

POLITYKA OCHRONY DANYCH OSOBOWYCH

- Gdańskie Stowarzyszenie Alliance Française w Gdańsku 80-227, ul. Sienkiewicza 5/3, wpisane do rejestru przedsiębiorców i rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, prowadzonych przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy KRS, pod numerem KRS: 0000229953, NIP: 525-23-52-899, REGON: 140088489

1. PODSTAWA PRAWNA

Niniejsza „Polityka” jest polityką ochrony danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L 119), dalej zwanego RODO.

2. CEL OPRACOWANIA DOKUMENTU

Celem opracowania niniejszego dokumentu jest wytyczenie zasad i wymagań w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez Gdańskie Stowarzyszenie Alliance Française w Gdańsku 80-227, ul. Sienkiewicza 5/3, wpisane do rejestru przedsiębiorców i rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, prowadzonych przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy KRS, pod numerem KRS: 0000229953, NIP: 525-23-52-899, REGON: 140088489, zwane dalej również jako „**Stowarzyszenie**”, biorąc pod uwagę, że w Stowarzyszeniu nie został powołany inspektor ochrony danych osobowych i Stowarzyszenie nie jest zobowiązane do prowadzenia rejestru czynności przetwarzania danych osobowych. Ponadto, celem niniejszej Polityki jest ochrona danych osobowych, przetwarzanych przez Stowarzyszenie, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem. Wypracowane zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji systemów informatycznych, na poziomie odpowiadającym potrzebom Spółki.

3. ZAKRES POLITYKI

Polityka zawiera:

- a. opis zasad ochrony danych osobowych obowiązujących w Stowarzyszeniu;
- b. odwołania do załączników zawierających:

Załącznik nr 1: wzór umowy o powierzenie przetwarzania danych osobowych

Załącznik nr 2: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),

Załącznik nr 3: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych,

Załącznik nr 4: ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5: wzór upoważnienia do przetwarzania danych osobowych

Wskazane Załączniki stanowią integralną część Polityki.

4. DEFINICJE

1. **Administrator danych** – Gdańskie Stowarzyszenie Alliance Française w Gdańsku 80-227, ul. Sienkiewicza 5/3, wpisane do rejestru przedsiębiorców i rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, prowadzonych przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy KRS, pod numerem KRS: 0000229953, NIP: 525-23-52-899, REGON: 140088489 (również jako: Stowarzyszenie”),
2. **Dane dzieci** – oznaczają dane osób poniżej 16 roku życia;
3. **Dane karne** – dane, o których stanowi art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń;
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne);
5. **Dane wrażliwe** – dane, o których stanowi art. 9 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, podglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
6. **Eksport danych osobowych** – oznacza przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
7. **Informatyczne nośniki danych** – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,
8. **Instrukcja Zarządzania Systemem Informatycznym** - dokument wewnętrzny wydany przez Stowarzyszenie.
9. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
10. **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
11. **Podmiot przetwarzający** – oznacza organizację lub osobę, której Stowarzyszenie powierzyło przetwarzanie danych osobowych (np. zewnętrzna księgowość),

12. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
13. **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowotnej, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
14. **Przetwarzający** – oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych;
15. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, w szczególności takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych,

5. STOSOWANIE POLITYKI

1. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Stowarzyszenia.
2. Zobowiązani do stosowania niniejszej Polityki jest Stowarzyszenie, członkowie Stowarzyszenia i wszyscy członkowie personelu Stowarzyszenia.
3. Spółka jest zobowiązana do zapewnienia zgodności postępowania kontrahentów Stowarzyszenia z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Stowarzyszenie.

6. ZASADY OGÓLNE OCHRONY DANYCH OSOBOWYCH

1. Stowarzyszenie dba o ochronę prywatności i przetwarza dane osobowe zgodnie z prawem.
2. Stowarzyszenie zapewnia odpowiedni poziom bezpieczeństwa danych osobowych, podejmując stałe działania w tym zakresie.
3. Stowarzyszenie umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. Stowarzyszenie dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
5. Stowarzyszenie przetwarza dane osobowe z poszanowaniem następujących zasad:
 - a. w oparciu o podstawę prawną i zgodnie z prawem;
 - b. rzetelnie i uczciwie;
 - c. w sposób przejrzysty dla osoby, której dane dotyczą;
 - d. w konkretnych celach, w minimalnym zakresie;
 - e. w zakresie adekwatnym do potrzeb;
 - f. z dbałością o prawidłowość danych;

- g. przez czas adekwatny do potrzeb;
- h. zapewniając odpowiednie bezpieczeństwo.

7. SYSTEM OCHRONY DANYCH OSOBOWYCH

Na system ochrony danych osobowych w Stowarzyszeniu składają się następujące elementy:

1. **Inwentaryzacja danych osobowych** polegająca na identyfikacji zasobów danych osobowych, rodzajów danych osobowych, zależności między zasobami danych osobowych, identyfikacji sposobów wykorzystania danych osobowych, w tym:
 - a. przypadków przetwarzania danych wrażliwych i danych karnych;
 - b. przypadków przetwarzania danych osób, których Stowarzyszenie nie identyfikuje;
 - c. przypadków przetwarzania danych dzieci;
 - d. profilowania
 - e. współadministrowania danymi;
2. **Identyfikacja i weryfikacja podstaw prawnych przetwarzania danych osobowych**, w tym:
 - a. utrzymanie systemu zarządzania zgodami na przetwarzanie danych osobowych i komunikację na odległość;
 - b. inwentaryzacja i uszczegóławianie uzasadnienie przypadków, gdy Stowarzyszenie przetwarza dane na podstawie prawnie uzasadnionego interesu Stowarzyszenia.
3. **Wykonywanie obowiązku informacyjnego** względem osób, których dane Stowarzyszenie przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - a. przekazuje osobom fizycznym wymagane informacje przy zbieraniu danych i w innych sytuacjach dotyczące przetwarzania ich danych osobowych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
 - b. weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
 - c. zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i udokumentowane;
 - d. stosuje procedury pozwalające na wykonanie obowiązku zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem przy przetwarzaniu danych osobowych;
4. **Ustanowione zasady i metody zarządzania minimalizacją (*privacy by default*)**, a w tym:
 - a. zasady zarządzania adekwatnością danych;
 - b. zasady reglamentacji i zarządzania dostępem do danych;
 - c. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.
5. **Odpowiedni poziom bezpieczeństwa danych**, w tym:
 - a. przeprowadzane analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - b. dostosowanie środków ochrony danych do ustalonego ryzyka;

- c. posiadanie systemu zarządzania bezpieczeństwem informacji;
- d. stosowanie procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia w ochronie danych osobowych Urzędowi Ochrony Danych Osobowych-zarządza incydentami.
- 6. **Zasady doboru przetwarzających dane osobowe na rzecz Stowarzyszenia**, wymogów co do warunków przetwarzania (umowa powierzenia przetwarzania danych osobowych), zasad weryfikacji wykonywania umów powierzenia przetwarzania danych osobowych.
- 7. **Zasady weryfikacji czy Stowarzyszenie nie przekazuje danych do państw trzecich lub do organizacji międzynarodowych** oraz zapewnienia zgodnych z prawem warunków takiego przekazania, jeśli ma ono miejsce (**eksport danych osobowych**);
- 8. **Zarządzanie zmianami wpływającymi na prywatność**. W tym celu procedury uruchomienia nowych projektów i inwestycji w Stowarzyszeniu uwzględniają analizę ryzyka, zapewnienie prywatności (zgodność celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu (*privacy by design*);
- 9. **Zasady weryfikacji kiedy zachodzą przypadki przetwarzania transgranicznego** oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

8. INWENTARYZACJA DANYCH OSOBOWYCH

- 1. Stowarzyszenie identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe lub dane karne oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania sytuacji przetwarzania danych wrażliwych lub danych karnych Stowarzyszenie postępuje zgodnie z przyjętymi zasadami w tym zakresie.
- 2. Stowarzyszenie identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
- 3. Stowarzyszenie identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Stowarzyszenie postępuje zgodnie z przyjętymi zasadami w tym zakresie (**profilowanie**)
- 4. Stowarzyszenie identyfikuje przypadki współadministrowania danymi osobowymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami (**współadministrowanie**)

9. IDENTYFIKACJA I WERYFIKACJA PODSTAW PRAWNYCH PRZETWARZANIA DANYCH OSOBOWYCH

1. Wskazując w dokumentach ogólną podstawę prawną przetwarzania danych osobowych, Stowarzyszenie dookreśla tę podstawę w precyzyjny i zrozumiały sposób, gdy jest to potrzebne.
2. Stowarzyszenie wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych osobowych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
3. przedstawiciele Stowarzyszenia mają obowiązek znać podstawy prawne, na jakich Stowarzyszenie dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Stowarzyszenia, przedstawiciele Stowarzyszenia mają obowiązek znać konkretny realizowany przetwarzaniem interes Stowarzyszenia.

10. WYKONYWANIE OBOWIĄZKU INFORMACYJNEGO

1. Stowarzyszenie określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Stowarzyszenie dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
3. Stowarzyszenie informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. Stowarzyszenie informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. Stowarzyszenie określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym)
6. Stowarzyszenie informuje osobę o planowanej zmianie celu przetwarzania danych.
7. Stowarzyszenie informuje osobę przed uchycieniem ograniczenia przetwarzania.
8. Stowarzyszenie informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. Stowarzyszenie informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10. Stowarzyszenie bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
11. Stowarzyszenie ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Stowarzyszenia informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Stowarzyszeniu, w tym

wymaganiach dotyczących identyfikacji, metodach kontaktu ze Stowarzyszeniem w tym celu.

12. Stowarzyszenie dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane są przetwarzane.
13. Stowarzyszenie informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
14. Stowarzyszenie wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
15. W celu realizacji praw jednostki Stowarzyszenie zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Stowarzyszenie, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany;
16. Stowarzyszenie dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. ROZPATRYWANIE ŻĄDAŃ OSÓB

1. Realizując prawa osób, których dane dotyczą, Stowarzyszenie wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Stowarzyszenie może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. Stowarzyszenie informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. Stowarzyszenie informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Na żądanie osoby dotyczące dostępu do jej danych Stowarzyszenie informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Stowarzyszenia nie uzna za pierwszą, nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. Na żądanie **Stowarzyszenie wydaje osobie kopię danych** jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Stowarzyszenie wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

6. **Stowarzyszenie dokonuje sprostowania nieprawidłowych danych na żądanie osoby.** Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. **Stowarzyszenie uzupełnia i aktualizuje dane na żądanie osoby.** Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Spółka może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Stowarzyszenie procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Na żądanie osoby **Stowarzyszenie usuwa dane**, gdy:
 - a. dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
 - b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
 - c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
 - d. dane były przetwarzane niezgodnie z prawem, a konieczność usunięcia wynika z obowiązku prawnego,
 - e. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).
9. Stowarzyszenie określa metodę obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
10. Jeżeli dane podlegające usunięciu zostały upublicznione przez Stowarzyszenie, Stowarzyszenie podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.
11. W przypadku usunięcia danych Stowarzyszenie informuje osobę o odbiorcach danych, na żądanie tej osoby.
12. **Stowarzyszenie dokonuje ograniczenia przetwarzania danych na żądanie osoby**, gdy:
 - a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
 - b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
 - c. Stowarzyszenie nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

- d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Stowarzyszenia zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
- 13. W trakcie ograniczenia przetwarzania Stowarzyszenie przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
- 14. Stowarzyszenie informuje osobę przed uchyleniem ograniczenia przetwarzania.
- 15. W przypadku ograniczenia przetwarzania danych Stowarzyszenie informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 16. Na żądanie osoby Stowarzyszenie wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Stowarzyszeniu, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Stowarzyszenia.
- 17. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją **sprzeciw** względem przetwarzania jej danych, a dane przetwarzane są przez Stowarzyszenie w oparciu o uzasadniony interes Stowarzyszenia lub o powierzone Stowarzyszeniu zadanie w interesie publicznym, Stowarzyszenie uwzględni sprzeciw, o ile nie zachodzą po stronie Stowarzyszenia ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
- 18. Jeżeli Stowarzyszenie prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Stowarzyszenie uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
- 19. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Stowarzyszenie na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Stowarzyszenie uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
- 20. Jeżeli Stowarzyszenie przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Stowarzyszenie zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Stowarzyszenia, chyba że taka automatyczna decyzja:
 - a. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Stowarzyszeniem, lub
 - b. jest wprost dozwolona przepisami prawa, lub
 - c. opiera się na wyraźnej zgodzie odwołującej osoby.

12. ZASADY I METODY ZARZĄDZANIA MINIMALIZACJĄ (*PRIVACY BY DEFAULT*)

1. Stowarzyszenie dba o minimalizację przetwarzania danych pod kątem adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.
2. Stowarzyszenie zweryfikowało zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
3. Stowarzyszenie dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na trzy lata. Stowarzyszenie przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).
4. Stowarzyszenie stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
5. Stowarzyszenie stosuje kontrolę dostępu fizycznego.
6. Stowarzyszenie dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
7. Stowarzyszenie dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
8. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym.
9. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych Stowarzyszenia, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Stowarzyszenie. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

1. Stowarzyszenie zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Stowarzyszenie.
2. Stowarzyszenie przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
 - a. Stowarzyszenie zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji i ciągłości

Działania wewnątrznie lub ze wsparciem podmiotów wyspecjalizowanych;

b. Stowarzyszenie kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

3. Stowarzyszenie przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych

dla czynności przetwarzania danych lub ich kategorii. Stowarzyszenie analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

4. Stowarzyszenie stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Stowarzyszeniu i są bliżej opisane w procedurach przyjętych przez Stowarzyszenie dla tych obszarów.

5. Stowarzyszenie stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

6. Stowarzyszenie ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Stowarzyszenie ustala przydatność i stosuje takie środki i podejście, jak:

- a. pseudonimizacja,
- b. szyfrowanie danych osobowych,
- c. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

7. W ramach zabezpieczenia danych osobowych ochronie podlegają:

- a. sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne,
- b. oprogramowanie,
- c. dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
- d. hasła użytkowników,
- e. bazy danych i kopie zapasowe,
- f. wydruki,
- g. związana z przetwarzaniem danych dokumentacja papierowa.

8. Do elementów zabezpieczenia danych osobowych przez Spółkę zalicza się:

- a. stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (**zabezpieczenia fizyczne**),
 - b. odpowiednie środki zabezpieczenia danych w systemach informatycznych (**zabezpieczenia techniczne**),
 - c. nadzór administratora danych nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (**zabezpieczenie organizacyjne**),
 - d. **bezpieczeństwo osobowe.**
9. **Zabezpieczenia fizyczne** obejmują:
- a. wydzielenie obszaru przetwarzania danych,
 - b. dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęty jest systemem kontroli dostępu,
 - c. samodzielny dostęp do pomieszczeń jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności osób upoważnionych,
 - d. przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,
 - e. kopie zapasowe zbioru danych osobowych przechowywane są w sejfie w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
10. **Zabezpieczenia techniczne** obejmują:
- a. zastosowanie mechanizmów kontroli dostępu do systemów informatycznych i ich zasobów - uprawnienia są różne dla różnych grup użytkowników,
 - b. odpowiednie i regularne aktualizowanie narzędzi ochronnych, w tym oprogramowanie antywirusowe, które jest regularnie aktualizowane,
 - c. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
 - e. tworzenie regularnych kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych oraz kopie programów służących do przetwarzania danych osobowych,
 - f. zastosowanie zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (listwy przeciwzakłóceńowe),
11. **Zabezpieczenia organizacyjne** to:
- a. osobą odpowiedzialną za bezpieczeństwo danych osobowych jest administrator danych;
 - b. pracownicy Stowarzyszenia, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują administratora danych lub wyznaczoną przez niego osobę;
 - c. osoby upoważnione do przetwarzania danych osobowych mające dostęp do danych osobowych, które są w dyspozycji Stowarzyszenia zobowiązane są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z

określonego stanowiska, a także po ustaniu zatrudnienia; w tym celu osoby te podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia,

- d. przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych;
 - e. osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku. Określone stanowiska wraz z przypisanym zakresem upoważnienia znajdują się w ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowiącej załącznik 4 do niniejszej Polityki.
12. Zabezpieczenie osobowe polegają na:
- a. stosowaniu klauzul o zachowaniu poufności danych osobowych w umowach o pracę oraz w umowach ze zleceniobiorcami, z którymi związane jest przetwarzanie danych osobowych;
 - b. wprowadzaniu obowiązku raportowania do administratora danych wszelkich naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania.

14. ZASADY DOBORU PRZETWARZAJĄCYCH DANE OSOBOWE

- 1. Stowarzyszenie posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Stowarzyszenia opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Stowarzyszeniu.
- 2. Stowarzyszenie przyjęło minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 1 do Polityki – „Wzór umowy powierzenia przetwarzania danych”.
- 3. Stowarzyszenia rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia przetwarzania danych osobowych.

15. EKSPORT DANYCH OSOBOWYCH

Aby uniknąć sytuacji nieautoryzowanego eksportu danych osobowych, w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Stowarzyszenie okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

16. ZARZĄDZANIE ZMIANAMI WPLYWAJĄCYMI NA PRYWATNOŚĆ

Stowarzyszenie zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz

minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Stowarzyszenie odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

17. POSTANOWIENIA KOŃCOWE

1. Niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.). Wybrane jego elementy mogą zostać udostępnione innym podmiotom po zawarciu stosownej umowy o zachowaniu poufności.
2. Za zarządzanie dokumentem Polityki, w tym jego rozpowszechnianiem, aktualizacją, utrzymywaniem spójności z innymi dokumentami, jest odpowiedzialny administrator danych.
3. Z treścią niniejszego dokumentu powinny zostać zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z racji wykonywanych obowiązków i czynności mają dostęp do danych osobowych.

Załącznik nr: wzór umowy o powierzenie przetwarzania danych osobowych

Załącznik nr 2: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych)

L p.	Lokalizacja – adres i numer budynku	Numer pomieszczenia/ przeznaczenie	Uwagi
-----------------	--	---	--------------

1	Sienkiewicza ul. 5/3, 80-227,Gdańsk		
2			
3			

Załącznik nr 3: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych,

Załącznik nr 4: Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko	Imię	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik nr 5: wzór upoważnienia do przetwarzania danych osobowych