

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 Aktywności Lokalnej „Dolina Kacanki”. (dalej jako **Organizacja**).
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 Organizacji;
- 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 Zarząd Organizacji, a w ramach Zarządu:

- a) Członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych;
- b) osoba wyznaczona przez Zarząd do zapewnienia zgodności z ochroną danych osobowych; za nadzór i monitorowanie przestrzegania Polityki odpowiadają;
- c) Inspektor Ochrony Danych, jeżeli został powołany w Organizacji;
- d) komórka audytu wewnętrznego, jeżeli funkcjonuje w Organizacji; za stosowanie niniejszej Polityki odpowiedzialni są:
- e) Organizacja;
- f) komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;
- g) komórki organizacyjne przetwarzające dane osobowe w dużym rozmiarze;
- h) pozostałe komórki organizacyjne;
- i) wszyscy członkowie personelu Organizacji.

Organizacja powinna też zapewnić zgodność postępowania kontrahentów Organizacji z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Organizację.

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.

Dane dzieci oznaczają dane osób poniżej 16. roku życia.

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

Podmiot przetwarzający oznacza organizację lub osobę, której Organizacja powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

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.

Organizacja oznacza Stowarzyszenie Aktywności Lokalnej „Dolina Kacanki” z siedzibą: Wiązownica Kolonia 90, 28-200 Staszów, KRS 0000464319, NIP 8661734418.

5. OCHRONA DANYCH OSOBOWYCH W ORGANIZACJI – ZASADY OGÓLNE

1.1. Filary ochrony danych osobowych w Organizacji:

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

1.2. Zasady ochrony danych

Organizacja 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).

1.3. System ochrony danych

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

- 1) **Inwentaryzacja danych.** Organizacja dokonuje identyfikacji zasobów danych osobowych w Organizacji, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
 - a) przypadków przetwarzania danych specjalnych i danych „kryminalnych” (**dane wrażliwe**);
 - b) przypadków przetwarzania danych osób, których Organizacja nie identyfikuje (**dane niezidentyfikowane/UFO**);
 - c) przypadków przetwarzania danych dzieci;
 - d) profilowania;
 - e) współadministrowania danymi.
- 2) **Rejestr.** Organizacja opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Organizacji (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Organizacji.
- 3) **Podstawy prawne.** Organizacja zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
 - a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
 - b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Organizacja przetwarza dane na podstawie prawnie uzasadnionego interesu Organizacji.
- 4) **Obsługa praw jednostki.** Organizacja spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - a) **Obowiązki informacyjne.** Organizacja przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
 - b) **Możliwość wykonania żądań.** Organizacja weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
 - c) **Obsługa żądań.** Organizacja zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
 - d) **Zawiadamianie o naruszeniach.** Organizacja stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
- 5) **Minimalizacja.** Organizacja 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.
- 6) **Bezpieczeństwo.** Organizacja 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;
 - d) posiada system zarządzania bezpieczeństwem informacji;
 - e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

- 7) **Przetwarzający.** Organizacja posiada zasady doboru przetwarzających dane na rzecz Organizacji, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
- 8) **Eksport danych.** Organizacja posiada zasady weryfikacji, czy Organizacja nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
- 9) **Privacy by design.** Organizacja zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Organizacji uwzględniają 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.
- 10) **Przetwarzanie transgraniczne.** Organizacja posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. **INWENTARYZACJA**

1.1. **Dane wrażliwe**

Organizacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Organizacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

1.2. **Dane niezidentyfikowane**

Organizacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

1.3. **Profilowanie**

Organizacja 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, Organizacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

1.4. **Współadministrowanie**

Organizacja identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

7. **REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH**

- 1.1. 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.
- 1.2. Organizacja prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
- 1.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Organizacji rozliczanie większości obowiązków ochrony danych.

- 1.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Organizacja uznała za odrębną dla potrzeb Rejestru, Organizacja odnotowuje 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 Organizacji, 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.
- 1.5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”**. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Organizacja 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

- 1.1. Organizacja dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- 1.2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Organizacji) Organizacja 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.
- 1.3. Organizacja 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.).
- 1.4. Kierownik komórki organizacyjnej Organizacji ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Organizacji, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Organizacji.

2. Sposób obsługi praw jednostki i obowiązków informacyjnych

- 2.1. Organizacja dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
- 2.2. Organizacja ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Organizacji informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Organizacji, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Organizacją w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.
- 2.3. Organizacja dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.
- 2.4. Organizacja wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- 2.5. W celu realizacji praw jednostki Organizacja zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Organizację, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
- 2.6. Organizacja dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

3. Obowiązki informacyjne

- 3.1. Organizacja określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

- 3.2. Organizacja informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- 3.3. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- 3.4. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
- 3.5. Organizacja określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
- 3.6. Organizacja informuje osobę o planowanej zmianie celu przetwarzania danych.
- 3.7. Organizacja informuje osobę przed uchycieniem ograniczenia przetwarzania.
- 3.8. Organizacja informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- 3.9. Organizacja informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- 3.10. Organizacja bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

4. **Żądania osób**

- 4.1. **Prawa osób trzecich.** Realizując prawa osób, których dane dotyczą, Organizacja 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.), Organizacja może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
- 4.2. **Nieprzetwarzanie.** Organizacja informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
- 4.3. **Odmowa.** Organizacja informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
- 4.4. **Dostęp do danych.** Na żądanie osoby dotyczące dostępu do jej danych, Organizacja 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 Organizacja nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
- 4.5. **Kopie danych.** Na żądanie Organizacja wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Organizacja 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.
- 4.6. **Sprostowanie danych.** Organizacja dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Organizacja ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Organizacja informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 4.7. **Uzupełnienie danych.** Organizacja uzupełnia i aktualizuje dane na żądanie osoby. Organizacja ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Organizacja nie musi przetwarzać danych, które są Organizacji zbędne). Organizacja może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to

niewystarczające w świetle przyjętych przez Organizację procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

4.8. **Usunięcie danych.** Na żądanie osoby Organizacja 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,
- (6) 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).

Organizacja określa sposób 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. Jeżeli dane podlegające usunięciu zostały upublicznione przez Organizację, Organizacja 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 Organizacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

4.9. **Ograniczenie przetwarzania.** Organizacja 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) Organizacja 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 Organizacji zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Organizacja 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.

Organizacja informuje osobę przed uchyceniem ograniczenia przetwarzania.

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

4.10. **Przenoszenie danych.** Na żądanie osoby Organizacja 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 Organizacji, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Organizacji.

4.11. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Organizację w oparciu o uzasadniony interes Organizacji lub o powierzone Organizacji zadanie w interesie publicznym, Organizacja **uwzględni** sprzeciw, o ile nie zachodzą po stronie Organizacji ważne prawnie

uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

- 4.12. **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli Organizacja prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Organizacja uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
- 4.13. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Organizację na potrzeby marketingu bezpośredniego (w tym **ewentualnie** profilowania), Organizacja uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
- 4.14. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Organizacja 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**, Organizacja zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Organizacji, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Organizacją; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

5. MINIMALIZACJA

Organizacja 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.

5.1. Minimalizacja zakresu

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

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

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

5.2. Minimalizacja dostępu

Organizacja 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).

Organizacja stosuje kontrolę dostępu fizycznego.

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

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

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Organizacji.

5.3. Minimalizacja czasu

Organizacja wdraża mechanizmy kontroli cyklu życia danych osobowych w Organizacji, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Organizacji, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Organizację. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

6. **BEZPIECZEŃSTWO**

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

6.1. **Analizy ryzyka i adekwatności środków bezpieczeństwa**

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

- (1) Organizacja zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych.
- (2) Organizacja kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- (3) Organizacja przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Organizacja 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) Organizacja ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Organizacja ustala przydatność i stosuje takie środki i podejście jak:
 - (i) pseudonimizacja,
 - (ii) szyfrowanie danych osobowych,
 - (iii) inne 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 katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

6.2. **Oceny skutków dla ochrony danych**

Organizacja dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

Organizacja stosuje metodykę oceny skutków przyjętą w Organizacji.

6.3. **Środki bezpieczeństwa**

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

Organizacja bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Organizacji i są bliżej opisane w procedurach przyjętych przez Organizację dla tych obszarów.

6.4. **Zgłaszanie naruszeń**

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

7. **PRZETWARZAJĄCY**

Organizacja posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Organizacji 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 Organizacji.

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

Organizacja rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

8. **EKSPORT DANYCH**

Organizacja rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

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

9. **PROJEKTOWANIE PRYWATNOŚCI**

Organizacja 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 Organizację 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.