

POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **STOWARZYSZENIU PROMOCJI BEZPIECZEŃSTWA PRACY w TARNOBRZEGU** z adresem: ul. Wyspiańskiego 12, 39-400 Tarnobrzeg (dalej jako **Stowarzyszenie**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

2. Polityka zawiera:
 - a) opis zasad ochrony danych obowiązujących w Stowarzyszeniu;
 - b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);
3. Odpowiedzialny
 - za wdrożenie i utrzymanie niniejszej Polityki jest:
 - (i) Prezes Zarządu Stowarzyszenia;
 - za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
 - (ii) wszyscy członkowie Zarządu Stowarzyszenia.

W Stowarzyszeniu, na podstawie art. 37 RODO nie został powołany Inspektor Ochrony Danych Osobowych. Stowarzyszenie dąży także do zapewnienia zgodności postępowania kontrahentów Stowarzyszenia z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Stowarzyszenie.

4. **Skróty i definicje:**

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane wrażliwe oznaczają dane specjalne i dane karne.

Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy 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.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający oznacza organizację lub osobę, której Stowarzyszenie powierzyło przetwarzanie danych osobowych.

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu 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, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Stowarzyszenie oznacza Stowarzyszenie Promocji Bezpieczeństwa Pracy w Tarnobrzegu KRS:45796

5. Ochrona danych osobowych w Stowarzyszeniu – zasady ogólne

5.1. Filary ochrony danych osobowych w Stowarzyszeniu:

- (1) **Legalność** – Stowarzyszenie dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
- (2) **Bezpieczeństwo** – Stowarzyszenie zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
- (3) **Prawa Jednostki** – Stowarzyszenie umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- (4) **Rozliczalność** – Stowarzyszenie dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych

Stowarzyszenie przetwarza dane osobowe z poszanowaniem następujących zasad:

- (1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- (2) rzetelnie i uczciwie (rzetelność);
- (3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- (4) w konkretnych celach i nie „na zapas” (minimalizacja);
- (5) nie więcej niż potrzeba (adekwatność);
- (6) z dbałością o prawidłowość danych (prawidłowość);
- (7) nie dłużej niż potrzeba (czasowość);
- (8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3. System ochrony danych

System ochrony danych osobowych w Stowarzyszeniu składa się z następujących elementów:

- 1) **Rejestr.** Stowarzyszenie opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Stowarzyszeniu (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Firmie.
- 2) **Podstawy prawne.** Stowarzyszenie zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
 - a) utrzymuje system zarządzania zgodami na przetwarzanie danych,
 - b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Stowarzyszenie przetwarza dane na podstawie prawnie uzasadnionego interesu Firmy.
- 3) **Obsługa praw jednostki.** Stowarzyszenie spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - a) **Obowiązki informacyjne.** Stowarzyszenie przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
 - b) **Możliwość wykonania żądań.** Stowarzyszenie weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
 - c) **Obsługa żądań.** Stowarzyszenie zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
 - d) **Zawiadamianie o naruszeniach.** Stowarzyszenie stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

- 4) **Minimalizacja.** Stowarzyszenie posiada 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) **Bezpieczeństwo.** Stowarzyszenie zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
 - a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
 - c) dostosowuje środki ochrony danych do ustalonego ryzyka;
- 6) **Przetwarzający.** Stowarzyszenie dobiera podmioty przetwarzające dane na rzecz Stowarzyszenia, pod kątem spełniania przez nie wymogów co do warunków przetwarzania (umowa powierzenia);
- 7) **Eksport danych.** Stowarzyszenie weryfikuje, czy Stowarzyszenie nie przekazuje danych do państw trzecich (poza UE, GB, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych, a jeżeli ma ono miejsce zapewnia zgodne z prawem warunki takiego przekazywania.
- 8) **Privacy by design.** Stowarzyszenie zarządza zmianami mającymi wpływ na prywatność. W tym celu uruchamiając nowe projekty i inwestycje w Stowarzyszeniu uwzględnia się konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
- 9) **Przetwarzanie transgraniczne.** Stowarzyszenie weryfikuje czy zachodzą przypadki przetwarzania transgranicznego oraz, w razie zidentyfikowania takiego stanu, ustala wiodący organ nadzorczy i głównej jednostki organizacyjne w rozumieniu RODO.
- 10) **Rejestr upoważnień.** Stowarzyszenie zapewnia przetwarzanie danych osobowych, którymi administruje wyłącznie przez osoby do tego upoważnione. **Załącznik nr 7 do Polityki – „Wzór upoważnienia do przetwarzania danych”**. Dla zapewnienia przejrzystości Stowarzyszenie prowadzi rejestr upoważnień, w którym uwzględnia udzielone i odwołane upoważnienia. **Załącznik nr 8 do Polityki – „Wzór rejestru upoważnień”**.

6. Inwentaryzacja

6.1. Dane wrażliwe

Stowarzyszenie nie przetwarza danych szczególnych kategorii.

6.2. Dane niezidentyfikowane

Stowarzyszenie monitoruje sytuacje, w których może przetwarzać dane niezidentyfikowane.

6.3. Profilowanie

Stowarzyszenie nie profiluje danych osobowych.

6.4. Współadministrowanie

Stowarzyszenie monitoruje potencjalne sytuacje współadministrowania danymi i w razie zidentyfikowania takiego przypadku podejmuje niezbędne działania określone w art. 26 RODO.

7. Rejestr Czynności Przetwarzania Danych

7.1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2. Stowarzyszenie prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

- 7.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Stowarzyszeniu rozliczanie większości obowiązków ochrony danych.
- 7.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Stowarzyszenie uznała za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Stowarzyszenia, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.
- 7.5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”**. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Stowarzyszenie rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

8. Podstawy przetwarzania

- 8.1. Stowarzyszenie dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- 8.2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, uzasadniony cel Stowarzyszenia) Stowarzyszenie dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.
- 8.3. Stowarzyszenie wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
- 8.4. Personel Stowarzyszenia ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Stowarzyszenia, członek personelu ma obowiązek znać konkretny realizowany w związku z przetwarzaniem interes Stowarzyszenia.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

- 9.1. Stowarzyszenie dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
- 9.2. 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.
- 9.3. Stowarzyszenie dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
- 9.4. Stowarzyszenie wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- 9.5. Stowarzyszenie dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. Obowiązki informacyjne

- 10.1. Stowarzyszenie informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

- 10.2. Stowarzyszenie informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- 10.3. Stowarzyszenie informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej (informowanie może następować za pośrednictwem innych osób) oraz o przysługujących jej prawach.
- 10.4. Stowarzyszenie informuje osoby o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym - o ile dotyczy).
- 10.5. Stowarzyszenie bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

11. Żądania osób

- 11.1. **Prawa osób trzecich.** 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 itp.), Stowarzyszenie może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
- 11.2. **Nieprzetwarzanie.** Stowarzyszenie informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
- 11.3. **Odmowa.** Stowarzyszenie informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
- 11.4. **Dostęp do danych.** 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 (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), 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 Stowarzyszenie nie uznaje za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
- 11.5. **Kopie danych.** 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 w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
- 11.6. **Sprostowanie danych.** Stowarzyszenie dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Stowarzyszenie ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Stowarzyszenie informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 11.7. **Uzupełnienie danych.** Stowarzyszenie uzupełnia i aktualizuje dane na żądanie osoby. Stowarzyszenie ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Stowarzyszenie nie musi przetwarzać danych, które są Stowarzyszeniu zbędne). Stowarzyszenie może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Firmę procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8. Usunięcie danych. Na żądanie osoby, Stowarzyszenie usuwa dane, gdy:

- (1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
- (2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
- (3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- (4) dane były przetwarzane niezgodnie z prawem,
- (5) konieczność usunięcia wynika z obowiązku prawnego,

Stowarzyszenie zapewnia efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikuje, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

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.

W przypadku usunięcia danych Stowarzyszenie informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania. 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.

W trakcie ograniczenia przetwarzania Stowarzyszenie przechowuje dane, natomiast nie przetwarza ich w inny sposób (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.

Stowarzyszenie informuje osobę przed uchynieniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Stowarzyszenie informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10. Przenoszenie danych. 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 Firmy.

11.11. Sprzeciw w szczególnej sytuacji. 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.

11.12. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. 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.

11.13. Sprzeciw względem marketingu bezpośredniego. 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.

11.14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. 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 (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Stowarzyszenie; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

12. MINIMALIZACJA

Stowarzyszenie dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

12.1. Minimalizacja zakresu

Stowarzyszenie zweryfikowało zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Stowarzyszenie dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Stowarzyszenie przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2. Minimalizacja dostępu

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).

Stowarzyszenie stosuje kontrolę dostępu fizycznego.

Stowarzyszenie dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

Stowarzyszenie dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

12.3. Minimalizacja czasu

Stowarzyszenie systematycznie weryfikuje dalszą przydatność danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów biznesowych Stowarzyszenia. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Stowarzyszenie. Archiwizacja i korzystanie z archiwów, tworzenie i wykorzystanie kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

Stowarzyszenie zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Stowarzyszenie.

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

Stowarzyszenie przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

- (1) Stowarzyszenie zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych.
- (2) 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 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:
 - (i) politykę czystego biurka
 - (ii) korzystanie w korespondencji mailowej wyłącznie z poczty elektronicznej oznaczonej własną domeną „.....@spbp.tarnobrzeg.pl.”
 - (iii) środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 - (iv) środki zapewnienia ciągłości działania i zapobiegania skutkom naruszeń, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

13.2. Oceny skutków dla ochrony danych

Stowarzyszenie dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie (o ile takie stwierdzono).

13.3. Środki bezpieczeństwa

Stowarzyszenie stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

13.4. Zgłaszanie naruszeń

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

14. PRZETWARZAJĄCY

Stowarzyszenie dokonuje weryfikacji przetwarzających dane na rzecz Stowarzyszenia 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.

Stowarzyszenie przyjęło minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**.

15. EKSPORT DANYCH

Stowarzyszenie nie dokonuje eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

16. PROJEKTOWANIE PRYWATNOŚCI

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

17. PROCEDURY

17.1. Obowiązki informacyjne

W przypadku gdy przetwarzanie danych wymaga zgody osoby, członek personelu prosi osobę o udzielenie takiej zgody - **Załącznik nr 3 do Polityki – „Wzór –zgoda”**.

Uzyskanie zgody/odmowa udzielenia zgody odnotowywana jest w rejestrze; **Załącznik nr 4 do Polityki – „Wzór rejestru zgód”**.

Członek personelu przy pierwszym kontakcie Stowarzyszenia z osobą, której dane zbiera realizuje obowiązek informacyjny, przekazując jej niezbędne informacje, o których mowa w art. 13 ust. 1 i ust. 2 RODO; wzór informacji stanowi **Załącznik nr 5 do Polityki – „Wzór zawiadomienia osoby – zbieranie danych od osoby, której dane dotyczą”**.

W przypadku gdy dane zbierane są od innej osoby, niż od osoby której dotyczą, członek personelu, który zbiera dane realizuje obowiązek informacyjny wobec osoby, której dane dotyczą i przekazuje jej informacja, o których mowa w art. 14 ust. 1 i ust. 2 RODO; wzór informacji stanowi **Załącznik nr 6 do Polityki – „Wzór zawiadomienia osoby – zbieranie danych w inny sposób niż od osoby, której dane dotyczą”**, chyba że administrator uzyskał potwierdzenie, że osoba której dane dotyczą została poinformowana w odpowiednim zakresie o przetwarzaniu jej danych przez Stowarzyszenie.

17.2. Obsługa żądań

Członek personelu Stowarzyszenia, który otrzymał od osoby żądanie dotyczące danych osobowych, które mogą być przetwarzane w Stowarzyszeniu, niezwłocznie (najpóźniej dnia następnego) informuje o tym Prezesa Zarządu w formie pisemnej lub elektronicznej na adres: biuro@spbp.tarnobrzeg.pl przekazując żądanie.

17.3. Zawiadamianie o naruszeniach

W przypadku zidentyfikowania naruszenia ochrony danych osobowych *lub uzasadnionego podejrzenia naruszenia*, członek personelu, który takie naruszenie lub *podejrzenie* zidentyfikował zobowiązany jest do niezwłocznego (nie później niż w ciągu 1 godziny od zidentyfikowania naruszenia *lub uzasadnionego podejrzenia naruszenia*), poinformowania o tym Zarządu telefonicznie oraz w formie elektronicznej na adres: biuro@spbp.tarnobrzeg.pl podając podstawowe informacje.

Prezes Zarządu analizuje informacje oraz, w razie konieczności, realizuje zawiadomienia właściwego organu nadzorczego oraz osoby dotkniętej zidentyfikowanym naruszeniem danych – zgodnie z art. 33 i art. 34 RODO.

17.4. Inwentaryzacja

Członek personelu, który zidentyfikował w systemie Stowarzyszenia dane (poza zakresem przetwarzanym w Stowarzyszeniu w oparciu o uzyskane zgody lub na podstawie obowiązujących regulacji prawnych) lub niezidentyfikowane zobowiązany jest do niezwłocznego (nie później niż dnia następnego) powiadomienia Prezesa Zarządu w formie elektronicznej na adres: biuro@spbp.tarnobrzeg.pl , przekazując podstawowe informacje.

18. POSTANOWIENIA KOŃCOWE

Polityka w powyższej treści obowiązuje od dnia 1 stycznia 2024 roku

Zarząd Stowarzyszenia: