Lublin, dnia 25 maja 2018r.

POLITYKA OCHRONY DANYCH OSOBOWYCH W PORADNI LEKARZA RODZINNEGO "ZDROWA RODZINA" RENATA SZEWCZAK

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej jako Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Poradni Lekarza Rodzinnego „Zdrowa Rodzina" Renata Szewczak (dalej jako poradnia).

   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 poradni;

   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 właściciel - Renata Szewczak. Za stosowanie niniejszej Polityki odpowiedzialni są: wszyscy członkowie personelu poradni.

Poradnia „Zdrowa Rodzina" powinna też zapewnić zgodność postępowania kontrahentów poradni z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez poradnię.

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 jednostka 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.

Poradnia Lekarza Rodzinnego „Zdrowa Rodzina" Renata Szewczak oznacza firmę przedsiębiorcy, dalej: poradnia, Zdrowa Rodzina.

5. Ochrona danych osobowych w poradni - zasady ogólne

5.1. Filary ochrony danych osobowych w poradni:

(1) Legalność - Zdrowa Rodzina dba o ochronę prywatności przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** Zdrowa Rodzina zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa** Jednostki-Zdrowa Rodzina umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) Rozliczalność - Zdrowa Rodzina dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych

Zdrowa Rodzina 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 poradni składa się z następujących elementów:

1) Inwentaryzacja danych. Zdrowa Rodzina dokonuje identyfikacji zasobów danych osobowych w poradni, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja}, w tym:

   a) przypadków przetwarzania danych specjalnych danych „kryminalnych" **(dane wrażliwe);**

   b) przypadków przetwarzania danych osób, których poradnia nie identyfikuje **(dane niezidentyfikowa**ne/UFO);

   c) przypadków przetwarzania danych dzieci;

   d) profilowania;

   e) współadministrowania danymi.

2) **Rejestr.** Zdrowa Rodzina opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w poradni (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w poradni.

3) **Podstawy prawne.** Zdrowa Rodzina zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   a) utrzymuje system zarządzania zgodami na przetwarzanie danych komunikację na odległość,

   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy poradnia przetwarza dane na podstawie prawnie uzasadnionego interesu Zdrowa Rodzina.

4) Obsługa praw jednostki. Poradnia spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   a) **Obowiązki** informacyjne. Zdrowa Rodzina przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

   b) Możliwość wykonania żądań. Zdrowa Rodzina weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) **Obsługa żądań.** Zdrowa Rodzina zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

d) **Zawiadamianie** o naruszeniach. Zdrowa Rodzina stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) Minimalizacja. Zdrowa Rodzina 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.** Zdrowa Rodzina zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

b) dostosowuje środki ochrony danych do ustalonego ryzyka;

c) posiada system zarządzania bezpieczeństwem informacji;

d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego_ naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.

7) **Przetwarzający.** Zdrowa Rodzina posiada zasady doboru przetwarzających dane na rzecz poradni, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) Eksport danych. Zdrowa Rodzina posiada zasady weryfikacji, czy poradnia 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.* Zdrowa Rodzina zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w poradni 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. Zdrowa Rodzina posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. Inwentaryzacja

6.1. Dane wrażliwe

Zdrowa Rodzina 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, Zdrowa Rodzina postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2. Dane niezidentyfikowane

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

6.3. Profilowanie

Zdrowa Rodzina nie dokonuje profilowania przetwarzanych danych.

6.4. Współadministrowanie

Zdrowa Rodzina w chwili obecnej nie współadministruje danymi osobowymi.

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

7.3. Rejestr jest jednym z podstawowych narzędzi umożliwiającym poradni rozliczanie większości obowiązków ochrony danych.

7.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Zdrowa Rodzina uznała za odrębną dla potrzeb Rejestru, poradnia 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 Spółki, 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 26 do dokumentacji RODO - „Wzór Rejestru Czynności_ Przetwarzania Danych". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Zdrowa Rodzina 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. Zdrowa Rodzina dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel poradni) Zdrowa Rodzina 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. Zdrowa Rodzina 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. Właściciel poradni ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes poradni, właściciel ma obowiązek znać konkretny realizowany przetwarzaniem interes poradni.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1. Zdrowa Rodzina dba o czytelność i styl przekazywanych informacji komunikacji z osobami, których dane przetwarza.

9.2. Zdrowa Rodzina ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej poradni informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w poradni, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z poradnią w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

9.3. Zdrowa Rodzina dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4. Poradnia wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

9.5. W celu realizacji praw jednostki Zdrowa Rodzina zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez poradnię, zintegrować te dane, wprowadzać do nich zmiany i usuwać **w** sposób zintegrowany,

9.6. Zdrowa Rodzina dokumentuje obsługę obowiązków informacyjnych, zawiadomień żądań osób.

10. **Obowiązki** informacyjne

10.1. Zdrowa Rodzina określa zgodne z prawem efektywne sposoby wykonywania obowiązków informacyjnych.

10.2. Zdrowa Rodzina informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3. Zdrowa Rodzina informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

10.4. Zdrowa Rodzina informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

10.5. Zdrowa Rodzina określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe.

10.6. Zdrowa Rodzina informuje osobę o planowanej zmianie celu przetwarzania danych.

10.7. Zdrowa Rodzina informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

10.9. Zdrowa Rodzina informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

10.10. Zdrowa Rodzina 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, Zdrowa Rodzina 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.), Zdrowa Rodzina może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

11.2. Nieprzetwarzanie. Zdrowa Rodzina informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3. Odmowa. Zdrowa Rodzina 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, Zdrowa Rodzina 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 Zdrowa Rodzina nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

11.5. Kopie danych. Na żądanie Zdrowa Rodzina wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Zdrowa Rodzina 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. Zdrowa Rodzina dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Poradnia ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Zdrowa Rodzina informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.7. Uzupełnienie danych. Zdrowa Rodzina uzupełnia i aktualizuje dane na żądanie osoby. Poradnia ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Zdrowa Rodzina nie musi przetwarzać danych, które są poradni zbędne). Zdrowa Rodzina może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez poradnię procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8. Usunięcie danych. Na żądanie osoby, Zdrowa Rodzina 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,

Zdrowa Rodzina 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 Zdrową Rodzinę, poradnia 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 Zdrowa Rodzina informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania. Zdrowa Rodzina 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) Zdrowa Rodzina 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 poradni zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Zdrowa Rodzina 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. Zdrowa Rodzina informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych Zdrowa Rodzina informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10. Przenoszenie danych. Na żądanie osoby Zdrowa Rodzina 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 poradni, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych poradni.

11.11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane *są* przez Zdrowa Rodzina w oparciu o uzasadniony interes poradni lub o powierzone poradni zadanie w interesie publicznym, Zdrowa Rodzina **uwzględni** sprzeciw, o ile nie zachodzą po stronie poradni 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 Zdrowa Rodzina prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Zdrowa Rodzina 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 Zdrowa Rodzina na potrzeby marketingu bezpośredniego (w tym **ewentualnie** profilowania), Zdrowa Rodzina uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

12. MINIMALIZACJA

Zdrowa Rodzina 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

Zdrowa Rodzina zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
Zdrowa Rodzina dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
Zdrowa Rodzina przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą *(privacy by design).*

12.2. Minimalizacja dostępu

Zdrowa Rodzina 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).
Zdrowa Rodzina stosuje kontrolę dostępu fizycznego.
Zdrowa Rodzina dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Zdrowa Rodzina 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 poradni.

12.3. Minimalizacja czasu

Zdrowa Rodzina wdraża mechanizmy kontroli cyklu życia danych osobowych w poradni, 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 poradni, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez poradnię. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

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

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

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

(1) poradnia zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(2) poradnia kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(3) poradnia przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Poradnia 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) poradnia ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym poradnia 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.

13.2. Oceny skutków dla ochrony danych

Zdrowa Rodzina dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
Zdrowa Rodzina stosuje metodykę oceny skutków przyjętą w poradni.

13.3. Środki bezpieczeństwa

Zdrowa Rodzina 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 poradni i są bliżej opisane w procedurach przyjętych przez poradnię dla tych obszarów.

13.4. Zgłaszanie naruszeń

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

14. PRZETWARZAJĄCY

Zdrowa Rodzina posiada zasady doboru i weryfikacji przetwarzających dane na rzecz poradni 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 poradni.

Zdrowa Rodzina przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 14 do dokumentacji RODO - „Wzór umowy powierzenia przetwarzania danych".

Zdrowa Rodzina rozlicza przetwarzających z wykorzystania pod przetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

15. EKSPORT DANYCH

Zdrowa Rodzina 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), Zdrowa Rodzina okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

16. PROJEKTOWANIE PRYWATNOŚCI

Zdrowa Rodzina 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 poradnię odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

17. POSTANOWIENIA KOŃCOWE

Zdrowa Rodzina zobowiązuje się ponadto do przedsięwzięcia wszelkich możliwych środków i sposobów eliminujących rzeczywiste i potencjalne zagrożenia w zakresie ochrony danych osobowych swoich pacjentów, pracowników, jak i wszystkich podmiotów współpracujących z poradnią.