Załącznik do Uchwały Zarządu NGR
nr 1/21.05.2025 z dnia 21 maja 2025 roku

POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ NADNOTECKĄ GRUPĘ RYBACKĄ

przyjęta uchwałą Zarządu Stowarzyszenia NGR nr 1/21.05.2025 z dnia 21.05.2025 roku

Spis treści

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

1. Niniejszy dokument, zwany dalej „**Polityką**”, reguluje zasady przetwarzania danych osobowych przez Nadnotecką Grupę Rybacką, zwane dalej „**Stowarzyszeniem**” lub „**NGR**”.

Celem Polityki jest:

1) ustalenie reguł postępowania, które gwarantują przestrzeganie przez NGR zasad domyślnej prywatności (*privacy by default*), prywatności od etapu projektowania (*privacy by default*) oraz minimalizacji danych;
2) określenie, w jaki sposób NGR 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 NGR;
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 NGR, tj. Politykę przetwarzania danych osobowych przez Nadnotecką Grupę Rybacką przyjęty uchwałą Zarządu Stowarzyszenia NGR nr 1/1.10.2018 z dnia 1 października 2018 roku.

2. Bezpośrednim powodem przyjęcia Polityki było rozpoczęcie wdrażania nowej Lokalnej Strategii Rozwoju finansowanej ze środków programu Fundusze Europejskie dla Rybactwa na lata 2021-2027 i związane z tym ryzyka, nieuwzględniane w trakcie przygotowywania poprzedniej polityki, o której mowa w pkt 1 Polityki, tj. przede wszystkim elektroniczna obsługa naborów, z wykorzystaniem systemu CST. Było to także wyrazem wynikającej z poprzedniej Polityki reguły zakładającej konieczność okresowej oceny Polityki w kontekście jej adekwatności do realizowanych w Stowarzyszeniu procesów.

3. Opracowanie Polityki zostało poprzedzone dokonaniem analizy procesów przetwarzania danych przez NGR, dotychczasowych doświadczeń na tym polu, posiadanych zasobów organizacyjnych, technicznych i osobowych. Na tej podstawie Stowarzyszenie wdrożyło rozwiązania znajdujące odzwierciedlenie w treści Polityki.

4. W celu dostosowania sposobu postępowania do podejścia opartego na ryzyku (*risk based approach*), NGR, 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 analizę** zagadnień związanych z przetwarzaniem danych osobowych i ustali, czy istnieje potrzeba aktualizacji Polityki i sposobu postępowania z danymi osobowymi.

Przeprowadzenie takiej analizy stanowi wyraz stosowania przez NGR 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* wyjaśniono w dalszej części Polityki.

5. 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:

1) **Polityka** – niniejszy dokument;
2) **administrator** – podmiot decydujący o celach i warunkach przetwarzania danych osobowych (np. NGR 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);
3) **Zarząd** – Zarząd NGR;
4) **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);
5) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych;
6) **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;
7) **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;
8) **podmiot** – zarówno osoba fizyczna, jak i osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej, a także organ publiczny (organ administracji publicznej);
9) **osoba, której dane dotyczą** – konkretna osoba fizyczna, której dane przetwarza NGR i która zwraca się do Stowarzyszenia z określonym wnioskiem, z którą Stowarzyszenie się kontaktuje, wobec danych której NGR podejmuje określone działania;
10) **podmiot przetwarzający** – podmiot, który przetwarza dane osobowe w imieniu NGR (np. przechowuje, 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;
11) **strona (osoba) trzecia** – każdy podmiot, inny niż: (a) osoba, której dane dotyczą, (b) NGR, (c) podmiot przetwarzający (d) osoby, które z upoważnienia NGR lub podmiotu przetwarzającego mogą przetwarzać dane osobowe, których administratorem jest Stowarzyszenie;

12) **odbiorca** – podmiot, któremu NGR 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 im dane osobowe);

13) **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 NGR 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.

6. **Adresatem Polityki** (osobami zobowiązanymi do jej stosowania) są:

1) członkowie organów Stowarzyszenia, w tym członkowie Stowarzyszenia, jeżeli przetwarzają dane osobowe, których NGR jest administratorem;

2) pracownicy Stowarzyszenia (od momentu ich zatrudnienia);

3) stali współpracownicy Stowarzyszenia mający dostęp do danych osobowych (w szczególności osoby zatrudnione przez Stowarzyszenie na podstawie umów cywilnoprawnych do prac w biurze NGR, stażyści, wolontariusze);

4) podmioty przetwarzające Stowarzyszenia – w ograniczonym zakresie: z tymi podmiotami NGR 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.

7. **Polityka jest dokumentem, z którym zapoznać się powinni wszyscy pracownicy i stali współpracownicy Stowarzyszenia oraz członkowie organów Stowarzyszenia**.

8. 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), 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 NGR

Zasady i wartości

9. NGR przetwarza dane osobowe zgodnie z poniższymi, **podstawowymi zasadami,** które znajdują swoje odzwierciedlenie w dalszej treści Polityki:

1) dane są **przetwarzane zgodnie z prawem**;
2) dane są **zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach** i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) Stowarzyszenie **przetwarza tylko takie dane osobowe** i **tylko w takim zakresie, jaki jest niezbędny** dla realizacji celu zgodnego z prawem;
4) przetwarzanie danych osobowych przez Stowarzyszenie jest **ograniczone w czasie,** tj. dane osobowe są przetwarzane (w tym – przechowywane) **nie dłużej niż jest to niezbędne do realizacji celów**, dla których zostały zebrane;
5) dane są przetwarzane w sposób **przejrzysty** dla osoby, której dane dotyczą;
6) Stowarzyszenie podejmuje rozsądne działania, aby **przetwarzane dane osobowe były zgodne z prawdą i aktualne**, a **nieprawidłowe dane zostały usunięte**;
7) 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.

10. Zgodność z prawem.

W zakresie zgodności z prawem przetwarzania danych kluczową kwestią jest posiadanie odpowiedniej, zgodnej z prawem podstawy do ich przetwarzania. **NGR przetwarza wyłącznie te dane osobowe, co do których, w świetle art. 6 ust. 1, art. 9 ust. 2 lub art. 10 RODO, ma uzasadnioną podstawę**. Jeżeli NGR stwierdzi, że przetwarza dane osobowe (np. wyłącznie przechowuje), co do których nie ma uzasadnionej podstawy (np. zgody osoby, której dane dotyczą), albo jeżeli nie jest w stanie udokumentować takiej podstawy, zaprzestaje przetwarzania danych i niezwłocznie je usuwa ze swoich systemów / zbiorów dokumentów.

11. 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 NGR i adresatów Polityki jako dobro (zasób) stanowiące 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, dane zebrane w celu przeprowadzenia naboru i oceny wniosków, po dokonanej ocenie mogą być archiwizowane przez okres, który wynika z przepisów prawa i wiążących Stowarzyszenie umów o przyznanie pomocy);

5) minimalizować liczbę gromadzonych, używanych i ujawnianych danych osobowych do tylko tych danych, których przetwarzanie 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 niż minimalny 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 – Stowarzyszenie musi określić dla każdego procesu przetwarzania jak długo dane zgromadzone przy okazji tego procesu są potrzebne (tzw. okres retencji) i kiedy powinny zostać usunięte, a po upływie tego okresu dokonać ich usunięcia. Brak usuwania niepotrzebnych już danych stanowi częste naruszenie zasad RODO, które potencjalnie wiąże się z ryzykiem ich wycieku (dane niepotrzebne nie są wystarczająco chronione, często administrator sam nie ma świadomości, że znajduje się w ich posiadaniu).

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

Najważniejsze decyzje dotyczące przetwarzania danych są dokumentowane, a osoby przetwarzające dane działają w zakresie swoich obowiązków, których zakres jest udokumentowany.

Zarząd NGR 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 (w szczególności przekazuje do zapoznania się Politykę lub jej podsumowanie zawierające najważniejsze ustalenia i obowiązki jakie wprowadza dla pracownika).

Rejestr czynności przetwarzania

13. W celu zapewnienie kontroli nad procesem przetwarzania danych: nad tym jakie dane osobowe, w jakim celu i na jakiej podstawie są przetwarzane, **NGR prowadzi Rejestr czynności przetwarzania („RCP")**, którego **wzór stanowi załącznik nr 1 do Polityki**. W Rejestrze tym zamieszcza się informacje o przetwarzaniu przez Stowarzyszenie danych osobowych, dla których NGR 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 NGR będzie miała 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, NGR może np. usunąć dane określonej osoby fizycznej. Należy pamiętać, że aktualny Rejestr czynności przetwarzania jest najważniejszym dokumentem obrazującym jakie dane osobowe są przetwarzane w konkretnym okresie w Stowarzyszeniu, w jakim celu i na jakich zasadach. Ten dokument jest również pierwszym, który badają organy kontroli, w tym PUODO. Z tego powodu pilnowanie, by jego treść byłą aktualna i adekwatna do rzeczywistości jest jednym z najważniejszych zadań administratora.

14. W sytuacji, w której NGR przetwarza dane osobowe dla kogoś innego (np. przechowuje takie dane dla innego podmiotu, gromadzi je na jego zlecenie), Stowarzyszenie działa jako podmiot przetwarzający. Fakt ten powinien zostać uwzględniony w **Rejestrze kategorii czynności przetwarzania („RKCP"),** którego **wzór stanowi załącznik nr 2 do Polityki.**

15. **Za prowadzenie RCP i RKCP, o których mowa w pkt 13 i 14 Polityki, odpowiada Zarząd**, który może powierzyć obowiązek prowadzenia i aktualizacji tych Rejestrów pracownikowi, o którym mowa w **pkt 26 Procedury.**

Zarząd (lub wspomniana osoba) dokonuje analizy czy zapisy w RCP i RCKP pozostają aktualne, czy w tych rejestrach znajdują się informacje o wszystkich procesach przetwarzania danych osobowych przez NGR.

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

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

Security by design.

W zależności od wyników analizy, Zarząd podejmuje następujące działania:

1) **ustala**:
   a) jakiego **rodzaju dane osobowe** będą przetwarzane w ramach procesu,
   b) czy wszystkie kategorie danych osobowych, planowanych do pozyskania, są konieczne dla prawidłowego wdrożenia procesu,
   c) jaka jest **podstawa prawna** takiego przetworzenia;
   d) **kiedy należy usunąć dane** osobowe pozyskane w trakcie procesu,
   e) jakie ryzyka wiążą się z przetwarzaniem danych osobowych (np. w jaki sposób dane mogą ulec zniszczeniu, ujawnieniu osobom nieupoważnionym i jakie będą tego skutki), a także jak można zapobiegać takim wydarzeniom lub ograniczać ich negatywne skutki;
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 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) lub danych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, o których mowa w art. 10 RODO.

W celu dokonania takiej analizy NGR wykorzystuje szablon analizy ryzyka, który stanowi **załącznik nr 3 do Polityki**.

Privacy by default

NGR przetwarzając dane osobowe, wprowadza rozwiązania zmierzające do tego, by chroniona była 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, np. rejestrujących w bazie adresatów mailingu, zapisu na newsletter itp.) – 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 NGR na formularzu, który przygotowało Stowarzyszenie i który zawiera pytania na różne tematy, NGR wyraźnie odznacza kategorie danych, których podanie jest konieczne;

3) stosuje zindywidualizowane konta w systemach i programach wykorzystywanych do przetwarzania danych osobowych (np. indywidualne loginy i hasła do systemu CST używanego do przyjmowania wniosków w ramach naborów i korespondencji z wnioskodawcami), a osoby upoważnione do korzystania z tych systemów i programów nie mogą przekazywać nikomu loginów i haseł – w ten sposób inni użytkownicy mają ograniczony dostęp do danych osobowych i śledzenia aktywności innych użytkowników.

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 NGR danego zadania, a jedynie ułatwi NGR wykonanie pewnych obowiązków, Stowarzyszenie nie uzależnia wykonania tego zadania od podania tych „dodatkowych" danych;
2) prowadzi retencję danych osobowych w założonych z góry terminach, wynikających z Rejestru czynności przetwarzania, tj. usuwa dane osobowe, które nie są już potrzebne NGR i brak jest podstaw do ich dalszego przetwarzania przez Stowarzyszenie (np. w celu obowiązkowej archiwizacji).

Przetwarzanie danych osobowych przez osoby upoważnione

17. Przetwarzanie danych osobowych, których administratorem jest NGR, jest dopuszczalne jedynie przez osoby do tego upoważnione i jedynie w takim zakresie, w jakim określa to upoważnienie. **Upoważnień do przetwarzania danych osobowych udziela Zarząd**. Udzielanie upoważnień może zostać powierzone osobie wyznaczonej przez Zarząd.

W celu spełnienia zasady rozliczalności opisanej w RODO – NGR 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 NGR oraz innym osobom, które są zatrudnione w NGR (w tym np. praktykantom, stażystom, wolontariuszom) na podstawie umów cywilnoprawnych, jeżeli wykonują zadania dla Stowarzyszenia korzystając ze sprzętu i infrastruktury NGR;
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**. Wygaśnięcie upoważnienia należy zaznaczyć w tym Rejestrze.

Upoważnień nie udziela się członkom organów Zarządu NGR, którzy w okresie pełnienia swoich funkcji mają dostęp do wszystkich czynności przetwarzania w Stowarzyszeniu, wykonując zadania administratora danych. Upoważnienie członków Zarządu wynika bezpośrednio z charakteru pełnionych przez nich funkcji.

Członkowie Komisji Rewizyjnej NGR również nie otrzymują odrębnych pisemnych upoważnień, lecz są uprawnieni do przetwarzania danych wyłącznie w takim zakresie, w jakim jest to niezbędne do realizacji ich uprawnień kontrolnych wynikających ze Statutu NGR (przetwarzanie przez nich danych w szerszym zakresie wymaga już odrębnego, pisemnego upoważnienia).

Członkowie Rady NGR (konkretne osoby fizyczne uczestniczące w pracach organu) otrzymują upoważnienia. 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 (w tym: osobom fizycznym reprezentującym w Radzie członków – osoby prawne) udziela się upoważnień i ten fakt wpisuje się do Rejestru upoważnień.

Członkom NGR udziela się upoważnień, jeżeli w ramach wykonywania zadań dla Stowarzyszenia (realizowane w ramach obowiązków członkowskich, a nie na podstawie odrębnej

umowy), mają mieć dostęp do danych osobowych przetwarzanych przez NGR w szerszym zakresie niż jedynie udział w Walnym Zebrani Członków (np. jeżeli członek NGR miałby obsługiwać wydarzenie organizowane przez Stowarzyszenie, np. rejestrując uczestników, zbierając ich deklaracje itp.).

Podział osób upoważnionych na grupy przedstawia poniższa tabela:

KATEGORIA OSÓB	ZAKRES DANYCH OSOBOWYCH, KTÓRE CZŁONEK GRUPY MOŻE PRZETWARZAĆ (opis ma charakter zakresowy, generalne, poszczególne osoby z danej grupy mogą mieć węższy zakres upoważnienia)	Czy konieczne upoważnienie w formie odrębnego dokumentu?
Członkowie Zarządu	Wszystkie dane osobowe przetwarzane przez Stowarzyszenie	NIE
Członkowie Komisji Rewizyjnej	Wszystkie dane osobowe przetwarzane przez Stowarzyszenie, ale jedynie w zakresie wglądu do nich i ich kopiowania na potrzeby wykonywania obowiązków członka tego organu (bez możliwości modyfikacji, usuwania, itp.) – w zakresie niezbędnym do wykonywania zadań statutowych.	NIE
Członkowie Rady	Dane osobowe zawarte we wnioskach o przyznanie pomocy, załącznikach do wniosków, składanych wyjaśnieniach i uzupełnieniach, protestach, wnioskach o aneks do umowy o przyznanie pomocy	TAK
Pracownicy biura Stowarzyszenia	Dane osobowe przetwarzane przez Stowarzyszenie dotyczące spraw, które mieszczą się w zakresie ich obowiązków pracowniczych. Zakres danych i czynności ograniczony upoważnieniem.	TAK
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. Zakres danych i czynności ograniczony upoważnieniem lub umową powierzenia.	TAK
Stażyści, wolontariusze	Dane osobowe niezbędne do realizacji zadań określonych w dokumencie, na podstawie którego te osoby wykonują świadczenia dla Stowarzyszenia. Zakres danych i czynności ograniczony upoważnieniem.	TAK
Członkowie Stowarzyszenia	Dane osobowe niezbędne do realizacji zadań dla Stowarzyszenia.	TAK

Pozostają w mocy upoważnienia do przetwarzania danych osobowych, które zostały udzielone przed wejściem w życie Polityki (tj. na podstawie Polityk przyjętej uchwałą Zarządu Stowarzyszenia NGR nr 1/1.10.2018 z dnia 1 października 2018 roku).

– nie ma potrzeby osobom dotychczas upoważnionym odwoływać udzielonych upoważnień, po to tylko, żeby przyznać im je po chwili na nowo, w oparciu o Politykę, jeżeli zakres upoważnienia nie zmienił się. Jeżeli jednak zakres upoważnienia po wejściu w życie Polityki miałby się zmienić w stosunku do zakresu dotychczasowego upoważnienia – należy wydać nowe upoważnienie.

Powierzenie podmiotom trzecim danych, których administratorem jest NGR

18. Przetwarzanie danych osobowych przez NGR 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 NGR, wykonując określone zadania, które realizować powinno Stowarzyszenie i wykorzystując przy tym przetwarzaniu swoje zaplecze organizacyjne i techniczne (np. swój komputer, niepodpięty do systemu NGR, swoje programy, pracowników i biuro). Podmiot przetwarzający jest zatem „podwykonawcą" Stowarzyszenia w przetwarzaniu danych osobowych.

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) 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 NGR, z reguły są podmiotami przetwarzającymi, ponieważ cechą działalności gospodarczej jest prowadzenie czynności we własnym imieniu, na własny rachunek i ryzyko.

19. **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. Weryfikacja odbywa się poprzez zadanie pytań na temat stosowanych zabezpieczeń, udzielania upoważnień osobom mającym dostęp do danych osobowych, prowadzenia Rejestru kategorii czynności przetwarzania, itp.

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 udziela odpowiedzi na pytania, lub można oczekiwać, że ich nie udzieli, 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.

20. Powierzając podmiotowi trzeciemu dane osobowe, **NGR 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]

Sprawdzenia dokonuje się weryfikując informacje podane przez ten podmiot w jego Regulaminie wykonywania usług, na jego stronie internetowej w odpowiedzi na zadanie przez Stowarzyszenie pytania, itp.

Wybór podmiotu, który nie spełnia powyższych warunków przetwarzania danych na obszarze Unii, EOG lub krajów bezpiecznych, jest dopuszczalny jedynie wyjątkowo.

[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://uodo.gov.pl/pl/535/2502. Lista może być aktualizowana

Zawierając umowę związaną z przekazywaniem danych osobowych poza granice UE lub EOG, NGR może skorzystać z wzorcowych klauzul umownych opracowanych przez KE.

21. NGR 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 NGR, regulaminu świadczenia usług, w ramach których mają być przetwarzane dane osobowe powierzone przez Stowarzyszenie, którego akceptacja jest konieczna do świadczenia usług).

22. W celu powierzenia przetwarzania danych osobowych, NGR:

1) 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 6 do Polityki**;

2) 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.

NGR jako podmiot przetwarzający

23. Jeżeli NGR 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 2 do Polityki**);

3) **nie może zlecać wykonywania jakichkolwiek czynności wobec takich danych osobowych innym podmiotom** (tj. innym osobom niż pracownicy i organy NGR, (tzw. „**podpowierzenie**"), chyba że:

   a) uzyskała zgodę administratora tych danych lub

   b) uprzedziła 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, NGR niezwłocznie informuje administratora tych danych** o takim zdarzeniu i udziela mu wszelkiej niezbędnej pomocy w celu zapobieżenia lub ograniczenia skutków takiego zdarzenia.

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

Zadania Zarządu

24. 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.**

25. Do kompetencji Zarządu należy w szczególności:

1) udzielanie i cofanie pracownikom i członkom pozostałych organów Stowarzyszenia upoważnień do przetwarzania danych osobowych (kompetencja może zostać przekazana innej osobie, np. jednemu z członków Zarządu);
2) prowadzenie Rejestru czynności przetwarzania i Rejestru kategorii czynności przetwarzania (zadanie do może powierzyć pracownikowi ds. bezpieczeństwa);
3) zgłaszanie, w stosownych przypadkach, PUODO oraz osobom, których dane osobowe zostały naruszone, informacji o naruszeniu bezpieczeństwa danych osobowych;
4) podejmowanie stosownych działań (np. dyscyplinujących) w przypadku stwierdzenia naruszenia przez adresatów Polityki zasad przetwarzania danych osobowych przez Stowarzyszenie, określonych w przepisach prawa i Polityce;
5) podejmowanie decyzji o powierzeniu podmiotowi trzeciemu przetwarzania danych osobowych, których administratorem jest NGR, podejmowanie decyzji dotyczących dalszej współpracy z takim podmiotem w przypadku stwierdzenia naruszenia przez niego warunków przetwarzania danych osobowych administrowanych przez Stowarzyszenie;
6) przeprowadzanie okresowych analiz związanych z przetwarzaniem danych osobowych, aktualizacja i dokonywanie zmian Polityki;
7) zapewnianie, w razie potrzeby, zewnętrznych szkoleń dla pracowników i członków organów Stowarzyszenia z obowiązujących przepisów w zakresie ochrony danych osobowych oraz z postanowień Polityki;
8) 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 – podjęcie decyzji dotyczącej 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).

26. W celu koordynowania w Stowarzyszeniu bieżących procesów związanych z przetwarzaniem danych osobowych, Zarząd może wyznaczyć jedną osobę (np. pracownika biura NGR) odpowiedzialnego za te kwestie.

Wskazana wyżej osoba wyznaczona przez Zarząd **nie będzie wówczas inspektorem ochrony danych** w rozumieniu art. 37 RODO – jego wyznaczenie będzie miało 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 tej osobie charakterystycznej dla inspektora ochrony danych samodzielnej pozycji w organizacji.

27. Wyznaczenie osoby, o której mowa w pkt 26 Polityki, powinno i może wiązać się ze zmianą zakresu obowiązku służbowych.

28. Do zadań osoby, o której mowa w pkt 26 Polityki, może należeć:

1) czuwanie nad przestrzeganiem postanowień Polityki w ramach bieżącego funkcjonowania Stowarzyszenia, a zwłaszcza biura;
2) prowadzenie i aktualizacja Rejestru osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu, a także – jeżeli zleci to Zarząd – prowadzenie i aktualizacja Rejestru Czynności Przetwarzania i Rejestru Kategorii Czynności Przetwarzania;
3) monitorowanie przepisów prawnych w kontekście zasad przetwarzania danych osobowych przez Stowarzyszenie;
4) 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;
5) sygnalizowanie Zarządowi konieczności dokonania zmian w Polityce;
6) zaznajamianie nowych pracowników Stowarzyszenia z zasadami przetwarzania danych osobowych przez Stowarzyszenie;
7) 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;
8) 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;
9) przygotowywanie, w porozumieniu, projektu upoważnienia do przetwarzania danych osobowych dla nowych pracowników lub dla pracowników, którzy mają uzyskać upoważnienie do przetwarzania danych w szerszym niż dotychczas zakresie.

Przewodniczący Komisji Rewizyjnej i Rady NGR

29. Przewodniczący. 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:

1) **zaznajamianie członków organów z zasadami przetwarzania danych osobowych przez Stowarzyszenie** w związku z pracami danego organu i przypominanie im o obowiązku zachowania poufności – zachowania w tajemnicy informacji i danych osobowych uzyskanych w trakcie prac w danym organie Stowarzyszenia;
2) **by sporządzana w efekcie prac organów dokumentacja była zgodna z Polityką** (w szczególności realizowała wymóg minimalizacji danych osobowych, pseudonimizacji, by dane osobowe były należyte zabezpieczone);
3) **identyfikowanie i dokumentowanie oraz informowanie Zarządu o wykrytych przypadkach naruszenia ochrony danych** osobowych lub nieprzestrzegania Polityki przez członków danego organu;
4) **stosowanie przez dany organ rozwiązań zgodnych z rozporządzeniem RODO,** w szczególności zmierzających do ograniczenia ilości przetwarzanych danych, ograniczenia liczb kopii danych osobowych.

30. Niezależnie od zadań wskazanych w ust. 1, Przewodniczący Rady:

1) 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,

2) sygnalizuje Zarządowi konieczność dokonania zmian w procedurach i kryteriach stosowanych przez Radę w kontekście zapewnienia lepszego poziomu ochrony danych;

3) dba o to, by dane osobowe zawarte we wnioskach o dofinansowanie, były traktowane ze szczególną ostrożnością, by członkowie Rady nie sporządzali na prywatny użytek kopii lub wypisków z wniosku, a także by i informacje dotyczące przebiegu posiedzenia w sprawie oceny operacji były zachowywane w poufności (poza informacjami publicznymi, zamieszczanymi w protokole z posiedzenia).

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

Ogólne zasady

31. Stowarzyszenie podejmuje niezbędne działania, aby prawa osób, których dane są przetwarzane przez NGR, 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).

32. Realizując uprawnienia osoby, której dane dotyczą, NGR 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 NGR z żądaniem określonego działania związanego z jej danymi osobowymi, Stowarzyszenie:

1) **ustala tożsamość osoby, która zwróciła się o wykonanie przez NGR określonego działania związanego z danymi osobowymi**. Ustalenie tożsamości powinno zostać dokonane w ten sposób, że NGR upewnia się, działania, których oczekuje dana osoba, rzeczywiście dotyczą jej danych:
   - 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 tożsamości lub o przedstawienie informacji potwierdzającej tożsamość wnioskującego o podjęcie określonych działań;
   - jeżeli żądanie zostało złożone w innej formie, NGR weryfikuje, czy żądanie zostało przesłane do Stowarzyszenia z tego samego adresu, numeru telefonu itp., który został przypisany w dokumentacji prowadzonej przez NGR do osoby, której dane mają zostać przekazane;
   - jeżeli NGR, 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 NGR 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;
2) 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).

33. Realizacja uprawnień osoby, której dane osobowe przetwarza NGR, wymaga komunikacji z tą osobą. W celu właściwego wypełnienia obowiązków Stowarzyszenia, wprowadza się następujące reguły dotyczące komunikacji z osobami, których dane przetwarza NGR.

- komunikacja powinna odbywać się za pomocą zwięzłych, przejrzystych i zrozumiałych komunikatów, słownictwo powinno być proste;

- **komunikacja powinna odbywać się na piśmie**, w tej samej formie, w jakiej zwróciła się osoba trzecia, żądająca od NGR określonego działania;
- jeżeli osoba, której dane dotyczą, tego zażąda, **informacji można udzielić ustnie**;
- **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, powinno taką informację przekazać temu podmiotowi** – 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, NGR 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

34. 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 uzyskaniem zgody na przetwarzanie danych. Obowiązek informacyjne realizowany jest niezależnie od podstawy przetwarzania danych. Pomimo pozyskania zgody danej osoby na przetwarzanie jej danych, konieczne jest jej poinformowanie o kwestiach dotyczących przetwarzania jej danych osobowych, zaś zrealizowanie obowiązku informacyjnego nie oznacza uzyskania zgody na przetwarzanie danych osobowych.

Przekazanie informacji może w szczególności polegać na:

1) przekazaniu osobie zainteresowanej wydrukowanej informacji (dla celów dowodowych warto odbierać od takiej osoby podpis potwierdzający zapoznanie się z informacją);
2) umieszczeniu informacji pod lub na drugiej stronie formularza o zgodzie 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 zasadę rozliczalności, nakazującą administratorowi realizować obowiązki w sposób pozwalający w razie potrzeby wykazać ich spełnienie.

Należy pamiętać, że każda klauzula informacyjna powinna być dostosowana do konkretnego procesu przetwarzania i modyfikowana w razie potrzeby – m.in. o zmianie, w zależności od sytuacji podlegać powinna podstawa prawna, cele przetwarzania, prawa osoby przetwarzanej, okres przetwarzania.

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

- 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 odwiedzających stronę, pliki cookies, mechanizmy Google Analitics, itp.);
- w przypadku rejestracji nowych członków NGR, do formularza deklaracji członkowskiej dołącza klauzulę informacyjną;
- w przypadku umów zawieranych przez NGR dodaje jako osobny załącznik klauzulę informacyjną, bądź przed zawarciem umowy informuje w udokumentowany sposób kontrahenta o kwestiach określonych w art. 13 RODO;
- nowy pracownik wraz zawarciem umowy potwierdza zapoznanie się z klauzulą informacyjną oraz Polityką przetwarzania danych osobowych;
- w przypadku składania przez wnioskodawców dokumentów w ramach naborów i konkursów ogłoszonych w związku z realizacją LSR – zapewnia rozwiązania pozwalające na zapoznanie się wnioskodawcy z klauzulą informacyjną NGR (np. jako element formularza wniosku);
- przekazuje klauzulę informacyjną w przypadku doradztwa świadczonego w związku z realizacją LSR;
- na formularzach zgłoszeniowych na wydarzenia organizowane przez NGR 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);
- w przypadku publikowania ogłoszeń o pracę w Stowarzyszeniu do ogłoszenia należy dołączyć klauzulę informacyjną.

35. 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 NGR), **ma obowiązek poinformować taką osobę o okolicznościach wskazanych w art. 14 RODO.**

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.**

Prawo dostępu do danych osobowych

36. Osoba, której dane dotyczą, jest uprawniona do uzyskania od NGR:

1) **potwierdzenia czy Stowarzyszenie przetwarza dane osobowe jej dotyczące**.

W przypadku zgłoszenia się do NGR 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 32 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 NGR przetwarza albo nie przetwarza dane osobowe dotyczące osoby pytającej);

2) **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);

3) **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 NGR – w zależności od konkretnego przypadku i podstawy przetwarzania danych – sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz możliwości wniesienia sprzeciwu wobec przetwarzania;
- prawa do wniesienia skargi do PUODO;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich informacji o źródle danych;

4) **uzyskania kopii danych osobowych**, które przetwarza NGR, przy czym prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych – **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.

37. Osoba zainteresowana, jeżeli jest uprawniona (co podlega weryfikacji opisanej wyżej), może skorzystać z jednego, kilku lub wszystkich uprawnień opisanych wyżej.

Prawo do sprostowania danych

38. Osoba, której dane dotyczą, ma prawo żądania od NGR:

1) **niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe;**

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

a) uprzedniej weryfikacji, czy podmiot zwracający się z żądaniem faktycznie jest podmiotem, którego dane dotycząc (patrz pkt 32 Polityki);

b) sprawdzeniu, czy dane są faktycznie nieprawidłowe (np. nieaktualne, błędne).

Jeżeli dane są rzeczywiście nieprawidłowe lub nieaktualne NGR;

a) niezwłocznie je prostuje we wszystkich swoich dokumentach i systemach, o czym informuje osobę, która zwróciła się do niego z żądaniem sprostowania;

b) zawiadamia wszystkich odbiorców danych, że osoba, której dane dotyczą, żąda, sprostowania nieprawidłowych lub nieaktualnych danych (np. jeżeli w ramach projektu, w którym uczestniczy NGR, Stowarzyszenie zebrało dane od uczestników wyjazdu integracyjnego i następnie przekazała je innym partnerom projektu, to wniosek uczestnika o sprostowanie nieprawidłowego nazwiska jednego z uczestników wyjazdu należy przekazać do tych partnerów);

2) **żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia**

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

a) uprzedniej weryfikacji, czy podmiot zwracający się z żądaniem faktycznie jest podmiotem, którego dane dotycząc (patrz pkt 32 Polityki);

b) ustaleniu, czy uzupełnienie danych osobowych **jest zgodne z celami, dla których dane zostały zebrane** (NGR 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:

a) niezwłocznie je uzupełnia, o czym informuje osobę, która zwróciła się do niego z żądaniem uzupełnienia;

b) zawiadamia wszystkich odbiorców danych, że osoba, której dane dotyczą, żąda, uzupełnienia jej danych (np. jeżeli w ramach projektu, w którym uczestniczy NGR, Stowarzyszenie zebrało dane od uczestników wyjazdu integracyjnego i następnie przekazała je innym partnerom projektu, to wniosek uczestnika o uzupełnienie nieprawidłowego nazwiska jednego z uczestników wyjazdu należy przekazać do tych partnerów).

Prawo do bycia zapomnianym

39. Osoba, której dane dotyczą, ma prawo żądania od NGR 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 (patrz pkt 32 Polityki);

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:

   a) dane osobowe **nie są już niezbędne** do celów, w których zostały zebrane lub w inny sposób przetwarzane,

   b) osoba, której dane dotyczą, **cofnęła zgodę,** na której opiera się przetwarzanie,

   c) osoba, której dane dotyczą, **wnosi sprzeciw**, o którym mowa w pkt 46 Polityki, wobec przetwarzania jej danych osobowych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania tych danych przez NGR,

   d) osoba, które dane dotyczą **wniosła sprzeciw**, o którym mowa w pkt 46 Polityki, a przetwarzane dane wykorzystywane były do **marketingu bezpośredniego**,

   e) dane osobowe **były przetwarzane niezgodnie z prawem**,

   f) dane osobowe **muszą zostać usunięte w celu wywiązania się z obowiązku prawnego** przewidzianego w prawie (np. minął już okres obowiązkowego przechowywania określonych kategorii danych),

   g) 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).

   Stowarzyszenie **nie jest zobowiązane do usunięcia danych**, jeżeli dane są w dalszym ciągu niezbędne z uwagi na choćby jedną z poniższych okoliczności:

   a) do korzystania z prawa do wolności wypowiedzi i informacji,

   b) 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),

   c) do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej NGR,

   d) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,

   e) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do bycia zapomnianym w tym konkretnym przypadku uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,

   f) do ustalenia, dochodzenia lub obrony roszczeń.

W przypadku stwierdzenia, że NGR 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.

40. 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**).

41. W celu skutecznej realizacji prawa do bycia zapomnianym NGR 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.

Prawo do ograniczenia przetwarzania

42. Osoba, której dane dotyczą, ma prawo żądania od NGR 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.

43. Po otrzymaniu żądania dotyczącego ograniczenia przetwarzania NGR:

1) **ustala tożsamość osoby**, która zwróciła się do Stowarzyszenia z takim żądaniem (patrz pkt 32 Polityki);

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 38 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 NGR jest **niezgodne z prawem, ale osoba, której dane dotyczą, sprzeciwia się usunięciu swoich danych osobowych**, żądając jedynie ograniczenia ich wykorzystywania (w związku z tym NGR musi zablokować możliwość wykorzystywania danych osobowych, możliwość wglądu do nich, modyfikacji, wyświetlania itp., ale nie może ich usunąć);

3) **NGR nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą**, do ustalenia, dochodzenia lub obrony roszczeń (przeciwko NGR lub przeciwko innemu podmiotowi);

4) **osoba, której dane dotyczą, wniosła sprzeciw**, o którym mowa w pkt 46 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 pozwalające na odmówienie usunięcia danych.

44. Nawet jeżeli Stowarzyszenie ograniczy przetwarzanie danych osobowych stosownie do żądania osoby zainteresowanej, to j**ednak w pewnych może 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 NGR,

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

45. Osoba, której dane dotyczą, ma prawo:

1) **otrzymać dane** osobowe jej dotyczące, które dostarczyła do NGR (np. wypełniając drogą elektroniczną formularz rejestracyjny, składając wniosek);

2) **przesłać dane** osobowe jej dotyczące, które dostarczyła do NGR**, innemu administratorowi** bez przeszkód ze strony Stowarzyszenia;

3) **zażądać od NGR**, 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.).

NGR jest zobowiązana do zrealizowania czynności, których żąda dana osoba, po zweryfikowaniu tożsamości osoby wnioskującej (pkt 32 Polityki), jeżeli spełnione są łącznie następujące przesłanki:

1) Stowarzyszenie przetwarza dane osobowe tego podmiotu:

   a) **na podstawie jego zgody lub**

   b) **w celu zawarcia lub realizacji umowy**, której stronami są Stowarzyszenie i ten podmiot;

2) przetwarzanie danych **odbywa się w sposób zautomatyzowany**, tzn. są to dane możliwe do odczytania i edycji na komputerze, zapisane na w pamięci elektronicznej.

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

1) pozyskała 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.;

2) przetwarza dane osobowe **w formie papierowej** (nie posiada ich elektronicznej kopii).

Prawo do sprzeciwu

46. Osoba, której dane dotyczą, ma prawo – w sytuacji określonej w pkt 47 Polityki – wnieść sprzeciw wobec przetwarzania jej danych.

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

1) weryfikuje tożsamość wnoszącego sprzeciw (pkt 32 Polityki);

2) ustala czy zachodzą przesłanki do uwzględnienia sprzeciwu.

47. Prawo do wniesienia sprzeciwu przysługuje, jeżeli:

1) 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*”);

2) 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 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);

3) dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego.

48. W przypadku wniesienia sprzeciwu w sytuacji, o której mowa w pkt 47 Polityki, Stowarzyszenie nie może już przetwarzać danych osobowych tego, kto wniósł sprzeciw, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Zautomatyzowane podejmowanie decyzji i profilowanie

49. 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.

Profilowanie jest dopuszczalne, ale **należy o tym informować osoby profilowane.**

50. Zautomatyzowane podejmowanie decyzji

Osoba, której dane dotyczą, ma **prawo do tego, by nie podlegać decyzji NGR, 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.

Zautomatyzowane podejmowanie decyzji 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).

51. NGR nie stosuje profilowania ani nie podejmuje zautomatyzowanych decyzji.

W przypadku rozpoczęcia procesów obejmujących profilowanie lub podejmowanie zautomatyzowanych decyzji NGR dokona analizy ryzyka tego procesu oraz zaktualizuje niniejszą Politykę.

ROZDZIAŁ V
STOSOWANE PRZEZ STOWARZYSZENIE ŚRODKI ZABEZPIECZENIA DANYCH

52. NGR wdraża opisane w niniejszym rozdziale środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami prawa, aby przeciwdziałać incydentom bezpieczeństwa oraz zmniejszyć ryzyko ich wystąpienia, a także.

53. Środki techniczne i organizacyjne opisane niżej uwzględniają wynik dokonanej przez NGR 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.

54. Przyjęte przez NGR środki dzielą się na: organizacyjne, fizyczne i techniczne.

Środki organizacyjne:

55. Do **najważniejszych środków organizacyjnych,** które zostały przyjęte w celu zapewnienia należytego poziomu ochrony danych osobowych, należą następujące zasady:

1) 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;

2) **naruszenie postanowień Polityki lub przepisów prawa regulujących zasady przetwarzania danych osobowych wiążę się z konsekwencjami** dyscyplinarnymi lub organizacyjnymi dla naruszyciela, o czym adresaci Polityki są informowani przez Zarząd NGR;

3) **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 naruszenia ochrony danych osobowych mógł być odpowiedzialny za takie zdarzenie);

4) Stowarzyszenie, w celu zapewnienia zasady minimalizacji danych, **ogranicza przetwarzanie poszczególnych kategorii danych do określonych grup osób** (nie dopuszcza się wszystkich osób do wszystkich danych);

5) **pracownicy i nowi członkowie organów NGR, pierwszego dnia wykonywania swoich obowiązków, zapoznają się z Polityką i jej najważniejszymi zasadami**, by byli świadomi swoich obowiązków, odpowiedzialności oraz zasad przetwarzania danych osobowych w Stowarzyszeniu. Są oni również pouczani o tym, że naruszenie zasad Polityki i przepisów dotyczących ochrony danych osobowych stanowi podstawę ich odpowiedzialności dyscyplinarnej, organizacyjnej lub umownej, a także może stanowić wykroczenie lub przestępstwo, a w przypadku gdy takie osoby stwierdzą naruszenie ochrony danych osobowych (nawet takie, za które oni sami nie odpowiadają) mają obowiązek niezwłocznego zgłoszenia go Zarządowi;

6) NGR **określiła podział odpowiedzialności poszczególnych osób za kwestie związane z przetwarzaniem danych osobowych**:

- za wszystkie sprawy związane z przetwarzaniem danych odpowiedzialny jest Zarząd;
- Zarząd może wyznaczyć osobę (spośród swoich członków lub np. pracowników biura NGR), 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;
- **NGR 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. NGR przetwarza z niewielkim zakresie szczególne kategorie danych, jednak z uwagi na pojedyncze rekordy takich danych, uznała, że przetwarzanie to nie odbywa się na „dużą skalę", o której mowa w art. 37 ust. 1 RODO;**

7) NGR **wybiera podmioty przetwarzające dane osobowe, którymi administruje, po przeprowadzeniu ich weryfikacji**:
   - analizie odpowiedzi na pytania zadanie przez Stowarzyszenie, dotyczące zasad przetwarzania danych osobowych przez podmiot (np. czy podmiot sporządził dokumentację dotyczącą przetwarzania danych osobowych, czy istnieją procedury reagowania na naruszenie zasad przetwarzania danych osobowych, czy podmiot stosuje upoważnienia do przetwarzania danych osobowych, czy dane osobowe będą przetwarzane poza obszarem Europejskiego Obszaru Gospodarczego),
   - 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;
   - preferowane są podmioty posiadające siedzibę na terenie Unii Europejskiej lub deklarujące przetwarzanie danych na terenie Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
8) **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;
9) **weryfikacja podmiotów (firm) będących procesorami danych osobowych Stowarzyszenia w chwili wejścia w życie Polityki** – pod kątem dostosowania się tych podmiotów do wymagań rozporządzenia RODO;
10) 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**);
11) **okresowe analizy treści Polityki,** w tym weryfikacja przyjętych środków ochrony danych osobowych, w kontekście ich aktualności i adekwatności do poziomu ryzyka w danym momencie;
12) **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;

13) **wdrożenie zasady *privacy by default* oraz minimalizacji danych – NGR 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;

14) **okresowe szkolenia dla osób upoważnionych do przetwarzania danych osobowych, członków organów, stałych współpracowników NGR** – ze znajomości przepisów dotyczących przetwarzania danych osobowych oraz z postanowień Polityki;

15) **obowiązywać będzie zasada czystego biurka:** po godzinach pracy pracownik zostawia po sobie czyste biurko (dokumenty wracają do segregatorów, segregatory, dokumenty i teczki umieszczane są w szafie), w trakcie pracy na biurku znajdują się wyłącznie dokumenty, z których aktualnie korzysta pracownik;

16) obsługa interesantów Stowarzyszenia odbywa się w ten sposób, by uniknąć przebywania w jednym pomieszczeniu biura NGR więcej niż jednego interesanta (w celu uniknięcia ryzyka podejrzenia na dokumentach lub usłyszenia informacji stanowiących dane osobowe lub inne dane wrażliwe);

17) 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;

18) pracownikom korzystającym z systemów informatycznych zawierających dane osobowe przyznawane są indywidualne loginy i hasła, którymi nie mogą się dzielić z innymi osobami. W szczególności dotyczy to systemu CST, za pomocą którego odbywa się obsługa naborów ogłaszanych przez NGR w związku z realizacją LSR;

19) 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 bez uprzedniej zgody przełożonego;

20) na stronie internetowej administrowanej przez Stowarzyszenie zostanie zamieszczona Polityka prywatności, stanowiąca dokument z jednej strony realizujący wobec osób trzecich obowiązek wynikający z art. 13 i 14 RODO (w sytuacji, w której bezpośrednie przekazanie wymaganych klauzul informacyjnych byłoby trudne, czaso- lub kosztochłonne), z drugiej zaś mający na celu zaznajomienie tych osób z podstawnymi procesami przetwarzania danych osobowych przez Stowarzyszenie;

21) została przyjęta **procedura zapewnienia ciągłości działania Stowarzyszenia** (art. 32 ust. 1 pkt b RODO) oraz procedura odtwarzania systemu po awarii, oraz ich testowania (art. 32 ust. 1 pkt c i d RODO) – opisane w dalszej części Polityki;

22) Przyjęto zasady korzystania z poczty elektronicznej NGR (stanowiące **załącznik nr 7 do Polityki**) oraz zasady korzystania przez pracowników z komputerów służbowych (**załącznik nr 8 do Polityki**);

23) każdy incydent bezpieczeństwa lub zdarzenie budzące wątpliwości w kontekście nieuprawnionego ujawnienia, zmodyfikowania lub utraty danych osobowych jest niezwłocznie zgłaszane przez członków Stowarzyszenia, jego pracowników, współpracowników, stażystów, wolontariuszy, praktykantów lub członków organów Stowarzyszenia do pracownika, o którym mowa w pkt 26 Polityki, oraz do Zarządu;

24) ogranicza się wysyłanie wiadomości do wielu adresatów; w przypadku wysyłania wiadomości do wielu adresatów spoza Stowarzyszenia należy korzystać z opcji ukrycia ich adresów

(np. „UDW"), tak by nie były widoczne dla pozostałych osób uczestniczących w korespondencji; wyjątkowo dopuszcza się odstępstwo od tej zasady w sytuacji, gdy adresaci takiej wiadomości mają uczestniczyć między sobą w dalszej korespondencji w sprawie, której dotyczy pierwsza wiadomość;

25) w związku z korzystaniem z systemu CST do obsługi naborów ogłaszanych w związku z wdrażaniem LSR, opracowana została szczególna Polityka bezpieczeństwa oraz przetwarzania danych przez RLGD w CST2021 oraz portalu Fundusze Europejskie, w zakresie naborów ogłaszanych przez RLGD, która stanowi odrębny dokument.

Środki fizycznej ochrony

56. Do **najważniejszych elementów fizycznej ochrony**, które zostały przyjęte w celu zapewnienia należytego poziomu ochrony danych osobowych, należą następujące środki:

1) **przetwarzanie danych osobowych odbywa się co do zasady w biurze Stowarzyszenia**, dlatego pomieszczenia biura są **zabezpieczone przed wejściem nieuprawnionych osób**:

- biuro NGR jest zabezpieczone na klucz;
- budynek, w którym znajduje się biuro Stowarzyszenia objęty jest ochroną fizyczną i monitoringiem;
- biuro i poszczególne pomieszczenia biura, w czasie, gdy nie znajdują się w nich pracownicy Stowarzyszenia, są zamykane na klucz; w przypadku opuszczenia pomieszczenia, w którym przetwarza się dane osobowe, przez ostatnią osobę, pomieszczenie zamykane jest na klucz i oddawane na recepcje, 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) **należy do minimum ograniczyć posługiwanie się małymi 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,
- dysk jest zaszyfrowany i dostęp niego został zabezpieczony hasłem.

Zaleca się zablokowanie dostępu do portów USB w komputerach, ew. dostęp do nich jedynie po wpisaniu hasła przez użytkownika.

5) przenośne urządzenia elektroniczne zawierające dane osobowe (laptopy pracowników Biura, laptopy członków Zarządu, na których przetwarzają dane osobowe) mają zaszyfrowane dyski, możliwość zalogowania się do urządzenia jest poprzedzona wpisaniem hasła;

6) **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

57. NGR w następujący sposób zabezpiecza dane osobowe, które przetwarza za pomocą swoich urządzeń elektronicznych:

1) pracownicy i osoby stale współpracujące ze Stowarzyszeniem przetwarzają dane osobowe w sieci Stowarzyszenia, za pomocą urządzeń należących do Stowarzyszenia;

2) 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 zadeklarowaniu, że osoba upoważniona:

- korzysta z urządzenia posiadającego odpowiednią ochronę antywirusową, spyware, maleware, która jest regularnie aktualizowana,
- zabezpiecza dostęp do urządzenia hasłem;
- w przypadku przetwarzania danych osobowych w systemie informatycznym NGR służącym do oceny wniosków – dostęp do tego programu jest zabezpieczony indywidualnym hasłem, a każda aktywność użytkownika w tym systemie (np. kopiowanie danych na urządzenie) jest rejestrowana;

- zabronione jest kopiowanie na prywatne urządzenia danych osobowych, których administratorem jest Stowarzyszenie – dane skopiowane dla bieżącej pracy powinny zostać niezwłocznie po jej zakończeniu usunięte;

3) **dostęp do sieci NGR, serwisów, intranetu, wspólnego dysku, dysku w chmurze itp. zabezpieczany jest hasłem**;

4) **przesyłanie danych w sieci Stowarzyszenia jest szyfrowane**;

5) szyfrowanie połączenia przez Internet za pomocą systemu SSL;

6) w celu korzystania z komputerów podpiętych do systemu Stowarzyszenia lub z programów wykorzystywanych przez NGR 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 NGR „do rąk własnych”, na wydrukowanej kartce, w zamkniętej kopercie lub pocztą e-mail, na podany wcześniej adres przez użytkownika;
   - przy pierwszym logowaniu **system wymusza zmianę hasła**;
   - hasła służące do logowania się do systemu oraz do programów komputerowych służących do obsługi naborów i do oceny wniosków złożonych do NGR w związku z wdrażaniem LSR 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;
     - w przypadku, gdy użytkownik zapomniał hasła, osoba odpowiedzialna za prowadzenie serwisów internetowych, sieci NGR, ustala hasło tymczasowe, z wymuszeniem jego zmiany podczas kolejnego logowania użytkownika;
   - konta nieaktywnych użytkowników (np. byłych pracowników, członków Zarządu NGR, członków Stowarzyszenia) utworzone w systemie Stowarzyszenia lub w serwisach służących do wymiany informacji, dokumentów itp. w ramach NGR, 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);

7) w przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego;

8) na komputerach użytkowników włączone są **wygaszacze ekranu** oraz **automatyczne wylogowanie się** (w przypadku kilkuminutowej nieaktywności użytkownika na komputerze system wymusza ponowne zalogowanie się);

9) **urządzenia należące do sieci NGR 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);

10) **w celu zapewnienia stałej dostępności danych NGR regularnie wykonuje kopie zapasowe** danych osobowych:
    - co najmniej raz na miesiąc sporządzana jest kopia całkowita danych – ręcznie (*albo – rekomendowane*);
    - co najmniej 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/urządzeń, na których na co dzień pracują pracownicy NGR, nie wiązała się z utratą wszystkich danych;
11) **NGR 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

58. W wyniku dokonanej analizy NGR 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).

59. Przypadki zakwalifikowane jako naruszenie lub groźba naruszenia bezpieczeństwa danych osobowych, to w szczególności (w nawiasie – w skali od 1 do 5 – jako pierwszą liczbę zaznaczono prawdopodobieństwo zdarzenia, jako drugą liczbę zaś poziom dotkliwość skutku danego rodzaju zdarzenia, wagę incydentu ustalono poprzez pomnożenie pierwszej wartość przez drugą):

A. 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, 5);

B. zgubienie lub utrata dokumentów Stowarzyszenia, zgubienie nośnika danych, na którym zapisane były dokumenty Stowarzyszenia (2, 2);

C. 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 (2 ,3);

D. upublicznienie loginu lub haseł dostępowych do systemu lub programów, które są wykorzystywane przez Stowarzyszenie do przetwarzania danych (3, 4);

E. awaria sprzętu lub oprogramowania, na skutek której nastąpiła utrata dostępu do danych, ich modyfikacja lub upublicznienie (2, 5);

F. 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) (3, 3);

G. przetwarzanie danych osobowych bez podstawy prawnej (np. bez zgody osoby zainteresowanej) (3, 3);

H. przekazanie osobie trzeciej danych osobowych innego podmiotu (np. w mylnym przekonaniu, że przekazuje się je osobie, której dane dotyczą, bez sprawdzenia tożsamości wnioskującego) (2, 2);

I. 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, 5);

J. włamanie do biura Stowarzyszenia; kradzież dokumentów należących do Stowarzyszenia (1, 5);

K. podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych (2, 4);

L. awaria sprzętu lub oprogramowania wskazująca na umyślne działanie osób trzecich (2, 4);

M. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń (1, 4);

N. utrata dostępu do danych Stowarzyszenia na skutek odmowy świadczenia usług przez podmiot przetwarzający (1, 3);

O. 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) (2, 3);

P. 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, 3);

Q. nieusunięcie kont nieaktywnych użytkowników, którzy powinni byli utracić dostęp do systemu (2, 4);

R. utrata danych osobowych w wyniku wykonywania niepełnych kopii zapasowych danych (2, 3);

S. utrata danych spowodowana niemożnością odtworzenia danych z kopii zapasowej (1, 4).

T. zgubienie nośników, na których przetwarzane są dane osobowe (np. pendrive) (3, 2).

60. Zdarzenia wymienione w pkt 59 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.

61. 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.

1	6 **C, G, O, P, R, T**	11	16	21
2	7	12 **D**	17	22
3 **N**	8 **K, L, M, Q**	13	18	23
4 **B, H, S**	9 **F, G**	14	19	24
5 **A, I, J**	10 **E**	15	20	24

LEGENDA:

Zagrożenie minimalne	Zagrożenie niewielkie
Zagrożenie dopuszczalne	Zagrożenie znaczące
Bardzo duże zagrożenie	Zagrożenie niedopuszczalne

62. W celu ograniczenia możliwości wystąpienia zdarzeń wiążących się z zagrożeniem bezpieczeństwa danych osobowych, których prawdopodobieństwo wystąpienia jest największe, NGR 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).

Procedura reagowania na naruszenia ochrony danych osobowych

63. W przypadku wystąpienia zdarzeń określonych w pkt 59 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 też 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;

64. 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 zostać dokonane na formularzu opublikowanym przez PUODO.

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.

Zarząd, w celu weryfikacji, czy doszło do naruszenia danych osobowych lub ustalenia rozmiarów i charakteru tego naruszenia, może skorzystać z usług wyspecjalizowanego podmiotu, w szczególności jeżeli do naruszenia doszło w obszarze IT. Z podmiotem takim zawierana jest umowa w formie pisemnej, zawierająca klauzulę poufności oraz klauzulę powierzenia danych.

W razie uprawdopodobnienia, że mogło dojść do naruszenia danych osobowych, Zarząd niezwłocznie podejmuje działania mające na celu ograniczenie skutków naruszenia (np. zablokowanie systemów, zmiana haseł, odebranie uprawnień).

65. Jeżeli **naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, NGR 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 dokonywane jest drogą elektroniczną oraz telefonicznie, chyba że Stowarzyszenie nie dysponuje adresem e-mail danej osoby lub numerem telefonu – wówczas dokonuje zawiadomienia tym środkiem komunikacji, który gwarantuje najszybszą możliwość przekazania komunikatu do odbiorcy.

Zawiadomienie osoby, której dane dotyczą nie jest konieczne, jeżeli

- NGR 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;
- NGR, 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 NGR wydaje na swojej stronie publiczny komunikat o naruszeniu.

66. 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 9 do Polityki**.

67. **Opisane w poprzednich punktach postępowanie stosuje się również w sytuacji, gdy o naruszeniu ochrony danych osobowych, których administratorem jest NGR (lub o podejrzeniu takiego naruszenia) poinformuje podmiot przetwarzający** (np. księgowa, dostawca określonych usług w Internecie).

68. Na podstawie dokonanego wpisu do Rejestru naruszeń, pracownik, o którym mowa w pkt 26 Polityki (a w razie jego niepowołania – Zarząd), przygotowuje rekomendację mającą na celu zmniejszenie prawdopodobieństwa i dolegliwości podobnych naruszeń w przyszłości.

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;

69. Na podstawie dokonanego wpisu do Rejestru naruszeń, pracownik, o którym mowa w pkt 26 Polityki (a w razie jego niepowołania – Zarząd), przygotowuje rekomendację mającą na celu zmniejszenie prawdopodobieństwa i dolegliwości podobnych naruszeń w przyszłości.

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;
- dokonuje przeglądu funkcjonujących procedur i zabezpieczeń i w razie potrzeby podejmuje działania, by podobne zdarzenia nie zdarzyły się w przyszłości (działania minimalizujące ryzyko wystąpienia podobnych naruszeń).

Plan ciągłości działania i procedury odtwarzania systemu po awarii, oraz ich testowanie

70. W przypadku zdarzeń polegających na:

1) awarii systemu informatycznego Stowarzyszenia lub awarii programu, na którym zapisane były dane osobowe przetwarzane przez Stowarzyszenie;
2) fizycznej utraty dokumentów zawierających dane osobowe na skutek kradzieży, włamania, zniszczenia, zgubienia, itp.;
3) awarii serwera, na którym zapisane były dane osobowe
4) uzyskaniu informacji od dostawców usług, które wykorzystuje Stowarzyszenie do przetwarzania danych osobowych, o naruszeniu w ich systemach zabezpieczeń danych osobowych, o incydentach bezpieczeństwa (np. wyciek danych u dostawcy programu wykorzystywanego przez NGR do oceny wniosków).

– adresat Polityki, który to stwierdził zawiadamia o tym zdarzeniu pracownika, o którym mowa w pkt 26 Polityki, lub któregokolwiek z członków Zarządu.

Pracownik, o którym mowa w pkt 26 Polityki, lub członek Zarządu informacji uruchamia w razie potrzeby i po ewentualnym skonsultowanie tego faktu z podmiotem zapewniającym informatyczną obsługę Stowarzyszenia, najbardziej aktualną kopię zapasową utraconych danych.

71. Pierwsze uruchomienie ma charakter próbny – pracownik, o którym mowa w pkt 26 Polityki, lub członek Zarządu, wraz z podmiotem zapewniającym informatyczną obsługę Stowarzyszenia, uruchamiając dany program lub plik, weryfikuje, czy ostatnia kopia zapasowa jest kompletna i aktualna, działa prawidłowo.

72. W przypadku gdy próbne uruchomienie programu lub pliku się powiedzie (nie wystąpią żadne błędy, nieścisłości itp., nieprzewidywane braki lub sprzeczności w danych osobowych) pracownik, o którym mowa w pkt 26 Polityki, lub członek Zarządu uruchamia na stałe kopię zapasową utraconych danych.

73. Jeżeli brak jest adekwatnej kopii zapasowej utraconych danych, uruchomienie kopii zapasowej napotkało poważne błędy lub przeszkody Stowarzyszenie zawiadamia o tym fakcie PUODO oraz rozważa zawiadomienie osób, których dane osobowe są objęte wskazanym problemem. Następnie Stowarzyszenie, na podstawie dostępnych środków i danych (innych nośników, dokumentów, itp.), podejmują działania pozwalające przywrócić w jak największym stopniu utracone dane.

Wykaz załączników:

1) Załącznik nr 1 – Rejestr czynności przetwarzania;
2) Załącznik nr 2 – Rejestr kategorii czynności przetwarzania;
3) Załącznik nr 3 – Szablon analizy ryzyka;
4) Załącznik nr 4 – Wzór upoważnienia;
5) Załącznik nr 5 – Rejestr upoważnień;
6) Załącznik nr 6 – Wzór umowy powierzenia danych osobowych;
7) Załącznik nr 7 – Zasady korzystania z poczty elektronicznej NGR
8) Załącznik nr 8 – Zasady korzystania przez pracowników z komputerów służbowych;
9) Załącznik nr 9 – Rejestr naruszeń ochrony danych osobowych.