

Polityka ochrony danych osobowych w Fizjoterapii Optima w Poznaniu.

Celem Polityki ochrony danych osobowych, zwanej dalej Polityką, jest wprowadzenie i utrzymanie wymaganej przez przepisy rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) właściwej ochrony danych osobowych w związku z przetwarzaniem danych osobowych w Fizjoterapii Optima w Poznaniu Mariola Ejzenchart – Wojkiewicz, ul. Kochanowskiego 22/6, 60-846 Poznań, NIP 781 155 87 68.

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

W skład obszaru przetwarzania danych osobowych w Fizjoterapii Optima Mariola Ejzenchart – Wojkiewicz w Poznaniu wchodzi lokalność położona w Poznaniu przy ul. Kochanowskiego 22/6, 60-846 Poznań oraz przy ul. Kościelnej 42, 60-538 Poznań

Określenia użyte w Polityce ochrony danych osobowych oznaczają:

1. **administrator danych osobowych (ADO)** – Fizjoterapia Optima Mariola Ejzenchart - Wojkiewicz
2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **przetwarzanie danych osobowych** – gromadzenie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. **użytkownik** – osoba upoważniona do przetwarzania danych osobowych,
5. **system informatyczny** – system (urządzenia, narzędzia, programy), w którym przetwarzane są dane osobowe,
6. **zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą,

7. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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,

8. **ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

1. Zasady przetwarzania danych osobowych

1.1. Administrator danych przetwarza dane osobowe:

- zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”),
- zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu”),
- adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),
- prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość”),
- przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”),
- w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

1.2.

W celu realizacji tych zasad administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje przysługujące im uprawnienia takie jak prawo do:

- dostępu do danych,
- sprostowania danych,

- usunięcia danych (prawo do bycia zapomnianym),
- przenoszenia,
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania,
- wniesienia skargi do organu nadzorczego,
- sprzeciwu wobec bycia profilowanym.

Administrator danych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających realizujących obowiązki wynikające z RODO. W razie wystąpienia incydentu technicznego lub fizycznego administrator danych zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

1.3.

Potwierdzenie spełniania obowiązków informacyjnych przez administratora danych stanowią klauzule informacyjne przekazywane osobom, których dane są przetwarzane. W przypadku pracowników przedstawia się im klauzule do podpisania i zamieszcza w aktach osobowych pracowników)

W przypadku klientów i kontrahentów przekazywane im są w momencie zawierania umowy, są również wywieszane w widocznym miejscu w Fizjoterapii Optima.

2. Upoważnienia do przetwarzania danych Administrator danych zapewnia aby dostęp do danych osobowych w Fizjoterapii Optima Mariola Ejzenchart – Wojkiewicz miały tylko osoby legitymujące się nadanym przez ADO upoważnieniem. Upoważnienia określają do jakich operacji użytkownicy są uprawnieni, tj. tworzenia, usuwania, wglądu, przekazywania danych, w jakich systemach oraz na jaki czas. Administrator danych prowadzi ewidencję osób upoważnionych. Upoważnienia do przetwarzania danych osobowych mogą być nadawane na wniosek bezpośredniego przełożonego użytkownika systemu.

3. Analiza ryzyka

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie raz w roku, lub po wprowadzeniu znaczących zmian w przetwarzaniu danych lub po wystąpieniu naruszenia ochrony danych osobowych. Analiza danych prowadzona jest osobno dla każdego zbioru danych lub dla kilku zbiorów o podobnym zakresie danych. W

przypadku konieczności przeprowadza się ocenę skutków dla oceny ryzyka na mocy art. 35 RODO.

4. Wykaz zabezpieczeń

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

5. Rejestr czynności przetwarzania

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza się:

- a) imię i nazwisko oraz dane kontaktowe administratora,
- b) cele przetwarzania,
- c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- e) gdy ma to zastosowanie, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,
- f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

6. Powołanie inspektora ochrony danych

Administrator Danych Osobowych może powołać inspektora ochrony danych. W przypadku powołania inspektora ochrony danych do jego zadań należą:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz ustawy o ochronie danych osobowych,
- monitorowanie przestrzegania przepisów RODO oraz ustawy o ochronie danych osobowych oraz Polityki ochrony danych obowiązującej w jednostce, w tym podział obowiązków, działania

zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,

- współpraca z organem nadzorczym, tj. Prezesem Urzędu Ochrony Danych Osobowych,

- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

W przypadku wyznaczenia inspektora ochrony danych należy zgłosić jego powołanie Prezesowi Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

7. Procedura postępowania z incydentami.

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana właścicielowi Fizjoterapii Optima Marioli Ejzenchart – Wojkiewicz.

Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekami, kradzieżami i utratą danych osobowych, udostępnienie haseł osobom postronnym,

- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),

- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,

- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,

- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,

- obecność osób postronnych w jednostce,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
- awarie serwera, komputerów, twardego dysku, oprogramowania,
- udostępnienie danych osobowych osobom nieupoważnionym,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardego dysku, pen-drive z danymi osobowymi,
- maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
- zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze.

W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

8. Umowy powierzenia przetwarzania danych osobowych

8.1. W przypadku zlecenia przetwarzania danych osobowych podmiotom zewnętrznym administrator danych zobowiązany jest zawrzeć umowę powierzenia. W jednostce prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.

8.2. Umowa określa kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ponadto zobowiązuje podmiot przetwarzający do:

- a) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- b) zapewniania, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- c) podejmowania wszelkich środków wymaganych na mocy art. 32 RODO,
- d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego,
- e) pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,
- f) pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,
- g) usuwania lub zwracania administratorowi danych osobowych oraz usuwania wszelkich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
- h) udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach RODO oraz umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji i przyczynia się do nich.

9. Czynności kontrolne

Nadzór i kontrolę nad ochroną danych osobowych sprawuje administrator danych. Czynności kontrolne przeprowadzane są co 6 miesięcy. Z czynności kontrolnych sporządza się protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności, a także zalecenia i działania naprawcze. Protokół podpisany jest przez osoby wykonujące czynności kontrolne.

10. Odpowiedzialność osób upoważnionych do przetwarzania danych

Niezastosowanie się do prowadzonej przez administratora danych Polityki ochrony danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Poznań, 25.05.2018 r.