoli przygotować spersonalizowany certyfikat potwierdzający udział w szkoleniu);
2. jeżeli Stowarzyszenie przetwarza dane osobowe uzyskane bezpośrednio od osoby, której dane dotyczą, wykonuje obowiązki informacyjne wynikające z RODO (formularze informacyjne stanowiące załączniki do Polityki), w szczególności informuje każdą osobę o tym, czy podanie przez nią danych osobowych jest obowiązkiem ustawowym lub umownym, ewentualnie jakie są konsekwencje niepodania danych osobowych (np. brak możliwości uzyskania punktów w ramach oceny wniosku na podstawie konkretnego kryterium).

## Przetwarzanie danych osobowych przez osoby upoważnione

1. Przetwarzanie danych osobowych, których administratorem jest LGD, jest dopuszczalne jedynie przez osoby fizyczne do tego upoważnione i jedynie w takim zakresie, w jakim określa to upoważnienie. **Upoważnień udziela Zarząd**. Udzielanie upoważnień może zostać powierzone pracownikowi ds. bezpieczeństwa, o którym mowa w pkt 27 Polityki.

W celu spełnienia zasady rozliczalności opisanej w RODO – LGD przyjmuje następujące zasady dotyczące tego kto i na jakich zasadach może w ramach Stowarzyszenia przetwarzać dane osobowe.

* 1. Zarząd pozwala przetwarzać dane osobowe **jedynie tym osobom i jedynie w takim zakresie, który jest niezbędny do wykonywania ich zadań**;
  2. upoważnień udziela się pracownikom LGD oraz osobom, które są zatrudnione w LGD na podstawie umów cywilnoprawnych, jeżeli wykonują zadania dla Stowarzyszenia korzystając ze sprzętu i infrastruktury LGD;
  3. upoważnień udziela się pisemnie, w dniu zawarcia z daną osobą umowy lub dopuszczenia danej osoby do wykonywania czynności związanych z dostępem do danych osobowych;
  4. upoważnienie wskazuje zakres danych, do jakich osoba upoważniona ma dostęp, ewentualne czynności przetwarzania danych, które osoba upoważniona może wykonywać, oraz okres, na jaki udzielono upoważnienie. **Wzór upoważnienia stanowi załącznik nr 4 do Polityki;**
  5. fakt udzielenia upoważnienia wpisuje się do Rejestru upoważnień, którego wzór stanowi **załącznik nr 5 do Polityki**.

**Upoważnień nie udziela się członkom organów Zarządu LGD**, którzy w okresie pełnienia swoich funkcji mają dostęp do wszystkich czynności przetwarzania w Stowarzyszeniu, wykonując zadania administratora danych.

**Członkowie Komisji Rewizyjnej LGD również nie otrzymują upoważnień**, lecz są uprawnieni wyłącznie do dostępu do danych osobowych przetwarzanych przez Stowarzyszenie, w takim zakresie, w jakim jest to niezbędne do realizacji ich uprawnień kontrolnych wynikających ze Statutu LGD.’

Ze względu na fakt, że – zgodnie z ustawą o RLKS – członkiem Rady Stowarzyszenia może być osoba prawna, aby dokładnie rejestrować do jakich danych miały dostęp określone osoby fizyczne w ramach funkcjonowania Rady, członkom tego organu udziela się upoważnień i ten fakt wpisuje się do Rejestru upoważnień.

**Członkom LGD udziela się upoważnień**, jeżeli w ramach wykonywania zadań dla Stowarzyszenia, mają mieć dostęp do danych osobowych przetwarzanych przez LGD. Upoważnień nie udziela się, jeżeli te zadania realizują za wynagrodzeniem, na podstawie umowy (są wówczas taktowani jak inne osoby wykonujące umowy cywilnoprawne dla Stowarzyszenia, którym udziela się upoważnienia albo jak podmioty, z którymi należy zawrzeć umowę powierzenia danych, jeżeli wykonują zadania z wykorzystaniem własnego sprzętu, infrastruktury, na własne ryzyko i rachunek, w formule B2B).

Podział osób upoważnionych na grupy przedstawia poniższa tabela:

|  |  |
| --- | --- |
| **KATEGORIA OSÓB** | **ZAKRES DANYCH OSOBOWYCH, KTÓRE CZŁONEK GRUPY MOŻE PRZETWARZAĆ** |
| **Członkowie Zarządu** | Wszystkie dane osobowe przetwarzane przez Stowarzyszenie |
| **Członkowie Komisji Rewizyjnej** | Wszystkie dane osobowe przetwarzane przez Stowarzyszenie, ale jedynie w zakresie wglądu do nich (bez możliwości modyfikacji, usuwania, itp.) – w zakresie niezbędnym do wykonywania zadań statutowych. |
| **Członkowie Rady** | Dane osobowe zawarte we wnioskach o przyznanie pomocy załącznikach do wniosków, protestach, wnioskach o aneks do umowy o przyznanie pomocy |
| **Pracownicy biura Stowarzyszenia** | Dane osobowe przetwarzane przez Stowarzyszenie dotyczące spraw, które mieszczą się w zakresie ich obowiązków pracowniczych. Zakres danych i czynności ograniczony upoważnieniem. |
| **Stali współpracownicy Stowarzyszenia (osoby zatrudnione na umowach cywilnoprawnych, korzystający z infrastruktury Stowarzyszenia)** | Dane osobowe przetwarzane przez Stowarzyszenie niezbędne do wykonania zadań w ramach umowy ze Stowarzyszeniem |
| **Stażyści, wolontariusze** | Dane osobowe niezbędne do realizacji zadań określonych w dokumencie na podstawie którego te osoby wykonują świadczenia dla Stowarzyszenia |
| **Członkowie Stowarzyszenia** | Dane osobowe niezbędne do realizacji zadań dla Stowarzyszenia. |

Upoważnienia do przetwarzania danych osobowych, które zostały udzielone przed wejście w życie Polityki (tj. na podstawie Polityki bezpieczeństwa wraz z Instrukcją zarządzania systemem informatycznym, które zostały przyjęte uchwałą nr XXII/56/2017/Z.) pozostają w mocy – nie ma potrzeby osobom dotychczas upoważnionym odwoływać udzielonych upoważnień, po to tyko żeby przyznać im je po chwili na nowo, w oparciu o Politykę.

## Powierzenie podmiotom trzecim danych, których administratorem jest LGD

1. Przetwarzanie danych osobowych przez LGD odbywa się nie tylko przy wykorzystaniu własnych pracowników (organów) i środków technicznych i organizacyjnych, ale również może być prowadzone za pomocą podmiotów trzecich (podmiotów przetwarzających).

Podmiot przetwarzający przetwarza dane osobowe, których administratorem jest LGD, wykonując określone zadania (usługi) dla Stowarzyszenia i wykorzystując swoje zaplecze organizacyjne i techniczne (np. swój komputer, niepodpięty do systemu LGD, swoje programy, pracowników i biuro).

**Podmiotowi przetwarzającemu nie udziela się upoważnienia**, o którym mowa w pkt 17 Polityki.

**Decydujące dla odróżnienia podmiotu przetwarzającego od osoby, której należy udzielić upoważnienia**, jest to, czy osoba przeprowadzająca operacje na danych osobowych   
(np. wyświetlająca, przechowująca lub modyfikująca je) co do zasady realizuje te czynności korzystając z własnej infrastruktury, sprzętu, programów (są to cechy charakteryzujące przetwarzanie przez podmiot przetwarzający), czy też na sprzęcie, programach, w pomieszczeniach Stowarzyszenia (to z kolei są cechy charakteryzujące sytuacje, w których należy udzielić upoważnienia). Osoby fizyczne prowadzące działalność gospodarczą, które przetwarzają dane osobowe, których administratorem jest LGD, z reguły są podmiotami przetwarzającymi, ponieważ cechą działalności gospodarczej jest prowadzenie czynności we własnym imieniu, na własny rachunek i ryzyko.

1. **Powierzenie danych do przetwarzania podmiotowi trzeciemu może nastąpić po uprzedniej weryfikacji, czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych,** by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą:

W celu zweryfikowania warunków pozwalających na powierzenie przetwarzania danych osobowych:

* 1. jeżeli LGD po raz pierwszy nawiązuje współpracę z podmiotem przetwarzającym, przed podjęciem decyzji o powierzeniu danych, zwraca się do niego z prośbą o wypełnienie kwestionariusza pozwalającego na weryfikację, czy spełnia on wymagania pozwalające na powierzenie mu danych osobowych.

Wzór kwestionariusza stanowi **załącznik nr 6 do Polityki**.

Weryfikacja odbywa się poprzez analizę odpowiedzi na kwestionariuszu: zaznaczenie odpowiedzi „NIE” w którymkolwiek pytaniu z pierwszej części kwestionariusza świadczy o tym, że podmiot nie daje wystarczających gwarancji, by powierzyć mu dane do przetwarzania. Odpowiedzi „NIE” w drugiej części mogą być traktowane jako okoliczność przemawiająca za wyborem innego wykonawcy.

* 1. jeżeli Stowarzyszenie nie współpracowało wcześniej z podmiotem, ale podmiot ten, ze względu na charakter swojej działalności, wielkość, stosowaną praktykę (np. właściciel serwerów, dostawca globalnych aplikacji informatycznych, firma telekomunikacyjna), nie wypełnia kwestionariusza, lub można oczekiwać, że go nie wypełni, zweryfikowanie tego, czy spełnia gwarancje, o których mowa wyżej, odbywa się poprzez analizę regulaminu świadczenia usług przez taki podmiot, deklarowanie przez niego stosowania mechanizmów certyfikacji lub zatwierdzonych kodeksów postępowania, o których mowa w RODO, norm ISO dotyczących ochrony danych lub deklarowanie przestrzegania innych zasad pozwalających uznać, że zabezpieczenie powierzonych danych osobowych będzie odpowiednie.

W sytuacjach, w których podmiot przetwarzający miałby dokonywać czynności jedynie sporadycznie, wobec niewielkiej ilości danych osobowych, nie obejmując danych wrażliwych, możliwe jest zrezygnowanie ze stosowania powyższych sposobów weryfikacji.

1. Powierzając podmiotowi trzeciemu dane osobowe, **LGD weryfikuje, gdzie ten podmiot ma siedzibę i gdzie będzie dokonywał czynności związanych z przetwarzaniem danych**. Stowarzyszenie wybiera podmioty, które przetwarzają dane osobowe na terenie Unii Europejskiej, Europejskiego Obszaru Gospodarczego lub w tzw. krajach bezpiecznych[[1]](#footnote-1) lub też – w przypadku firm amerykańskich – zostały objęte programem *Privacy shield*. Sprawdzenia dokonuje się w ramach kwestionariusza, o którym mowa wyżej, bądź sprawdzając informacje podane przez ten podmiot w jego Regulaminie wykonywania usług, na jego stronie internetowej itp.

Wybór podmiotu, który nie spełnia powyższych warunków jest dopuszczalny jedynie wyjątkowo.

1. W związku z przyjęciem Polityki oraz wejściem w życie RODO, Stowarzyszenie przeprowadzi audyt swoich dotychczasowych podmiotów przetwarzających pod kątem spełniania przez te firmy wymagań RODO i w razie potrzeby dokona zmian w umowach zawartych z tymi podmiotami   
   (ew. zweryfikuje, czy w związku z wejściem w życie RODO podmioty te zmodyfikowały swoje regulaminy świadczenia usług).

W przypadku niedostosowania się obecnych podmiotów przetwarzających do wymagań nowych przepisów, LGD będzie zmuszona zrezygnować z usług tych podmiotów.

1. LGD może powierzyć innemu podmiotowi przetwarzanie danych osobowych, których jest administratorem, **jedynie na podstawie umowy lub innego instrumentu prawnego**   
   (np. powierzenie przetwarzania może wynikać z przepisu prawa lub statutu organizacji, której członkiem jest LGD, regulaminu świadczenia usług, w ramach których mają być przetwarzane dane osobowe powierzone przez Stowarzyszenie, którego akceptacja jest konieczna do świadczenia usług).
2. W celu powierzenia przetwarzania danych osobowych, LGD:
3. zawiera umowę powierzenia przetwarzania albo w umowie dotyczącej świadczenia danej usługi zamieszcza klauzulę powierzenia danych do przetwarzania.

Wzór umowy powierzenia danych osobowych (który – po ewentualnych zmianach redakcyjnych – może zostać wykorzystany także jako klauzula w umowie, której przedmiot jest szerszy niż samo powierzenie danych osobowych) stanowi **załącznik nr 7 do Polityki**;

1. jeżeli dany podmiot nie wyraża zgody na zawarcie umowy zgodnej ze wzorem (lub zamieszczenia w umowie stosownej klauzuli), dopuszczalne jest powierzenie danych do przetwarzania, o ile w umowie, której zawarcie proponuje podmiot przetwarzający (lub w innym dokumencie, na podstawie którego będzie odbywało się wykonywanie przez niego usług, mającego dla tego podmiotu charakter wiążący – np. regulaminie świadczenia usług ) zawarte są postanowienia, o których mowa w art. 28 ust. 3 RODO.

## LGD jako podmiot przetwarzający

1. Jeżeli LGD przetwarza dane osobowe występując w charakterze podmiotu przetwarzającego (czyli wykonuje wobec danych osobowych określone czynności dla innego podmiotu, który jest ich administratorem, np. wdrażając jakiś projekt):
   1. stosuje wobec danych osobowych **co najmniej takie środki bezpieczeństwa, jak wobec danych osobowych, których jest administratorem** (chyba, że umowa lub inny instrument prawny, na podstawie którego przetwarza dane dla innego podmiotu przewiduje dalej idące środki bezpieczeństwa – wtedy stosuje te środki);
   2. zamieszcza stosowną informację w **Rejestrze kategorii czynności przetwarzania** dokonywanych w imieniu administratora (wzór rejestru stanowi załącznik nr 4 do Polityki);
   3. **nie może zlecać wykonywania jakichkolwiek czynności wobec takich danych osobowych innym podmiotom** (tj. innym osobom niż pracownicy i organy LGD, (tzw. „**podpowierzenie**”), chyba że:
      1. uzyskał zgodę administratora tych danych, lub
      2. uprzedził administratora tych danych o tym, że zamierza zlecić konkretnemu podmiotowi wykonywanie czynności związanych z tymi danymi, a administrator nie wyraził sprzeciwu na takie podpowierzenie;
   4. w przypadku wystąpienia zdarzenia, które może być klasyfikowane jako **naruszenie bezpieczeństwa ochrony danych, LGD niezwłocznie informuje administratora tych danych** o takim zdarzeniu i udziela mu wszelkiej niezbędnej pomocy   
      w celu zapobieżenia lub ograniczenia skutków takiego zdarzenia.

Opisana wyżej sytuacja, a co za tym idzie konieczność uzupełnienia Rejestru kategorii czynności przetwarzania może mieć miejsce w sytuacji, gdy np. LGD będzie przechowywało dokumentacje innego podmiotu. Co do zasady jednak – ze względu na specyfikę funkcjonowania LGD – taka sytuacja nie będzie jednak częsta.

# ROZDZIAŁ III OSOBY ODPOWIEDZIALNE W STOWARZYSZENIU ZA NADZÓR NAD PRZETWARZANIEM DANYCH OSOBOWYCH

## Zadania Zarządu

1. W imieniu Administratora **kierunkowe, najważniejsze decyzje dotyczące przetwarzania danych osobowych** przez Stowarzyszenie, ich ochrony, realizacji obowiązków ustawowych w tym zakresie oraz współpracy z PUODO i innymi organami lub podmiotami, **podejmuje Zarząd.**
2. Do kompetencji Zarządu należy w szczególności:
3. powoływanie i odwoływanie pracownika ds. bezpieczeństwa informacji;
4. udzielanie i cofanie pracownikom i członkom pozostałych organów Stowarzyszenia upoważnień do przetwarzania danych osobowych (kompetencja może zostać przekazana pracownikowi ds. bezpieczeństwa);
5. zgłaszanie, w stosownych przypadkach, PUODO oraz osobom, których dane osobowe zostały naruszone, informacji o naruszeniu bezpieczeństwa danych osobowych;
6. podejmowanie stosownych działań (np. dyscyplinujących) w przypadku stwierdzenia naruszenia przez adresatów Polityki zasad przetwarzania danych osobowych przez Stowarzyszenia, określonych w przepisach prawa i Polityce;
7. podejmowanie decyzji o powierzeniu podmiotowi trzeciemu przetwarzania danych osobowych, których administratorem jest przetwarzający, podejmowanie decyzji dotyczących dalszej współpracy z takim podmiotem w przypadku stwierdzenia naruszenia przez niego warunków przetwarzania danych osobowych administrowanych przez Stowarzyszenie;
8. przeprowadzanie okresowych audytów, aktualizacja i dokonywanie zmian Polityki;
9. zapewnianie, w razie potrzeby, zewnętrznych szkoleń dla pracowników i członków organów Stowarzyszenia z obowiązujących przepisów w zakresie ochrony danych osobowych oraz z postanowień Polityki;
10. w przypadku zatwierdzenia przez PUODO kodeksu przetwarzania danych osobowych, adresowanego do organizacji społecznych, lub organizacji, których wielkość i profil działalności jest zbliżony do tego, jaki charakteryzuje Stowarzyszenie Zarząd podejmie decyzję o podjęciu działań zmierzających do stosowania tego kodeksu (analogiczne działania zostaną podjęte w sytuacji uzyskania możliwości ubiegania się o certyfikację, jeżeli warunki certyfikacji będą adresowane do podmiotów o podobnej wielkości i profilu działalności, co Stowarzyszenie).

## Pracownik ds. bezpieczeństwa informacji

1. **W celu koordynowania w Stowarzyszeniu bieżących procesów związanych z przetwarzaniem** danych osobowych, Zarząd może wyznaczyć pracownika odpowiedzialnego za te kwestie (**pracownika ds. bezpieczeństwa informacji**). Pierwszym pracownikiem ds. bezpieczeństwa informacji zostaje dotychczasowy Administrator Bezpieczeństwa Informacji.
2. Pracownik ds. bezpieczeństwa informacji **nie jest inspektorem ochrony danych** w rozumieniu art. 37 RODO – jego wyznaczenie ma na celu wyłącznie przypisanie jednej osobie, w sposób stały zaangażowanej w bieżącą pracę Stowarzyszenia, a zwłaszcza biura Stowarzyszenia, odpowiedzialności za zagadnienia związane z zapewnieniem przetwarzania danych osobowych zgodnie z przepisami, Polityką – jednak bez nadawania temu pracownikowi charakterystycznej dla inspektora ochrony danych, pozycji w organizacji.
3. Wyznaczenie pracownika ds. bezpieczeństwa informacji może zostać dokonane poprzez pismo Zarządu przekazane pracownikowi (wówczas konieczne może być zawarcie aneksu do umowy o pracę) lub przypisanie poniższych obowiązków w sposób wyraźny do danego stanowiska pracy w biurze Stowarzyszenia (jako element obowiązków umownych, wynikających np. z opisu stanowiska) poprzez uchwałę Zarządu,
4. Do zadań pracownika ds. bezpieczeństwa informacji należy:
5. czuwanie nad przestrzeganiem postanowień Polityki w ramach bieżącego funkcjonowania Stowarzyszenia, a zwłaszcza biura;
6. prowadzenie i aktualizacja Rejestru osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu;
7. monitorowanie przepisów prawnych w kontekście zasad przetwarzania danych osobowych przez Stowarzyszenie;
8. monitorowanie stosowanych przez Stowarzyszenie procedur oraz środków technicznych i organizacyjnych w kontekście ich adekwatności i aktualności, w szczególności tego, czy zapewniają poufność, dostępność i integralność danych osobowych przetwarzanych przez Stowarzyszenie;
9. sygnalizowanie Zarządowi konieczności dokonania zmian w Polityce;
10. zaznajamianie nowych pracowników Stowarzyszenia z zasadami przetwarzania danych osobowych przez Stowarzyszenie;
11. identyfikowanie i dokumentowanie oraz informowanie Zarządu o wykrytych przypadkach naruszenia ochrony danych osobowych lub nieprzestrzegania Polityki przez ich adresatów, dokonywanie wpisów w Rejestrze naruszeń ochrony danych osobowych;
12. utrzymywanie bieżącego kontaktu z podmiotami przetwarzającymi w celu weryfikacji, czy przestrzegają oni warunków przetwarzania danych osobowych, których administratorem jest Stowarzyszenie, informuje Zarząd o każdym przypadku zdarzenia identyfikowanego jako naruszenie ochrony .danych osobowych.

## Przewodniczący Komisji Rewizyjnej LGD

1. Przewodniczący organów Stowarzyszenia (tj. Rady i Komisji Rewizyjnej) są odpowiedzialni za to, by przetwarzanie danych osobowych w ramach funkcjonowania organów, którymi kierują, było zgodne z przepisami prawa oraz Polityką. W szczególności są odpowiedzialni za:
2. zaznajamianie członków organów z zasadami przetwarzania danych osobowych przez Stowarzyszenie w związku z pracami danego organu;
3. pracę danego organu oraz za to, by sporządzana w efekcie prac organów dokumentacja była zgodna z Polityką (w szczególności realizowała wymóg minimalizowania danych osobowych, pseudonimizacji, by dane osobowe były należyte zabezpieczone);
4. identyfikowanie i dokumentowanie oraz informowanie Zarządu o wykrytych przypadkach naruszenia ochrony danych osobowych lub nieprzestrzegania Polityki przez członków danego organu;
5. stosowanie przez dany organ rozwiązań zgodnych z rozporządzeniem RODO, w szczególności zmierzających do ograniczenia ilości przetwarzanych danych (minimalizacji danych), ograniczenia liczb kopii danych osobowych, sporządzenie kopii zapasowych z danych, które organ, wykorzystuje.
6. Niezależnie od zadań wskazanych w ust. 1, Przewodniczący Rady:
7. monitoruje stosowane przez Stowarzyszenie procedury i kryteria oceny wniosków oraz środki techniczne i organizacyjne, obowiązujące z związku z oceną operacji i ustalaniem kwoty wsparcia w ramach realizacji LSR – w kontekście ich adekwatności i aktualności, w szczególności tego, czy zapewniają poufność, dostępność i integralność danych osobowych zawartych we wnioskach i załącznikach,
8. sygnalizuje Zarządowi konieczność dokonania zmian w procedurach i kryteriach stosowanych przez Radę w kontekście zapewnienia lepszego poziomu ochrony danych.

## ROZDZIAŁ IV PRAWA OSÓB TRZECICH I SPOSÓB POSTĘPOWANIA PRZEZ STOWARZYSZENIE Z WNIOSKAMI TYCH OSOB

## Ogólne zasady

1. Stowarzyszenie podejmuje niezbędne działania, aby prawa osób, których dane są przetwarzane przez LGD, a zwłaszcza uprawnienia opisane w art. 12-22 RODO były przestrzegane.

Informacje zawarte w tym rozdziale dotyczą procedury realizowania uprawnień osób fizycznych opisanych w przywołanych wyżej przepisach rozporządzenia RODO. Stowarzyszenie zamieszcza ją w tym miejscu, by w Polityce zostały uregulowane kwestie odnoszące się do najważniejszych aspektów związanych z przetwarzaniem danych osobowych przez Stowarzyszenie (tak, by w jednym dokumencie zostały zawarte wskazówki dotyczące postępowania w najbardziej prawdopodobnych sytuacjach wiążących się z wykonywaniem uprawnień osób, których dane dotyczą).

1. Realizując uprawnienia osoby, której dane dotyczą, LGD postępuje tak, by – działając w dobrej wierze – nie naruszyć swoim postępowaniem praw tej osoby lub praw innej osoby.

Dlatego, w przypadku wystąpienia przez daną osobę do LGD z żądaniem określonego działania związanego z jej danymi osobowymi, Stowarzyszenie:

1. **ustala tożsamość osoby, która zwróciła się o wykonanie przez LGD określonego działania związanego z danymi osobowymi**. Ustalenie tożsamości powinno zostać dokonane w ten sposób, że LGD upewnia się, że dana osoba, która zwróciła się do Stowarzyszenia, jest tą, za którą się podaje, a działania, których oczekuje, rzeczywiście dotyczą jej danych osobowych:

* jeżeli żądanie zostało dokonane osobiście, a adresat Polityki, który otrzymał żądanie, nie ma pewności co do tożsamości występującego z żądaniem, prosi go o okazanie dowodu osobistego lub o przedstawienie informacji potwierdzającej tożsamość wnioskującego o podjęcie określonych działań;
* jeżeli żądanie zostało złożone w innej formie, LGD weryfikuje, czy żądanie zostało przesłane do Stowarzyszenia z tego samego adresu, numeru telefonu itp., który został przypisany w dokumentacji prowadzonej przez LGD do osoby, której dane mają zostać przekazane;
* jeżeli LGD, mimo podjęcia opisanych wyżej działań, nadal nie ma pewności co do tożsamości podmiotu, który zwrócił się do niego z określonym żądaniem dotyczącym danych osobowych danej osoby, odmawia uczynieniu zadość temu żądaniu, ale wyjaśnia wnioskującemu przyczyny takiej decyzji;
* wystąpienie przez LGD o przedstawienie przez daną osobę informacji pozwalającej ustalić jej tożsamość nie jest konieczne, gdy nie ma wątpliwości co do tożsamości osoby zwracającej się z żądaniem związanym z przetwarzaniem danych osobowych;

1. ustala – jeżeli żądanie zostało sformułowane w sposób nieprecyzyjny – dokładną treść żądania (np. czy wnioskujący domaga się wyłącznie dostępu do danych osobowych, czy również ich skopiowania).
2. Realizacja uprawnień osoby, której dane osobowe przetwarza LGD, wymaga komunikacji z tą osobą. W celu właściwego wypełnienia obowiązków Stowarzyszenia, wprowadza się następujące reguły dotyczące komunikacji z osobami, których dane przetwarza LGD.

* komunikacja powinna odbywać się za pomocą zwięzłych, przejrzystych i zrozumiałych komunikatów, słownictwo powinno być proste,
* powoływanie się w komunikacji na przepisy prawa, cytowanie fragmentów aktów prawnych, pełnych tytułów ustaw i rozporządzeń, numerów artykułów – jest dopuszczalne jedynie wyjątkowo, gdy bez ich powołania nie da się wypełnić obowiązków Stowarzyszenia, ich przywołanie jest niezbędne dla wskazania podstawy decyzji odmownej itp., gdy wnioskujący domaga się wyjaśnienia podstawy prawnej określonego działania, przytoczenia przepisów, itp.;
* **komunikacja powinna odbywać się na piśmie**, w tej samej formie, w jakiej zwróciła się osoba trzecia, żądająca od LGD określonego działania;
* jeżeli osoba, której dane dotyczą, tego zażąda, **informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą**;
* **udzielenie odpowiedzi** na żądanie osoby zainteresowanej powinno nastąpić **w terminie miesiąca** od dnia zgłoszenia wniosku. Jeżeli wykonanie w tym terminie żądania danej osoby nie jest możliwe, należy w terminie miesiąca poinformować o tym fakcie i przewidywanym terminie spełnienia żądania (nie może być on dłuższy niż łącznie 3 miesiące od dnia wystąpienia z żądaniem);
* **jeżeli Stowarzyszenie dojdzie do wniosku, że podmiot, który zwrócił się do niego z określonym żądaniem nie jest uprawniony do uzyskania tego, o co się zwrócił, jest o tym wyraźnie informowany** – odmowa spełnienia żądania danej osoby powinna zostać przekazana w terminie miesiąca, od dnia wystąpienia przez dany podmiot z żądaniem. Do informacji odmownej dołącza się wzmiankę o możliwości wniesienia skargi do PUODO lub skorzystania z sądowej drogi dochodzenia swoich uprawnień;
* z zastrzeżeniem wyjątków opisanych w niżej komunikacja i działania podejmowane na mocy art. 15–22 i 34 RODO są **wolne od opłat**;
* jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności maja charakter ustawiczny, LGD może:
* pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
* odmówić podjęcia działań w związku z żądaniem.

## Obowiązek informacyjny

1. **Zasady podawania informacji o przetwarzaniu danych osobowych, w przypadku zbierania tych danych od osoby, której dane dotyczą.**

Jeżeli Stowarzyszenie pozyskuje dane osobowe bezpośrednio od osoby, której te dane dotyczą (np. gdy przetwarzanie danych osobowych opiera się na zgodzie osoby zainteresowanej, albo gdy osoba podaje dane osobowe w celu zawarcia lub wykonania umowy ze Stowarzyszeniem), **Stowarzyszenie – przed pozyskaniem danych – informuje taką osobę o okolicznościach wskazanych w art. 13 RODO**.

**Obowiązek podania informacji nie jest tożsamy z obowiązkiem uzyskania zgody**. Dlatego, pomimo pozyskania zgody danej osoby na przetwarzanie jej danych, konieczne jest jej poinformowanie o kwestiach dotyczących przetwarzania jej danych osobowych.

Przekazanie informacji może w szczególności polegać na:

1. przekazaniu osobie zainteresowanej wydrukowanej informacji i potwierdzeniu zapoznania się z tą informacją w postaci podpisu osoby zainteresowanej;
2. umieszczeniu informacji pod lub na drugiej stronie formularza z zapytaniem o zgodę na przetwarzanie danych osobowych – wówczas z samego faktu podpisania zgody na przetwarzanie danych osobowych można domniemywać, że osoba zainteresowana zapoznała się z informacjami dołączonymi do zapytania o zgodę;
3. jeżeli pozyskiwanie danych osobowych odbywa się za pośrednictwem programu lub strony internetowej – poprzez takie skonfigurowanie programu lub strony, by rozpoczęcie przetwarzania danych osobowych było możliwe dopiero po wyświetleniu strony z informacją lub zaznaczeniu w odrębnym checkboxie, że dana osoba zapoznała się z informacjami.

**Nie rekomenduje się realizowanie obowiązku informacyjnego poprzez ustne przekazanie wymaganych informacji** – ze względu na obowiązującą na gruncie RODO zasadę rozliczalności, nakazującą administratorowi realizować obowiązki w sposób pozwalający w razie potrzeby wykazać ich spełnienie.

Wzór klauzuli informacyjnej, przekazywanej osobie, której dane dotyczą, w przypadku pozyskania bezpośrednio od niej jej danych osobowych, stanowi **załącznik nr 8 do Polityki**. Klauzula powinna być modyfikowana w razie potrzeby – m.in. o zmianie, w zależności od sytuacji podlegać powinna podstawa prawna i cele przetwarzania.

W celu realizacji obowiązku informacyjnego określonego w art. 13 RODO, LGD:

* zamieszcza **Politykę prywatności** na każdej witrynie internetowej, którą administruje.   
  W Polityce prywatności zamieszcza się informacje na temat przetwarzania danych osobowych osób odwiedzających daną witrynę. Polityka powinna zawierać informacje wskazane w art. 13 RODO, a znajdujące odzwierciedlenie w klauzuli informacyjnej stanowiącej załącznik do Polityki, oraz informacje na temat mechanizmów śledzenia aktywności osób odwiedzjących stronę, pliki cookies, mechanizmy Google Analitics, itp.);
* w przypadku rejestracji nowych członków LGD, do formularza deklaracji członkowskiej należy dołączyć klauzulę informacyjną;
* w przypadku umów zawieranych przez LGD, jako osobny załącznik, należy przewidzieć klauzulę informacyjną, bądź – co najmniej przed zawarciem umowy należy poinformować kontrahenta o kwestiach określonych w art. 13 RODO, a w treści umowy zamieścić oświadczenie kontrahenta, że z tymi informacjami się zapoznał;
* w przypadku składania przez wnioskodawców dokumentów w ramach naborów ogłoszonych w związku z realizacją LSR, wnioskodawcy wraz z kopią pierwszej strony wniosku należy przekazać klauzule informacyjną;
* klauzulę informacyjną należy przekazać również w przypadku doradztwa świadczonego w związku z realizacją LSR;
* na formularzach zgłoszeniowych na wydarzenia organizowane przez LGD lub na listach obecności z takich wydarzeń zostaną zamieszczone informacje znajdujące się na klauzuli informacyjnej, zaś w przypadku rejestracji na takie wydarzenia za pośrednictwem formularzy internetowych, w panelu rejestracyjnym zostanie umieszczony wyraźnie oznaczony link do informacji zawartych w klauzuli (ew. można wprowadzić rozwiązanie, że rejestracja jest możliwa dopiero po kliknięciu checkboxa o zapoznaniu się z tymi informacjami).

1. **Zasady podawania informacji o przetwarzaniu danych osobowych, w przypadku ich zbierania w inny sposób niż od osoby, której danej dotyczą.**

Jeżeli Stowarzyszenie pozyskuje dane osobowe w inny sposób niż bezpośrednio od osoby, której te dane dotyczą (np. gdy od podmiotu trzeciego otrzymuje listę uczestników jakiegoś wydarzenia, którego organizatorem jest LGD) **Stowarzyszenie ma obowiązek poinformować taką osobę o okolicznościach wskazanych w art. 14 RODO.**

W tym celu przekazuje tym osobom informacje zawarte w **załączniku nr 9 do Polityki**   
(np. przesyłając im je pocztą elektroniczną lub umieszczając w widocznym miejscu w sali, w której odbywa się wydarzenie).

**Informacje, powinny zostać przekazane zainteresowanej osobie niezwłocznie, nie później jednak niż w terminie miesiąca od ich pozyskania**. W pewnych sytuacjach należy te informacje jednak podać **wcześniej:**

1. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej **przy pierwszej takiej komunikacji z osobą, której dane dotyczą**;
2. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej **przy ich pierwszym ujawnieniu.**
3. **Obowiązki informacyjne opisane w pkt 36 i 37 Polityki nie dotyczą danych osobowych, które zostały zebrane przez Stowarzyszenie przed 25 maja 2018 r.** (np. dane członków Stowarzyszenia, dane dawnych klientów, itp.). Jeżeli jednak z osobami tymi LGD ma stały kontakt, Stowarzyszenie gromadzi kolejne informacje o tym osobach, to obowiązek ten należy wykonać również wobec osób „zarejestrowanych” w bazach LGD przed 25 maja 2018 r.

## Prawo dostępu do danych osobowych

1. **Osoba, której dane dotyczą, jest uprawniona do uzyskania od LGD:**
   1. **potwierdzenia, czy Stowarzyszenie przetwarza dane osobowe jej dotyczące**.

W przypadku zgłoszenia się do LGD osoby z wnioskiem o przekazanie takiej informacji:

* w celu udzielenia odpowiedzi na tak zadane pytanie, Stowarzyszenie w pierwszej kolejności identyfikuje osobę zwracającą się z takim wnioskiem (patrz pkt 34 Polityki);
* po pozytywnej identyfikacji Stowarzyszenie weryfikuje w swojej dokumentacji, zarówno papierowej, jak i elektronicznej, we wszystkich programach i na wszystkich nośnikach, czy posiada jakiekolwiek dane, które może przypisać do tej osoby (tj. Stowarzyszenie ma pewność, że to są dane tej osoby);
* po dokonaniu weryfikacji, Stowarzyszenie informuje osobę, która zwróciła się z takim żądaniem, o wyniku weryfikacji (tj. przesyła – tym samym kanałem informacyjnym, którym otrzymała zapytanie, lub kanałem informacyjnym, który wskazała osoba zadająca pytanie – informację, że LGD przetwarza albo nie przetwarza dane osobowe dotyczące osoby pytającej);
  1. **uzyskania dostępu tych danych** (np. możliwość obejrzenia ich w programie używanym przez Stowarzyszenie, ale jedynie w obecności osoby upoważnionej do przetwarzania danych w Stowarzyszeniu i przy zachowaniu środków bezpieczeństwa, w celu ujawnienia funkcjonujących w Stowarzyszeniu zabezpieczeń, wglądu w dokumenty papierowe zawierające informacje o danej osobie – przy zakryciu danych osobowych dotyczących innych osób);
  2. **uzyskania informacji** na temat:
* celu przetwarzania danych;
* kategorii odnośnych danych osobowych (tj. wskazania, czy jest to tylko imię i nazwisko, czy również PESEL, miejsce zamieszkania, wykształcenie);
* odbiorców lub kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
* planowanego okresu przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
* możliwości żądania od LGD sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz możliwości wniesienia sprzeciwu wobec takiego przetwarzania;
* prawa do wniesienia skargi do PUODO;
* jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich informacji o źródle danych;
  1. **uzyskania kopii danych osobowych**, które przetwarza LGD (**pierwsza kopia danych sporządzana jest bezpłatnie**, za kolejne kopie (tj. informacje nieróżniące się swoją treścią od wcześniej przekazanych danej osobie Stowarzyszenie) może pobrać opłatę w wysokości równej kosztom pracy i materiałów niezbędnych do przygotowania kopii. Stowarzyszenie przesyła osobie występującej z żądaniem taką kopię drogą elektroniczną, chyba, że osoba, której dane dotyczą, inaczej sobie zażyczyła, a przekazanie informacji w ten sposób jest możliwe technicznie i nie wiąże się z nadmiernym utrudnieniem dla Stowarzyszenia.

1. Osoba zainteresowana, jeżeli jest uprawniona (co podlega weryfikacji opisanej wyżej), może skorzystać z jednego, kilku lub wszystkich uprawnień opisanych wyżej (np. może zwrócić się wyłącznie o uzyskanie informacji na temat tego, czy LGD przetwarza dane osobowe tej osoby i tego, jakie są te dane, ale może również zwrócić się – w razie pozytywnej odpowiedzi na pierwsze pytanie, o przekazanie kopii danych przetwarzanych przez LGD).

## Prawo do sprostowania danych

1. **Osoba, której dane dotyczą, ma prawo żądania od LGD:**
   1. **niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe;**

W przypadku zgłoszenia się osoby z takim żądaniem, Stowarzyszenie realizuje to uprawnienie po:

* + 1. uprzedniej weryfikacji, czy podmiot zwracający się z żądaniem faktycznie jest podmiotem, którego dane dotycząc (patrz pkt 34 Polityki);
    2. sprawdzeniu, czy dane są faktycznie nieprawidłowe (np. nieaktualne, błędne).

**Jeżeli dane są rzeczywiście nieprawidłowe** lub nieaktualne LGD;

1. niezwłocznie je prostuje we wszystkich swoich dokumentach i systemach, o czym informuje osobę, która zwróciła się do niego z żądaniem sprostowania;
2. zawiadamia wszystkich odbiorców danych, że osoba, której dane dotyczą, żąda, sprostowania nieprawidłowych lub nieaktualnych danych (np. jeżeli projekt współpracy, w którym uczestniczy LGD polega na zbieraniu danych od uczestników wyjazdu integracyjnego, a dane te są następnie przekazywane innej lokalnej grupie działania, to wniosek o sprostowanie nieprawidłowego nazwiska jednego z uczestników wyjazdu należy przekazać do tych lokalnych grup, którym przekazano nieprawidłowe dane tej osoby).;
   1. **żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia**

W przypadku zgłoszenia się osoby z takim żądaniem Stowarzyszenie wykonuje to uprawnienie po:

* + 1. uprzedniej weryfikacji, czy podmiot zwracający się z żądaniem faktycznie jest podmiotem, którego dane dotycząc (patrz pkt 34 Polityki);
    2. ustaleniu, czy uzupełnienie danych osobowych **jest zgodne z celami, dla których dane zostały zebrane** (LGD nie musi uzupełniać danych o takie informacje, które są jej niepotrzebne w świetle celów, dla których przetwarza dane osobowe).

**Jeżeli dane rzeczywiście wymagają uzupełnienia lub sprostowania**, Stowarzyszenie:

1. niezwłocznie je uzupełnia, o czym informuje osobę, która zwróciła się do niego z żądaniem uzupełnienia;
2. zawiadamia wszystkich odbiorców danych, że osoba, której dane dotyczą, żąda, uzupełnienia jej danych (np. jeżeli projekt współpracy, w którym uczestniczy LGD polega na zbieraniu danych od uczestników wyjazdu integracyjnego, a dane te są następnie przekazywane innej lokalnej grupie działania, to wniosek o uzupełnienie nieprawidłowego nazwiska jednego z uczestników wyjazdu /np. w przypadku kobiet informacji o tym, że nazwisko nie jest jednoczłonowe, a dwuczłonowe/ należy przekazać do tych lokalnych grup, którym wcześniej przekazano niekompletne dane tej osoby).

## Prawo do bycia zapomnianym

1. **Osoba, której dane dotyczą, ma prawo żądania od LGD niezwłocznego usunięcia dotyczących jej danych osobowych.**

Po otrzymaniu takiego żądania Stowarzyszenie:

1. ustala, czy osoba, która zwróciła się o realizację prawa do bycia zapomnianym jest osobą, której dane mają być usunięte (**weryfikacja tożsamości** osoby wnioskującej o usunięcie danych);
2. ustala, **czy zachodzą przesłanki** skorzystania z tego prawa przez osobę zainteresowaną oraz ustala, czy nie istnieją okoliczności mogące stanowić podstawę do odmowy wykonania przez Stowarzyszenie tego prawa:

Stowarzyszenie ma **obowiązek usunąć dane osobowe**, jeżeli zachodzi choćby jedna z następujących przesłanek:

* + 1. dane osobowe **nie są już niezbędne** do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    2. osoba, której dane dotyczą, **cofnęła zgodę,** na której opiera się przetwarzanie;
    3. osoba, której dane dotyczą, **wnosi sprzeciw**, o którym mowa w pkt 49 lit. a i b Polityki, wobec przetwarzania jej danych osobowych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania tych danych przez LGD,
    4. osoba, które dane dotyczą **wniosła sprzeciw**, o którym mowa w pkt 49 lit. c Polityki,   
       a przetwarzane dane wykorzystywane były do **marketingu bezpośredniego** (aktualnie nie dotyczy LGD);
    5. dane osobowe **były przetwarzane niezgodnie z prawem**;
    6. dane osobowe **muszą zostać usunięte w celu wywiązania się z obowiązku prawnego** przewidzianego w prawie (np. minął już okres obowiązkowego przechowywania określonych kategorii danych);
    7. dane osobowe zostały **zebrane w związku z oferowaniem usług społeczeństwa informacyjnego** (tj. każdej usługi świadczonej za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług, np. płatne webinarium – obecnie nie dotyczy to LGD).

Stowarzyszenie **nie jest zobowiązane do usunięcia danych**, jeżeli dane są w dalszym ciągu niezbędne:

1. do korzystania z prawa do wolności wypowiedzi i informacji;
2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na podstawie ustawy lub prawa unijnego (np. nie minął jeszcze okres obowiązkowego przechowywania danych wynikający z przepisów prawa);
3. do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej LGD (obecnie ta przesłanka nie występuje);
4. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
5. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania
6. do ustalenia, dochodzenia lub obrony roszczeń.

W przypadku stwierdzenia, że LGD powinno wykonać powyższe uprawnienie osoby trzeciej, Stowarzyszenie ustala:

1. **gdzie znajdują się wszystkie dane takiej osoby** (papierowe oraz elektroniczne), włączając w to kopie zapasowe danych – wykorzystując w pierwszej kolejności informacje zawarte w Rejestrze czynności przetwarzania,
2. **komu zostały przekazane te dane** (katalog odbiorców) – wykorzystując w pierwszej kolejności informacje zawarte w Rejestrze czynności przetwarzania.

Po ustaleniu tych okoliczności Stowarzyszenie:

1. **usuwa wszystkie rekordy** odnoszące się do danej osoby, a jeżeli jest to niemożliwe stosuje ich anonimizację (tj. zmienia ich treść w ten sposób, by ich odczytanie i dalsze przetwarzanie nie było już możliwe, by na podstawie treści informacji zanonimizowanej nie dało się już ustalić, kogo dane dotyczyły) – z usunięcia sporządza się protokół;
2. **zawiadamia wszystkich odbiorców** danych, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Stowarzyszenie – w celu wywiązania się z obowiązku rozliczalności przetwarzania danych – prowadzi Rejestr osób, których dane zostały wykreślone na ich żądanie oraz zachowuje kopię wniosków o usunięcie danych (tzw. **rejestr zapomnianych**).

LGD musi rejestrować wnioski o usunięcie danych osobowych wraz z informacją gdzie (w jakich bazach) znajdowały się rekordy na temat danej osoby (które usunięto) wyłącznie po to, by w razie potrzeby przywrócenia systemu, bazy itp. z backupu (kopii zapasowej) być w stanie z uruchamianej kopii zapasowej wykasować dane tych osób – by dalsza praca odbywała się z pominięciem tych rekordów na temat osób zapomnianych.

1. W celu skutecznej realizacji prawa do bycia zapomnianym LGD musi dysponować narzędziami pozwalającymi mu być w stanie ustalić jakie dokładnie dane osobowe posiada i w ilu kopiach. Wykonanie żądania wymaga bowiem zweryfikowania w jakich programach przetwarzane były dane osobowe, czy dane te zostały w nich zapisane, gdzie są przechowywane kopie. Realizacja prawa do bycia zapomnianym wymaga także ingerencji w treść kopii zapasowych. **Dlatego tak istotne jest prowadzenie Rejestru czynności przetwarzania i jego regularna aktualizacja**.

## Prawo do ograniczenia przetwarzania

1. **Osoba, której dane dotyczą, ma prawo żądania od LGD ograniczenia przetwarzania jej danych.**

Ograniczenie przetwarzania danych polega na tym, że **dane osobowe są wyłącznie przechowywane,** bez możliwości dokonywania na nich innych operacji przetwarzania   
(np. kopiowania, wglądu, usuwania, modyfikowania).

Ograniczenie przetwarzania danych może w szczególności polegać na:

* 1. czasowym przeniesieniu wybranych danych osobowych do innego systemu przetwarzania,
  2. uniemożliwieniu użytkownikom dostępu do wybranych danych,
  3. czasowym usunięciu opublikowanych danych ze strony internetowej.

W przypadku danych osobowych, które są zapisane na komputerze, na serwerach itp. (w wersji elektronicznej, a nie papierowej) przetwarzanie należy ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.

1. **Po otrzymaniu żądania dotyczącego ograniczenia przetwarzania LGD:**
   1. **ustala tożsamość osoby**, która zwróciła się do Stowarzyszenia z takim żądaniem;
   2. weryfikuje, **czy zachodzą przesłanki** pozwalające na zrealizowanie tego prawa.

**Ograniczenie przetwarzania danych osobowych danej osoby jest możliwe**, jeżeli:

1. osoba, której dane dotyczą, **zakwestionowała prawidłowość danych** osobowych jej dotyczących (czyli skorzystała z **prawa, o którym mowa w pkt 41 Polityki**) – wówczas należy ograniczyć przetwarzanie danych osobowych tej osoby – przez okres pozwalający Stowarzyszeniu sprawdzić prawidłowość tych danych. W tym czasie nie można danych osobowych tej osoby wykorzystywać w inny sposób (np. nie można na adres e-mail takiej osoby wysyłać wiadomości);
2. przetwarzanie danych osobowych konkretnej osoby przez LGD jest **niezgodne z prawem, ale osoba, której dane dotyczą, sprzeciwia się usunięciu swoich danych osobowych**, żądając jedynie ograniczenia ich wykorzystywania (w związku z tym LGD musi zablokować możliwość wykorzystywania danych osobowych, możliwość wglądu do nich, modyfikacji, wyświetlania itp., ale nie może ich usunąć);
3. **LGD nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą**, do ustalenia, dochodzenia lub obrony roszczeń (przeciwko LGD lub przeciwko innemu podmiotowi);
4. **osoba, której dane dotyczą, wniosła sprzeciw**, o którym mowa w pkt 49 Polityki – w takiej sytuacji Stowarzyszenie musi ograniczyć przetwarzanie danych tej osoby wyłącznie do ich przechowywania, do czasu stwierdzenia, czy Stowarzyszenie posiada prawnie uzasadnione podstawy, nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą (patrz pkt 49 Polityki) pozwalające na odmówienie usunięcia danych .
5. Nawet, jeżeli Stowarzyszenie ograniczy przetwarzanie danych osobowych, stosownie do żądania osoby zainteresowanej, to j**ednak może w pewnych sytuacjach przetwarzać te dane w szerszym zakresie, niż tylko samo ich przechowywanie**. Sytuacja taka wystąpi, jeżeli zostanie spełniona **choćby jedna z następujących przesłanek**:
   1. osoba zainteresowana wyraziła **zgodę** na takie przetwarzanie;
   2. przetwarzanie jest **niezbędne do ustalenia, dochodzenia lub obrony roszczeń** przez LGD,
   3. przetwarzanie jest niezbędne w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

## Prawo do przenoszenia danych

1. Osoba, której dane dotyczą, ma prawo:
   1. **otrzymać dane** osobowe jej dotyczące, które dostarczyła do LGD (np. wypełniając drogą elektroniczną formularz rejestracyjny);
   2. **przesłać dane** osobowe jej dotyczące, które dostarczyłado LGD**, innemu administratorowi** bez przeszkód ze strony Stowarzyszenia;
   3. **zażądać od LGD**, by **Stowarzyszenie przesłało dane tej osoby bezpośrednio innemu administratorowi,** o ile jest to technicznie możliwe.

Dane powinny być przekazywane osobie, której dane dotyczą lub innemu administratorowi w formie elektronicznej, w formacie powszechnie używanym (np.: w pliku \*.doc, \*.xml, \*.xlsx, \*.pdf,\*.rtf, \*.txt, itp.).

**LGD jest zobowiązana do zrealizowania czynności, których żąda dana osoba**, po zweryfikowaniu tożsamości osoby wnioskującej (pkt 34 Polityki), jeżeli spełnione są łącznie następujące przesłanki:

* + - 1. Stowarzyszenie przetwarza dane osobowe tego podmiotu:

1. **na podstawie jego zgody lub**
2. **w celu zawarcia lub realizacji umowy**, której stronami są Stowarzyszenie i ten podmiot ;
   * + 1. przetwarzanie danych **odbywa się w sposób zautomatyzowany**, tzn. są to dane możliwe do odczytania i edycji na komputerze, zapisane na w pamięci elektronicznej.

**LGD nie jest zobowiązana** do realizacji tego uprawnienia osoby zainteresowanej, jeżeli:

* pozyskało dane osoby w **inny sposób niż w wyniku uzyskania zgody osoby zainteresowanej lub zawarcia umowy**, np. gdy dane uzyskała od osoby trzeciej, z publicznie dostępnych rejestrów, itp.;
* przetwarza dane osobowe **w formie papierowej** (nie posiada ich elektronicznej kopii) – takie dane może przekazać w formie papierowej, ale wyłącznie osobie, której dane dotyczą (a nie podmiotowi trzeciemu) – wówczas odbywa się to jednak zgodnie z pkt 39 ppkt 4 Polityki.

## Prawo do sprzeciwu

1. Osoba, której dane dotyczą, ma prawo wnieść sprzeciw wobec przetwarzania jej danych.

**W przypadku wniesienia skutecznego sprzeciwu** Stowarzyszenie nie może już przetwarzać danych osobowych tego, kto wniósł sprzeciw (**dane powinny zostać usunięte** – zastosowanie zatem znajdują postanowienia pkt 42 Polityki).

W przypadku wniesienia przez daną osobę sprzeciwu wobec przetwarzania przez Stowarzyszenie jej danych osobowych, Stowarzyszenie:

* 1. weryfikuje tożsamość wnoszącego sprzeciw;
  2. ustala, czy zachodzą przesłanki do uwzględnienia sprzeciwu.

1. Prawo do wniesienia sprzeciwu przysługuje, jeżeli:
2. podstawą przetwarzania danych osobowych tej jest art. 6 ust. 1 lit e RODO („*przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi”*) – obecnie nie dotyczy to podstaw przetwarzania danych przez LGD;
3. podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit f RODO („*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*”) – np. wysyłanie newslettera informacyjnego (bez ofert handlowych) do klientów LGD mieści się w zakresie terminu „prawnie uzasadniony interes”, ale osoba, która otrzymuje takie newsletter może wnieść sprzeciw – wówczas jej dane trzeba będzie wykasować z bazy mailingowej newslettera);
4. dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego (np. wysyłanie do potencjalnych klientów LGD ofert szkoleniowych, itp. – obecnie nie dotyczy LGD).

**Stowarzyszenie może nie uwzględnić sprzeciwu** opartego na przesłankach wskazanych   
w lit. a i b powyżej, jeżeli:

1. wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub
2. dane osobowe, których dotyczy sprzeciw są jej potrzebne do ustalenia, dochodzenia lub obrony roszczeń.
3. Wykonanie przez Stowarzyszenie prawa do sprzeciwu polega na realizacji tych samych czynności, co w przypadku prawa do bycia zapomnianym (a dokładnej – jedną z przesłanek prawa do bycia zapomnianym jest wniesienie sprzeciwu). Dlatego, w przypadku wniesienia sprzeciwu, należy odpowiednio stosować pkt 42-44 Polityki.

## Zautomatyzowane podejmowanie decyzji i profilowanie

1. **Profilowanie.**

**Profilowanie to automatyczne wnioskowanie o określonych cechach danej osoby, na podstawie posiadanych przez administratora danych osobowych dotyczących tej osoby oraz danych innych osób** (np. na podstawie informacji o miejscu zamieszkania i pracodawcy wnioskuje się o określonych zainteresowaniach danej osoby i w oparciu o takie wnioski odpowiednio adresuje się reklamy wyświetlane w danym serwisie). Profilowanie opiera się na statystyce (porównanie aktywności i cech danej osoby i zestawieniu z aktywnością i cechami innych osób – wywnioskowanie na ten podstawie, że w innych sytuacjach dana osoba zachowywać się będzie podobnie, co osoby o tym samym profilu).

Profilowanie jest dopuszczalne, ale **należy o tym informować osoby profilowane** (np., jeżeli witryna internetowa korzysta z mechanizmów profilowania, tzn. na podstawie informacji o aktywności użytkownika w sieci, sugeruje mu określone decyzje, podsuwa określone reklamy, itp. – należy informacje na ten temat zamieścić w Polityce prywatności).

1. **Zautomatyzowane podejmowanie decyzji**

Osoba, której dane dotyczą, ma **prawo do tego, by nie podlegać decyzji LGD, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych** (dot. to sytuacji, w których człowiek nie ma wpływu na treść konkretnej decyzji, lecz jest ona wynikiem określonego algorytmu, decyzję podejmuje „automat”) i wywołuje wobec tej osoby określone skutki prawne lub w podobny sposób istotnie na nią wpływa (np. na tej podstawie ustalana jest wysokość opłaty, w wyniku takiej „komputerowej” decyzji zapada decyzja, by z danym podmiotem nie zawrzeć umowy). Obecnie takie mechanizmy nie zostały wdrożone w LGD.

Zautomatyzowane podejmowanie decyzji przez Stowarzyszenie jest dopuszczalne jedynie w sytuacjach, w których został spełniony co najmniej jeden z poniższych warunków:

Decyzja oparta o zautomatyzowane procesy:

* 1. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
  2. jest dozwolona prawem Unii lub prawem państwa członkowskiego,
  3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą (tj. na wyraźnej zgodzie na zautomatyzowane podjęcie decyzji lub profilowanie).

1. W momencie przyjęcia Polityki Stowarzyszenie nie przetwarza danych osobowych w ten sposób –tzn. nie podejmuje zautomatyzowanych decyzji ani nie profiluje użytkowników.

# ROZDZIAŁ V STOSOWANE PRZEZ STOWARZYSZENIE ŚRODKI ZABEZPIECZENIA DANYCH

1. LGD wdraża opisane w niniejszym rozdziale środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami prawa oraz aby móc to wykazać na wypadek kontroli, zdarzenia stanowiącego naruszenie bezpieczeństwa danych osobowych lub ewentualnych zarzutów podniesionych przeciwko Stowarzyszeniu przez osoby trzecie.
2. Środki techniczne i organizacyjne opisane niżej uwzględniają wynik dokonanej przez LGD analizy ryzyka, aktualnej na dzień przyjęcia Polityki. Środki te uwzględniają charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Przyjęte środki i zabezpieczenia będą w razie potrzeby uaktualniane, tak, by pozostawały adekwatne do ryzyka ochrony bezpieczeństwa danych osobowych.
3. Przyjęte przez LGD środki dzielą się na: organizacyjne, fizyczne i techniczne.

## Środki organizacyjne:

1. Do najważniejszych środków organizacyjnych, które zostały przyjęte w celu zapewnienia należytego poziomu ochrony danych osobowych, należą następujące zasady:
2. przetwarzanie danych osobowych w Stowarzyszeniu odbywa się zgodnie z postanowieniami Polityki. Osoby przetwarzające dane osobowe w Stowarzyszeniu nie mają zatem swobody w decydowaniu o tym co i jak robić postępując z danymi osobowymi, ale są zobligowane do postępowania zgodnie z niniejszym dokumentem;
3. naruszenie postanowień Polityki lub przepisów prawa regulujących zasady przetwarzania danych osobowych wiążę się z konsekwencjami dyscyplinarnymi dla naruszyciela, o czym adresaci Polityki są informowani przez Zarząd LGD;
4. **przetwarzanie danych osobowych w Stowarzyszeniu odbywa się na podstawie upoważnień**, które co do zasady przyjmują formę pisemnego (tj. papierowego lub przesłanego drogą elektroniczną) dokumentu – Stowarzyszenie prowadzi rejestr takich upoważnień, by wiedzieć kto w jakim okresie był upoważniony do przetwarzania określonych danych (ułatwia to ustalenie kto, w razie naruszenie ochrony danych osobowych mógł być odpowiedzialny za takie zdarzenie);
5. Stowarzyszenie, w celu zapewnienia zasady minimalizacji danych, ogranicza przetwarzanie poszczególnych kategorii danych do określonych grup osób. Jedynie członkowie Zarządu LGD mają dostęp do wszystkich danych osobowych w pełnym zakresie czynności przetwarzania;
6. **pracownicy i nowi członkowie LGD, pierwszego dnia wykonywania swoich obowiązków, otrzymują Politykę lub jej fragmenty, do zapoznania się**, by byli świadomi swoich obowiązków, odpowiedzialności oraz zasad przetwarzania danych osobowych w Stowarzyszeniu;
7. LGD **określiła podział odpowiedzialności poszczególnych osób za kwestie związane z przetwarzaniem danych osobowych**:

* za wszystkie sprawy związane z przetwarzaniem danych odpowiedzialny jest Zarząd LGD;
* Zarząd wyznacza pracownika ds. bezpieczeństwa informacji, w celu koordynowania bieżących kwestii związanych z przetwarzaniem danych osobowych;
* za przetwarzanie danych osobowych w Komisji Rewizyjnej i Radzie, w tym za czuwanie nad tym, by członkowie tego organu przetwarzali dane zgodnie z Polityką, odpowiada Przewodniczący danego organu;
* LGD nie powołało inspektora ochrony danych osobowych, o którym mowa   
  w art. 37 i nast. RODO na skutek świadomej decyzji poprzedzonej analizą charakteru i ilości danych osobowych, które przetwarza Stowarzyszenie, oraz oceną prawdopodobieństwa i ewentualnych skutków wystąpienia zdarzenia naruszenia bezpieczeństwa danych osobowych.

1. LGD **wybiera podmioty przetwarzające dane osobowe, którymi administruje, po przeprowadzeniu ich weryfikacji**:

* wypełnienie kwestionariusza przez podmiot przetwarzający,
* analiza regulaminów świadczenia usług, umów itp. stosowanych przez ten podmiot,
* weryfikacji, czy przetwarzanie powierzonych danych osobowych przez podmiot przetwarzający będzie odbywało się na obszarze państw Unii Europejskiej, Europejskiego Obszaru Gospodarczego lub w tzw. państwach bezpiecznych lub czy podmiot przetwarzający zapewnia należyty poziom ochrony danych (w przypadku podmiotów z USA: przystąpił do *Privacy shield*);
* preferowane są podmioty posiadające siedzibę na terenie Unii Europejskiej;

1. **powierzenie przetwarzania danych osobowych następuje wyłącznie na podstawie umowy powierzenia**, umowy zawierającej klauzulę powierzenia **lub innego instrumentu** prawnego zawierającego zobowiązania podmiotu przetwarzającego, analogiczne do tych, które wskazano we wzorze umowy powierzenia;
2. **weryfikacja podmiotów (firm) będących procesorami danych osobowych Stowarzyszenia w chwili wejścia w życie Polityki** – pod kątem dostosowania się tych podmiotów do wymagań rozporządzenia RODO;
3. przyjęcie w Polityce regulacji dotyczących reagowania na naruszenia ochrony danych osobowych, zasad reagowania na wnioski osób zainteresowanych dotyczące ich danych osobowych oraz zasad usuwania danych osobowych (polityka retencyjna);
4. **okresowe audyty** **Polityki,** w tym weryfikacja przyjętych środków ochrony danych osobowych, w kontekście ich aktualności i adekwatności do poziomu ryzyka w danym momencie;
5. **wdrożenie zasady *privacy by design*:** przed rozpoczęciem realizacji projektu Stowarzyszenie analizuje kwestie dotyczące przetwarzania danych osobowych w tym projekcie oraz wprowadza środki zapewniające zgodność przetwarzania z prawem i Polityką, w tym adekwatne środki ochrony;
6. **wdrożenie zasady *privacy by default* oraz minimalizacji danych –** LGD nie stosuje formularzy z automatycznie wypełnionymi polami (checkboxami) potwierdzającymi udzielenie zgody na przetwarzanie danych osobowych albo zapoznanie się z informacjami dot. przetwarzania danych, ogranicza liczbę gromadzonych i upublicznianych danych do minimum wynikającego z celu przetwarzania i z przepisów;
7. **okresowe szkolenia dla osób upoważnionych do przetwarzania danych osobowych, członków organów, stałych współpracowników LGD** – ze znajomości przepisów dotyczących przetwarzania danych osobowych oraz z postanowień Polityki;
8. **obowiązywać będzie zasada czystego biurka:** po godzinach pracy pracownik zostawia po sobie czyste biurko (dokumenty wracają do segregatorów, segregatory umieszczane są w szafie), w trakcie pracy na biurku znajdują się wyłącznie dokumenty, z których aktualnie korzysta pracownik;
9. obsługa interesantów Stowarzyszenia odbywa się w ten sposób, by w jednym pomieszczeniu biura LGD nie była w tym samym momencie obsługiwana więcej niż jedna osoba (w celu uniknięcia ryzyka podejrzenia na dokumentach lub usłyszenia informacji stanowiących dane osobowe lub inne dane wrażliwe);
10. pracownicy **ograniczają liczbę kopii dokumentów** (także w formie elektronicznych, jako kopie plików) do minimum niezbędnego do prawidłowej pracy, mając na uwadze konieczność sporządzania kopii zapasowych dokumentów;
11. pracownicy **nie wynoszą dokumentów** (w formie papierowej, elektronicznej) poza biuro Stowarzyszenia, chyba że jest to konieczne do wykonania konkretnych obowiązków zawodowych, wprowadza się zakaz zabierania przez pracowników dokumentów Stowarzyszenia do domu.

## Środki fizycznej ochrony

1. Do najważniejszych środków fizycznej ochrony, które zostały przyjęte w celu zapewnienia należytego poziomu ochrony danych osobowych, należą następujące zasady:
   1. przetwarzanie danych osobowych odbywa się co do zasady w biurze Stowarzyszenia, dlatego pomieszczenia biura są zabezpieczone przed wejściem nieuprawnionych osób:
      * biuro LGD jest zabezpieczone poprzez drzwi główne zamykane na zamek oraz drzwi wejściowe bezpośrednio do pomieszczeń biura zamykane na klucz;
      * biuro i poszczególne pomieszczenia biura, w czasie, gdy nie znajdują się w nich pracownicy Stowarzyszenia, są zamykane na klucz, istnieją zasady postępowania z kluczami po zamknięciu biura (ustala je osoba kierująca biurem i informuje o nich pracowników biura); w przypadku opuszczenia pomieszczenia, w którym przetwarza się dane osobowe, przez ostatnią osobę, pomieszczenie zamykane jest na klucz, także w godzinach pracy, obowiązuje absolutny zakaz wykonywania przez adresatów Polityki– bez zgody Zarządu – kopii kluczy;
      * w pomieszczeniach, w których przechowywane są dane osobowe (w formie papierowej lub elektronicznej), osoby trzecie mogą przebywać wyłącznie w obecności osoby upoważnionej przez Stowarzyszenie do przetwarzania danych;
      * w biurze znajduje się gaśnica (ew. w bezpośredniej bliskości, np. na korytarzu, znajduje się taka gaśnica lub dostęp do hydrantu);
      * w biurze znajduje się niszczarka do dokumentów;
      * urządzenia elektroniczne w biurze, wykorzystywane do przetwarzania danych osobowych (drukarki, komputery, fax, itp.), podłączone są do sieci elektrycznej w sposób zabezpieczający je przed przepięciami, zastosowanie zasilaczy zapasowych UPS w celu ochrony stanowisk komputerowych oraz serwerów przed skutkami zaniku zasilania;
   2. dokumenty (papierowe) Stowarzyszenia, na których znajdują się dane osobowe znajdują się w segregatorach. Segregatory, jeżeli nie są aktualnie używane, znajdują się w szafach zamykanych na klucz;
   3. **niszczenie papierowych dokumentów odbywa się z wykorzystaniem niszczarki** lub też – w sytuacji jej awarii – **poprzez podarcie dokumentu, tak by odczytanie danych na zniszczonym dokumencie było praktycznie niemożliwe;**
   4. **zakaz posługiwania się dyskami przenośnymi** (np. pendrive), w celu umieszczania na nich kopii dokumentów zawierających dane osobowe, **chyba że** dysk należy do Stowarzyszenia, zgodę na korzystanie z niego wydał Zarząd, a dostęp do dysku i do danych został zabezpieczony hasłem. Zaleca się zablokowanie dostępu do portów USB w komputerach, ew. dostęp do nich jedynie po wpisaniu hasła przez użytkownika.
   5. przetwarzanie danych osobowych poza biurem (tj. w wersji papierowej, lub przy użyciu komputerów znajdujących się poza biurem) jest możliwe jedynie w sytuacjach wyjątkowych. W przypadku konieczności przetwarzania danych osobowych poza biurem Stowarzyszenie podejmuje następujące środki bezpieczeństwa:
      * dokumenty (papierowe) zawierające dane osobowe lub urządzenia zawierające dane osobowe (komputery, dyski przenośne) transportowane są do innego miejsca przez pracowników Stowarzyszenia lub członków organów Stowarzyszenia posiadających upoważnienie do przetwarzania danych osobowych w odpowiednim zakresie;
      * dokumenty (papierowe), przed ich wyniesieniem poza biuro, są zabezpieczane (pakowane) w sposób, który uniemożliwia ich przypadkowe otwarcie, które mogłoby grozić utratą, zniszczeniem lub uszkodzeniem
      * przetwarzanie danych osobowych poza biurem dokonywane jest w sposób, który uniemożliwia zapoznanie się z danymi osobami przez osoby nieposiadające stosownych upoważnień do przetwarzania danych osobowych;
      * niedopuszczalne jest pozostawienie pomieszczeń lub pojazdów, w których znajdują się lub są transportowane dokumenty zawierające dane osobowe, bez pieczy osoby posiadającej stosowne upoważnienie do przetwarzania danych osobowych;
      * w trakcie przetwarzania danych osobowych poza biurem Stowarzyszenie podejmuje inne stosowne środki uniemożliwiające osobom postronnym zapoznanie się z danymi osobowymi;

## Środki ochrony technicznej

1. LGD w następujący sposób zabezpiecza dane osobowe, które przetwarza za pomocą swoich urządzeń elektronicznych:
2. pracownicy i osoby stale współpracujące ze Stowarzyszeniem przetwarzają dane osobowe w sieci Stowarzyszenia, za pomocą urządzeń należących do Stowarzyszenia;
3. w przypadku przetwarzania danych osobowych na urządzeniach prywatnych osób upoważnionych jest to dopuszczalne pod warunkiem, że dostęp do danych został ustanowiony przez Zarząd, po zweryfikowaniu lub zadeklarowanie, że osoba upoważniona:

* korzysta z urządzenia posiadającego odpowiednią ochronę antywirusową, spyware, maleware, która jest regularnie aktualizowana,
* zabezpiecza dostęp do urządzenia hasłem.

1. **dostęp do sieci LGD, serwisów, intranetu, wspólnego dysku, dysku w chmurze itp. zabezpieczany jest hasłem**;
2. przesyłanie danych w sieci Stowarzyszenia jest **szyfrowane**;
3. w celu korzystania z komputerów podpiętych do systemu Stowarzyszenia lub z programów wykorzystywanych przez LGD do wymiany dokumentów, informacji itp., **wymagane jest zalogowanie** się – loginy przyznawane są jedynie osobom posiadającym upoważnienie do przetwarzania danych osobowych o odpowiednim zakresie („**użytkownikom**”).

* każdy użytkownik posiada **unikalny login** (brak loginów współdzielonych między kilku użytkowników;
* użytkownik otrzymuje swój login i pierwsze hasło od Zarządu LGD „do rąk własnych”, na wydrukowanej kartce, w zamkniętej kopercie;
* przy pierwszym logowaniu **system wymusza zmianę hasła**;
* hasła służące do logowania się do systemu muszą spełniać następujące warunki:
  + hasło składa się z co najmniej 8 znaków, w tym dużej i małej litery oraz cyfry lub znaku technicznego;
  + hasło nie może być jednakowe z identyfikatorem użytkownika;
  + hasło musi być unikalne, tj. takie, które nie było w ciągu ostatniego roku stosowane przez użytkownika;
  + hasło nie może zawierać imienia, nazwiska lub daty urodzenia użytkownika;
  + **wymuszanie okresowej zmiany hasła** użytkownika – Zarząd podejmuje decyzję o tym, jak często (nie rzadziej niż raz na miesiąc);
  + w przypadku, gdy użytkownik zapomniał hasła, osoba odpowiedzialna za prowadzenie serwisów internetowych, sieci LGD, ustala hasło tymczasowe, z wymuszeniem jego zmiany podczas kolejnego logowania użytkownika;
* konta nieaktywnych użytkowników (np. byłych pracowników, członków Zarządu LGD, członków Stowarzyszenia) utworzone w systemie Stowarzyszenia lub w serwisach służących do wymiany informacji, dokumentów itp. w ramach LGD, są usuwane, po uprzednim zabezpieczeniu danych z tego konta do dalszego wykorzystania przez Stowarzyszenie;
* niedopuszczalne jest pozostawianie przez użytkowników swoich haseł w widocznym miejscu (np. kartka przyklejona do monitora);

1. w przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego;
2. na komputerach użytkowników włączone są **wygaszacze ekranu** oraz **automatyczne wylogowanie się** (w przypadku kilkuminutowej nieaktywności użytkownika na komputerze system wymusza ponowne zalogowanie się);
3. **urządzenia należące do sieci LGD są zabezpieczone przed nieuprawnionym dostępem osób trzecich, wirusami i trojanami:** posiadają ochronę antywirusową, spyware, maleware, ochrona jest regularnie aktualizowana (np. poprzez akceptację automatycznego instalowania aktualizacji);
4. **w celu zapewnienia stałej dostępności danych LGD** **regularnie wykonuje kopie zapasowe** danych osobowych:

* raz na miesiąc sporządzana jest kopia całkowita danych – ręcznie

(*albo – rekomendowane*);

* raz na tydzień sporządzany jest automatyczny backup systemu;
* kopie zapasowe przechowywane są w innym miejscu (kopie fizyczne) na innym serwerze (kopie sporządzane automatycznie) niż dane oryginalne – by awaria serwera nie wiązała się z utratą wszystkich danych;

1. **LGD regularnie usuwa niepotrzebne dane z systemu** (po okresie ich wykorzystywania oraz ewentualnym przedawnieniu się roszczeń związanych z danymi, wypełnieniem obowiązków wynikających z przepisów) – **raz do roku** przeprowadza się weryfikację danych znajdujących się w systemie i usuwa się dane niepotrzebne;

# ROZDZIAŁ VI ZDARZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH i REAKCJA NA TAKIE ZDARZENIA

## Naruszenia ochrony danych – przykłady

1. W wyniku dokonanej analizy LGD ustaliło listę sytuacji, które potencjalnie mogą wystąpić w  związku z prowadzoną działalnością, i które mogą się wiązać z zagrożeniem dla poufności, integralności i dostępności danych osobowych. Stowarzyszenie oszacowało również prawdopodobieństwo wystąpienia tego rodzaju zdarzeń i ewentualne skutki ich wystąpienia. Na podstawie tak dokonanej analizy, Stowarzyszenie opracowało zasady mające na celu zwiększenie bezpieczeństwa przetwarzania danych osobowych przez Stowarzyszenie (zasady te opisano w poprzednim rozdziale Polityki).
2. Przypadki zakwalifikowane jako naruszenie lub groźba naruszenia bezpieczeństwa danych osobowych, to w szczególności:
   * 1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu informatycznego lub dokumentację Stowarzyszenia, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej itp. (1, 4);
     2. zgubienie lub utrata dokumentów Stowarzyszenia, zgubienie nośnika danych, na którym zapisane były dokumenty Stowarzyszenia (4, 3);
     3. niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych – w stopniu, który może grozić zakłóceniem funkcjonowania urządzeń przetwarzających dane osobowe (1 ,4);
     4. upublicznienie loginu lub haseł dostępowych do systemu lub programów, które są wykorzystywane przez Stowarzyszenie do przetwarzania danych (2, 4);
     5. awaria sprzętu lub oprogramowania, na skutek której nastąpiła utrata dostępu do danych, ich modyfikacja upublicznienie (2, 4);
     6. upublicznienie danych osobowych na skutek błędu ludzkiego (np. zamieszczenie na stronie internetowe, w publiczne dostępnym miejscu, danych osobowych wnioskodawców, kopii wniosków, itp.), wysłanie maila do grupy adresatów bez zastosowania funkcji „UDW” (do ukrytej wiadomości) (2, 3);
     7. przetwarzanie danych osobowych bez podstawy prawnej (np. bez zgody osoby zainteresowanej) (3, 3);
     8. przekazanie osobie trzeciej danych osobowych innego podmiotu (np. w mylnym przekonaniu, że przekazuje się je osobie, której dane dotyczą, bez sprawdzenia tożsamości wnioskującego) (2, 3);
     9. nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie informatycznym wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp. (1, 4);
     10. włamanie do biura Stowarzyszenia; kradzież dokumentów należących do Stowarzyszenia (np. włamanie do samochodu, w którym były przewożone wnioski do Urzędu Marszałkowskiego, np. kradzież teczki z dokumentacją Stowarzyszenia) (1, 3);
     11. podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych (2, 2) ;
     12. awaria sprzętu lub oprogramowania wskazująca na umyślne działanie osób trzecich (1, 4);
     13. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń (4, 3);
     14. utrata dostępu do danych Stowarzyszenia na skutek odmowy świadczenia usług przez podmiot przetwarzający (1, 4);
     15. naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub na ksero przez czas, który umożliwia ich zabranie przez osoby nieupoważnione, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp., przesyłanie służbowych materiałów na prywatny adres e-mail) (3, 3);
     16. stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach (2, 4);
     17. nieusunięcie kont nieaktywnych użytkowników, którzy powinni byli utracić dostęp do systemu (2, 4);
     18. utrata danych osobowych w wyniku wykonywania niepełnych kopii zapasowych danych (3, 3);
     19. utrata danych spowodowana niemożnością odtworzenia danych z kopii zapasowej (3, 4).
3. Zdarzenia wymienione w pkt 61 Polityki stanowią również naruszenie ochrony danych osobowych w sytuacji, gdy Stowarzyszenie przetwarza dane dla innego podmiotu (jest podmiotem przetwarzającym). W takiej sytuacji Stowarzyszenie niezwłocznie informuje o tym zdarzeniu administratora danych, których dotyczyło naruszenie.
4. Jak wynika z przeprowadzonej prostej analizy ryzyka, przetwarzanie danych przez Stowarzyszenie przy zachowaniu zaproponowanych środków technicznych, organizacyjnych i fizycznych, nie wiąże się z dużym zagrożeniem naruszenia bezpieczeństwa, które mogłoby powodować duże negatywne konsekwencje zarówno dla Stowarzyszenia, jak i dla podmiotów, których dane Stowarzyszenie przetwarza. Większość przypadków naruszenia, jakie w ocenie Stowarzyszenia mogłyby nastąpić cechuje umiarkowane ryzyko wystąpienia, jak również niezbyt dotkliwe skutki. Nie występuje korelacja wysokiego prawdopodobieństwa i dotkliwych skutków (najwyższy wynik pomnożenia ryzyka przez skutek wynosi 12 pkt na 25 możliwych. Wynik analizy ryzyka obrazuje poniższa tabela.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 6  **F, H,** | 11 | 16 | 21 |
| 2 | 7 | 12  **B, M, S,** | 17 | 22 |
| 3  **J** | 8  **D, E, P, Q** | 13 | 18 | 23 |
| 4  **A, C, I, , K, L, N** | 9  **G, O, R** | 14 | 19 | 24 |
| 5 | 20 | 15 | 20 | 24 |

**LEGENDA:**

**Zagrożenie minimalne Zagrożenie niewielkie**

**Zagrożenie dopuszczalne Zagrożenie znaczące**

**Bardzo duże zagrożenie Zagrożenie niedopuszczalne**

1. W celu ograniczenia możliwości wystąpienia zdarzeń wiążących się z zagrożeniem bezpieczeństwa danych osobowych, których prawdopodobieństwo wystąpienia jest największe, LGD wdrożyło mechanizmy ograniczające skutki takiego zdarzenia oraz obniżające potencjalne ryzyko ich wystąpienia (np. zmiana dotychczasowych praktyk sporządzania kopii zapasowych, podwójne szyfrowanie nośników danych – pendrive i plik, zwrócenie uwagi pracownikom na konieczność transportu dokumentów i urządzeń elektronicznych zawierających dane z największa uwagą, rezygnacja z „ogólnej” skrzynki mailowej, rezygnacja z kontaktowania się z członkami Rady za pomocą adresów e-mail nieprzypisanych wyłącznie do jednego użytkownika).

## Procedura reagowania na naruszenia ochrony danych osobowych

1. W przypadku wystąpienia zdarzeń określonych w pkt 60 Polityki albo innych wydarzeń, które mogą zostać sklasyfikowane jako naruszenie ochrony danych osobowych **każdy adresat Polityki zobowiązany jest do niezwłocznego zawiadomienia o tym fakcie Zarządu**.

Po otrzymaniu zawiadomienia Zarząd stwierdza, czy zgłoszone zdarzenie należy sklasyfikować jako naruszenie ochrony danych osobowych, a jeżeli tak, to ustala:

* 1. okoliczności, w których doszło do naruszenia bezpieczeństwa ochrony danych, w szczególności czy do naruszenia doszło w wyniku przypadkowego zdarzenia czy tez na skutek celowego działania określonych osób;
  2. rodzaj danych osobowych, których dotyczy naruszenie, osoby, których dane osobowe zostały naruszone, ilość danych osobowych, których dotyczyło naruszenie;
  3. na czym polegało naruszenie i jak je należy sklasyfikować (jako utratę poufności, dostępności lub integralności danych);
  4. skutki naruszenia: te, które już nastąpiły i te, które są potencjalnie możliwe;
  5. możliwe do podjęcia działania zmierzające do zmniejszenia niekorzystnych skutków naruszenia;

1. W przypadku potwierdzenia, że dane zdarzenie należy sklasyfikować jako naruszenie ochrony danych osobowych, Zarząd:
   1. podejmuje niezbędne i możliwe działania zmierzające do zmniejszenia niekorzystnych skutków naruszenia;
   2. jeżeli mimo podjęcia tych działań, nadal jest prawdopodobne, że naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – **zgłasza naruszenie ochrony danych osobowych do PUODO:**

* zgłoszenie powinno zostać dokonane **nie później niż 72 godziny od chwili stwierdzenia zdarzenia** sklasyfikowanego jako naruszenie ochrony danych osobowych;
* zgłoszenie powinno 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;
* możliwe konsekwencje naruszenia ochrony danych osobowych;
* środki zastosowane lub proponowane przez LGD w celu zaradzenia naruszeniu ochrony danych osobowych.

Zawiadomienie PUODO nie jest konieczne, jeżeli Zarząd – na podstawie dokonanej analizy – stwierdzi, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, w szczególności, jeżeli na skutek podjętych działań udało się usunąć negatywne skutki naruszenia.

1. Jeżeli **naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, LGD niezwłocznie **zawiadamia osobę, której dane dotyczą, o takim naruszeniu** (jeżeli naruszenie dotyczyło większej liczby osób, należy powiadomić je wszystkie).

Zawiadomienie powinno zostać sformułowane **prostym językiem**.

**Zawiadomienie osoby, której dane dotycząc nie jest konieczne**, jeżeli

* LGD wdrożyło odpowiednie środki ochrony wobec danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
* LGD, po stwierdzeniu naruszenia, zastosowało środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
* zawiadomienie danej osoby lub osób wymagałoby niewspółmiernie dużego wysiłku –w takim przypadku LGD wydaje na swojej stronie publiczny komunikat o naruszeniu.

1. Po stwierdzeniu naruszenia ochrony danych osobowych, niezależnie od tego, czy naruszenie zostało uznane za takie, które wymaga poinformowania PUODO lub osoby, której dane zostały naruszone, Zarząd odnotowuje jego wystąpienie w Rejestrze naruszeń ochrony danych osobowych, którego wzór stanowi **załącznik nr 10 do Polityki**.
2. **Opisane w poprzednich punktach postępowanie stosuje się również w sytuacji, gdy o naruszeniu ochrony danych osobowych, których administratorem jest LGD, poinformuje podmiot przetwarzający** (np. księgowa, dostawca określonych usług w Internecie).
3. Po podjęciu działań opisanych powyżej, Zarząd:

* jeżeli naruszenia ochrony danych osobowych dopuścił się adresat Polityki – rozważa zastosowanie wobec niego środków odpowiedzialności dyscyplinarnej i porządkowej albo podjęcie stosownych działań zmierzających do odwołania go z pełnionej przez niego funkcji;
* jeżeli naruszenie może zostać sklasyfikowane jako wykroczenie lub przestępstwo –zawiadamia o naruszeniu Policję lub inne organy ścigania.

1. Kraje bezpieczne to kraje spoza UE i EOG, wobec których Komisja Europejska wydała stosowną decyzję: aktualna lista państw uznawanych za bezpieczne znajduje się pod adresem <https://giodo.gov.pl/163/id_art/1519/j/pl>. Lista może być aktualizowana. [↑](#footnote-ref-1)