POLITYKA OCHRONY DANYCH OSOBOWYCH W PUBLICZNEJ SZKOLE PODSTAWOWEJ NR 2 W RUDNIKU NAD SANEM

WSTĘP

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).
Ochrona przetwarzanych danych osobowych rozumiana jest natomiast jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Przy czym przez;

- poufność danych należy rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych należy rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych należy rozumieć właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- dostępność informacji należy rozumieć zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

Polityka zawiera:

a. opis zasad ochrony danych obowiązujących w Publicznej Szkole Podstawowej nr 1 im. Jana Pawła II w Rudniku nad Sanem,
b. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

1. 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)

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

Dane szczególnych kategorii 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 lub **podmiot danych** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Administrator Danych Osobowych (ADO) lub **Administrator** oznacza Publiczną Szkołę Podstawową nr 2 w Rudniku nad Sanem reprezentowaną przez Dyrektora Szkoły.

Podmiot przetwarzający oznacza instytucję lub osobę, której Publiczna Szkoła Podstawowa nr 2 w Rudniku nad Sanem powierzyła przetwarzanie danych osobowych.

IOD lub **Inspektor** oznacza Inspektora Ochrony Danych Osobowych.

System informatyczny oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

System tradycyjny oznacza zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.

RCPD lub **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Organizacja oznacza Publiczną Szkołę Podstawową nr 2 w Rudniku nad Sanem.

2. CEL POLITYKI OCHRONY DANYCH

2.1. Celem niniejszego dokumentu jest zapewnienie zgodności procesu przetwarzania danych osobowych w Organizacji z obowiązującymi przepisami prawa, w szczególności z RODO, a co za tym idzie zapewnienie przetwarzania tych danych w sposób gwarantujący ich bezpieczeństwo.

2.2. Regulacje wewnętrzne zawarte w niniejszym dokumencie określają środki i sposoby ochrony danych osobowych przyjętych przez Administratora danych. Zmiany organizacyjne, zmiany sposobu działania Administratora danych w zakresie mającym wpływ na proces przetwarzania danych osobowych oraz zmiany przepisów prawa będą powodowały konieczność aktualizacji niniejszego dokumentu.

3. ZAKRES STOSOWANIA POLITYKI OCHRONY DANYCH

3.1. Niniejszą Politykę stosuje się w odniesieniu do wszelkich danych osobowych, wobec których Organizacji przysługuje status Administratora Danych Osobowych, przetwarzanych zarówno w systemach informatycznych jak i w systemach tradycyjnych (papierowych) tj. księgach, skorowidzach, wykazach i innych zbiorach ewidencyjnych, w szczególności danych osobowych przetwarzanych w celach rekrutacyjnych, zatrudnienia i nawiązania współpracy, finansowych i rachunkowych, świadczenia usług, marketingowych oraz windykacyjnych.

3.2. Zakres stosowania Polityki obejmuje ponadto;

a. wszystkie lokalizacje - budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie,
b. wszystkich pracowników w rozumieniu przepisów Kodeksu pracy, współpracowników, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

3.3. Niniejszy dokument podlega przeglądom i aktualizacji, w szczególności w przypadku wystąpienia zmian w przepisach prawa oraz w przypadku wprowadzania zmian w działaniach Administratora danych związanych z przetwarzaniem danych osobowych.

4. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

4.1 **Administrator Danych Osobowych**

Na Administratorze danych spoczywa odpowiedzialność za realizację szeregu zadań wynikających z RODO. Są to w szczególności takie zadania jak;

a. utworzenie nowych klauzul informacyjnych wynikających z obowiązków ADO zawartych w art. 13-14 RODO (art.12),
b. ułatwianie podmiotom danych wykonywania ich praw wynikających z art. 15-22 RODO (art.15-22),
c. wdrożenie i uaktualnianie niniejszej dokumentacji wraz z procedurami ochrony danych (art.24),
d. uwzględnianie ochrony danych w fazie projektowania (art.25),
e. wyznaczanie podmiotów przetwarzających dane osobowe na podstawie umowy lub innego aktu prawnego (art.28),
f. weryfikacja i uaktualnienie upoważnień do przetwarzania danych osobowych (art.28),
g. prowadzenie rejestru czynności przetwarzania danych (art.30),
h. współpraca z organem nadzorczym (art. 31),
i. analiza ryzyka naruszenia praw podmiotów danych (art.32),
j. wdrożenie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa przetwarzania danych odpowiadającego analizowanym ryzykom (art.32),
k. zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (art.33),
l. prowadzenie rejestru naruszeń ochrony danych osobowych (art.33),
m. zawiadamianie podmiotów danych o naruszeniach ochrony ich danych osobowych (art.34),
n. opracowanie dokumentacji określanej jako „ocena skutków dla ochrony danych" w przypadkach wymienionych w art. 35 RODO (art.35),
o. prowadzenie tzw. „uprzednich konsultacji" z organem nadzorczym w przypadku wymienionym w art. 36 RODO (art.36),
p. wyznaczenie inspektora ochrony danych (art.37).

4.2. **Inspektor Ochrony Danych**

Wyznaczenie Inspektora Ochrony Danych jest obligatoryjne w przypadkach wymienionych w art.37 ust.1 RODO. Jest więc także jednym z obowiązków nałożonych na Administratora danych. Inspektor Ochrony Danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Do zadań tych należy;

a. informowanie Administratora danych oraz pracowników odpowiedzialnych za przetwarzanie danych o ich obowiązkach wynikających z RODO,
b. monitorowanie przestrzegania przepisów RODO, Polityki ochrony danych oraz innych przepisów dotyczących ochrony danych osobowych,
c. szkolenia personelu i inne działania zwiększające świadomość wagi przestrzegania przepisów dotyczących ochrony danych osobowych,

d. przeprowadzanie audytów związanych z przetwarzaniem danych osobowych,
e. udzielanie zaleceń co do „oceny skutków dla ochrony danych", wynikającej z art. 35 RODO,
f. współpraca z organem nadzorczym,
g. pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz podmiotów danych.

4.3. **Administrator Systemów Informatycznych (ASI)**

Wyznaczenie Administratora Systemów Informatycznych nie jest wymagane w żadnych regulacjach prawnych określających sposób zarządzania i zabezpieczania danych osobowych. Niemniej jednak w organizacjach korzystających z narzędzi informatycznych wydaje się być niezbędne. Warunkiem nieodzownym zatrudnienia ASI jest odpowiednia wiedza w zakresie IT. Do jego obowiązków należy w szczególności;

a. współpraca przy przygotowaniu i wdrażaniu dokumentacji ochrony danych osobowych,
b. współpraca przy przeprowadzaniu okresowych audytów związanych z przetwarzaniem danych osobowych,
c. zapewnienie ciągłości działania systemu,
d. zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej,
e. nadzór nad naprawą oraz likwidacją urządzeń komputerowych,
f. kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych,
g. zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,
h. dostosowanie wszystkich systemów informatycznych służących do przetwarzania danych osobowych do wymogów RODO,
i. zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
j. ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
k. nadzorowanie stosowania zasady „czystego ekranu".

4.4. **Osoby upoważnione do przetwarzania danych osobowych**

4.4.1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych w Organizacji zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO oraz niniejszej Polityki ochrony danych.

4.4.2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich przetwarzania i zabezpieczenia. Obowiązek ten istnieje także po ustaniu stosunku zatrudnienia oraz świadczenia usług.

4.5. **Osoby i instytucje, którym Organizacja powierza dane osobowe**

Każda osoba lub instytucja, której Organizacja powierza dane osobowe zobowiązana jest do ich ochrony oraz zachowania tajemnicy w sposób zgodny z przepisami RODO oraz zawartej Umowy powierzenia przetwarzania danych.

5. OCHRONA DANYCH OSOBOWYCH W ORGANIZACJI – ZASADY OGÓLNE

5.1. **Filary ochrony danych osobowych w Organizacji**:

a. Legalność – Organizacja dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
b. Bezpieczeństwo – Organizacja zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
c. Prawa jednostki – Organizacja umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
d. Rozliczalność –Organizacja dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z obowiązującymi przepisami.

5.2. **Zasady ochrony danych**

Organizacja przetwarza dane osobowe z poszanowaniem następujących zasad:

a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b. rzetelnie i uczciwie (rzetelność);
c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d. w konkretnych celach i nie „na zapas” (minimalizacja);
e. nie więcej niż potrzeba (adekwatność);
f. z dbałością o prawidłowość danych (prawidłowość);
g. nie dłużej niż potrzeba (czasowość);
h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6. SYSTEM OCHRONY DANYCH

System ochrony danych osobowych składa się z następujących elementów:

6.1. **Inwentaryzacja danych**

Organizacja dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
a. przypadków przetwarzania danych szczególnych kategorii i danych karnych,
b. przypadków przetwarzania danych osób, których Organizacja nie identyfikuje,
c. przypadków przetwarzania danych dzieci,
d) współadministrowania danymi.

6.2. **Rejestr**

Organizacja opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Organizacji.

6.3. **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 przetwarzania danych na podstawie prawnie uzasadnionego interesu.

6.4. **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 przez RODO oraz dokumentowane;
d. zawiadamianie o naruszeniach
   Organizacja stosuje zasady pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6.5. **Minimalizacja**

Celem Organizacji jest zoptymalizowanie zasad i metod zarządzania minimalizacją a w tym:

a. zasad zarządzania adekwatnością danych;
b. zasad reglamentacji i zarządzania dostępem do danych;
c. zasad zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6.6. **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.

6.7. **Przetwarzający**

Organizacja stosuje zasady doboru przetwarzających dane na rzecz Organizacji, wymogów co do warunków przetwarzania (umowa powierzenia) oraz zasady weryfikacji wykonywania umów powierzenia.

6.8. **Eksport danych**

Organizacja stosuje zasady weryfikacji dotyczące nie przekazywania danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

6.9. **Privacy by design**

Organizacja zarządza zmianami wpływającymi na prywatność. W tym celu w razie potrzeby utworzy procedury uruchamiania nowych projektów uwzględniające konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

6.10. **Przetwarzanie transgraniczne**

Organizacja stosuje zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

7. INWENTARYZACJA

7.1. **Dane szczególnych kategorii i dane karne**

Organizacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Organizacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

7.2. **Dane niezidentyfikowane**

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

7.3. **Współadministrowanie**

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

8. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

8.1. 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.

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

8.3. W Rejestrze dla każdej czynności przetwarzania danych, którą uznano za odrębną dla potrzeb Rejestru, Organizacja odnotowuje:

a. nazwę czynności,
b. cel przetwarzania,
c. opis kategorii osób,
d. opis kategorii danych,
e. podstawę prawną przetwarzania,
f. sposób zbierania danych,
g. opis kategorii odbiorców danych (w tym przetwarzających),
h. informację o przekazaniu poza EU/EOG,
i. ogólny opis technicznych i organizacyjnych środków ochrony danych.

8.4. Wzór Rejestru stanowi Załącznik 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.

9. PODSTAWY PRZETWARZANIA

9.1. Organizacja dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

9.2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, prawnie uzasadniony interes), Organizacja dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.

9.3. 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 (e -mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

10. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

10.1. Organizacja dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

10.2. Organizacja ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Organizacji, w tym wymaganiach dotyczących identyfikacji oraz metodach kontaktu z Organizacją w tym celu.

10.3. Organizacja dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

10.4. Organizacja wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

10.5. W celu realizacji praw jednostki Organizacja zapewnia mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Organizację, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

10.6. Organizacja dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. OBOWIĄZKI INFORMACYJNE

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

11.2. Organizacja informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

11.3. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

11.4. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

11.5. Organizacja określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

11.6. Organizacja informuje osobę o planowanej zmianie celu przetwarzania danych.

11.7. Organizacja informuje osobę przed uchyleniem ograniczenia przetwarzania.

11.8. Organizacja informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

11.9. Organizacja informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

11.10. Organizacja bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

12. ŻĄDANIA OSÓB

12.1. **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), Organizacja może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

12.2. **Nieprzetwarzanie.**

Organizacja informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

12.3. **Odmowa.**

Organizacja informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

12.4. **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.

12.5. **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 na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

12.6. **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.

12.7. **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.

12.8. **Usunięcie danych**. Na żądanie osoby Organizacja 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,
e. konieczność usunięcia wynika z obowiązku prawnego,

f. 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.

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

12.10. **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.

12.11. **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.

12.12. **Sprzeciw względem marketingu bezpośredniego**.

Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Organizację na potrzeby marketingu bezpośredniego Organizacja uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

13. MINIMALIZACJA

Organizacja dba o minimalizację przetwarzania danych pod kątem:

a. adekwatności danych do celów (ilości danych i zakresu przetwarzania),
b. dostępu do danych,
c. czasu przechowywania danych.

13.1. **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).

13.2. **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.

13.3. **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 informatycznych 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.

14. BEZPIECZEŃSTWO

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

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

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

14.1.1. Organizacja zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

14.1.2. Organizacja kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

14.1.3. 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 rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

14.1.4. 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:

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,
d. 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.

14.2. **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.

14.3. **Środki bezpieczeństwa**

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

14.4. **Zgłaszanie naruszeń**

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

15. PRZETWARZAJĄCY

Organizacja stosuje zasady doboru i weryfikacji podmiotów przetwarzających dane na rzecz Organizacji opracowane w celu zapewnienia, aby podmioty przetwarzające dawały 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 do Polityki – „Wzór umowy powierzenia przetwarzania danych".

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

16. EKSPORT DANYCH

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

17. 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.