Polityka ochrony danych osobowych

ACTIO Sport i Rehabilitacja Olga Bugaj-Jarząb

Niniejszy dokument stanowi kompleksową politykę ochrony danych osobowych podmiotu leczniczego *ACTIO Sport i Rehabilitacja Olga Bugaj-Jarząb* (dalej jako „Actio" lub „Administrator"). Zawiera on informacje wymagane przez art. 13 RODO (ogólnego rozporządzenia o ochronie danych) oraz opisuje procedury ochrony danych, rejestry czynności przetwarzania, zasady retencji dokumentacji itp., stosowane w naszej placówce. Polityka jest dostępna na stronie internetowej oraz w siedzibie Actio i przeznaczona do udostępnienia pacjentom (również w formie wydruku do podpisu, co potwierdza zapoznanie się z jej treścią).

Administrator danych osobowych

Administratorem Pani/Pana danych osobowych jest ACTIO Sport i Rehabilitacja Olga Bugaj-Jarząb z siedzibą przy ul. Słonecznikowej 4, 62-030 Luboń. Administrator prowadzi działalność leczniczą jako podmiot wykonujący działalność leczniczą (z zakresu fizjoterapii). Kontakt z Administratorem możliwy jest poprzez e-mail actio.fizjoterapia@gmail.com oraz telefon691560929.

Dane rejestrowe Administratora: Olga Bugaj-Jarząb prowadząca działalność gospodarczą pod firmą ACTIO Sport i Rehabilitacja Olga Bugaj-Jarząb, NIP: 7773166491, REGON: 387019330.

Inspektor ochrony danych

W Actio nie powołano Inspektora Ochrony Danych Osobowych (IOD), gdyż nie zachodzi ustawowy wymóg takiego powołania w przypadku działalności naszego gabinetu. W sprawach dotyczących przetwarzania danych osobowych prosimy kontaktować się bezpośrednio z Administratorem – dane kontaktowe powyżej.

Cele i podstawy przetwarzania danych

Przetwarzamy Pani/Pana dane osobowe wyłącznie w określonych celach, na odpowiedniej podstawie prawnej. Poniżej przedstawiamy główne czynności przetwarzania wraz z ich celami i podstawami prawnymi:

1) Udzielanie świadczeń zdrowotnych (rehabilitacyjnych) i prowadzenie dokumentacji medycznej: Pani/Pana dane są przetwarzane przede wszystkim w celu diagnozy oraz prowadzenia terapii fizjoterapeutycznej, a także obowiązkowego prowadzenia indywidualnej dokumentacji medycznej każdego pacjenta. Podstawą prawną jest art. 6 ust. 1 lit. c RODO (wypełnienie obowiązku prawnego ciążącego na Administratorze) w zw. z art. 24 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (obowiązek prowadzenia, przechowywania i udostępniania dokumentacji medycznej), a w przypadku danych o stanie zdrowia – art. 9 ust. 2 lit. h RODO (przetwarzanie niezbędne do udzielania świadczeń zdrowotnych przez osobę wykonującą zawód medyczny). Dodatkowo przetwarzanie danych może odbywać się na podstawie art. 6 ust. 1 lit. b RODO (niezbędność do wykonania umowy o

świadczenie usług medycznych) – dotyczy to sytuacji, gdy pomiędzy pacjentem a naszym gabinetem dochodzi do zawarcia umowy o usługę zdrowotną (np. w przypadku pacjentów komercyjnych korzystających z naszych usług odpłatnie poza systemem publicznym).

2) Umawianie wizyt i kontakt z pacjentem: W celu rejestracji wizyt, ich potwierdzania, odwoływania lub zmiany terminu, a także przekazywania zaleceń czy informacji o wynikach konsultacji, możemy przetwarzać Pani/Pana dane kontaktowe – numer telefonu oraz adres e-mail. Takie przetwarzanie danych kontaktowych odbywa się na podstawie naszego prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO), jakim jest zapewnienie sprawnej komunikacji z pacjentem w toku udzielania świadczeń oraz dbałość o wysoką jakość usług. Uwaga: Podanie numeru telefonu i adresu e-mail jest dobrowolne i ich niepodanie nie wpływa na uzyskanie świadczenia zdrowotnego – w wielu przypadkach utrudnia jednak kontakt i może obniżyć sprawność komunikacji oraz jakość obsługi. Jeżeli wyraził(a) Pan/Pani odrębną zgodę na kontakt (np. na otrzymywanie przypomnień SMS o wizytach lub komunikację e-mail), wówczas podstawą przetwarzania danych kontaktowych jest art. 6 ust. 1 lit. a RODO (zgoda). Taka zgoda może zostać w każdej chwili wycofana – jej wycofanie nie wpływa jednak na legalność wcześniejszego przetwarzania ani na możliwość udzielania świadczeń zdrowotnych. W praktyce oznacza to, że po wycofaniu zgody zaprzestaniemy np. wysyłania powiadomień SMS/e-mail, jednak w dalszym ciągu możemy kontaktować się w niezbędnym zakresie korzystając z innych podstaw prawnych (np. kontaktujemy się telefonicznie, jeśli będzie to konieczne w celu poinformowania o istotnych kwestiach dotyczących terapii – takie działanie nie wymaga odrębnej zgody zgodnie z tzw. kodeksem branżowym ochrony danych osobowych w służbie zdrowia).

3) Wystawianie zaświadczeń i formularzy medycznych: Na Pani/Pana prośbę wystawiamy określone zaświadczenia związane z procesem leczenia (np. zaświadczenie dla lekarza prowadzącego, opinię dla potrzeb komisji orzekającej o niepełnosprawności, itp.), wówczas przetwarzamy dane zawarte w dokumentacji medycznej w tym celu na podstawie przepisów prawa regulujących zasady wydawania takich dokumentów (co zwykle odbywa się w ramach celu udzielania świadczeń zdrowotnych, wskazanego powyżej – art. 9 ust. 2 lit. h RODO). Jeśli zaświadczenie jest wymagane przepisami (np. dokumentacja do celów ubezpieczenia społecznego), podstawą prawną może być również art. 6 ust. 1 lit. c RODO w zw. z właściwym przepisem (np. art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, gdy chodzi o wystawienie zaświadczenia o rehabilitacji dla celów zasiłku chorobowego).

4) Rozliczenia finansowe i księgowość: W zakresie, w jakim przetwarzanie Pani/Pana danych osobowych jest niezbędne do rozliczenia świadczonych usług, wystawienia rachunku lub faktury, prowadzenia ksiąg rachunkowych i wywiązania się z obowiązków podatkowych – podstawą prawną jest art. 6 ust. 1 lit. c RODO (obowiązek prawny) w zw. z ustawą o rachunkowości i przepisami

podatkowymi. Dotyczy to najczęściej takich danych jak imię i nazwisko (na fakturze imiennej) oraz ewentualnie adres – tylko jeżeli pacjent zażyczy sobie dokument sprzedaży ze swoimi danymi lub gdy wymagają tego przepisy. Nasze dokumenty finansowe przechowujemy przez okres wymagany prawem (5 lat, patrz część Polityka retencji).

5) Dochodzenie roszczeń prawnych i obrona przed roszczeniami: Pani/Pana dane mogą być także przetwarzane w celu ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami prawnymi – co stanowi nasz prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO). Przykładowo, jeżeli zaszłaby potrzeba dochodzenia od pacjenta zapłaty zaległych należności lub obrony przed zarzutem niewłaściwego wykonania usługi, możemy wykorzystywać niezbędne dane (w tym dokumentację medyczną) dla celów dowodowych. Dane w tych celach będą przetwarzane jedynie przez okres przedawnienia potencjalnych roszczeń zgodnie z przepisami prawa cywilnego (patrz Polityka retencji) i tylko w niezbędnym zakresie.

6) Marketing (brak regularnego przetwarzania): Nie wykorzystujemy Pani/Pana danych osobowych do celów marketingu usług własnych ani osób trzecich, nie przesyłamy niezamówionych informacji handlowych ani newsletterów bez wyraźnej zgody. Jeżeli w przyszłości chcielibyśmy przesłać np. informację o nowej usłudze czy promocji – poprosimy odrębnie o zgodę marketingową. Brak zgody (lub jej wycofanie) na cele marketingowe nie ma wpływu na korzystanie z naszych usług medycznych.

Zakres przetwarzanych danych

Przetwarzamy wyłącznie dane osobowe niezbędne do realizacji powyższych celów. Zakres danych pozyskiwanych od pacjenta obejmuje w szczególności:

1) Dane identyfikacyjne: imię i nazwisko, data urodzenia, PESEL (o ile został nadany, a w przypadku jego braku – rodzaj i numer dokumentu tożsamości), płeć, adres zamieszkania oraz inne dane wymagane do jednoznacznej identyfikacji pacjenta. W przypadku pacjenta małoletniego (poniżej 18 roku życia) gromadzimy również dane przedstawiciela ustawowego – tj. imię i nazwisko rodzica/opiekuna, jego adres, PESEL i kontakt. Dane identyfikacyjne są niezbędne do prowadzenia dokumentacji medycznej zgodnie z przepisami (m.in. pierwsza strona dokumentacji musi zawierać oznaczenie pacjenta: imię, nazwisko, datę urodzenia, adres, PESEL itp.).

2) Dane kontaktowe: numer telefonu, adres e-mail oraz ewentualnie adres do korespondencji. Dane te ułatwiają bieżący kontakt i obsługę pacjenta (np. umawianie wizyt, przesyłanie zaleceń). Ich podanie jest dobrowolne – patrz wyżej sekcja o podstawach przetwarzania (kontakt z pacjentem) odnośnie skutków niepodania tych danych.

3) Dane medyczne (szczególna kategoria danych): informacje o stanie zdrowia pacjenta, w tym zgłaszane dolegliwości, wyniki badań, diagnozy lekarskie, historia choroby, opis stanu funkcjonalnego, plan i przebieg procesu rehabilitacji, zastosowane zabiegi, postępy terapii, zalecenia itp. – słowem, pełna treść dokumentacji medycznej prowadzonej w naszym gabinecie. Mogą one obejmować także dostarczone przez pacjenta dokumenty medyczne (np. kopie wyników badań obrazowych, wypisów ze szpitala) – takie dokumenty włączamy do dokumentacji wewnętrznej lub odnotowujemy ich treść, a oryginały zwracamy pacjentowi. Dane o zdrowiu należą do tzw. szczególnych kategorii danych osobowych i podlegają specjalnej ochronie – przetwarzamy je wyłącznie w celu udzielania świadczeń zdrowotnych i z zachowaniem obowiązku tajemnicy zawodowej.

4) Inne dane zbierane w dokumentacji: Zgodnie z przepisami, w dokumentacji medycznej odnotowujemy także m.in. informacje o osobach upoważnionych przez pacjenta do dostępu do dokumentacji i do informacji o stanie zdrowia (jeśli pacjent takich wskaże), a także o wyrażeniu bądź niewyrażeniu zgód na określone działania (np. zgoda na udzielenie świadczenia zdrowotnego). Prosimy zatem pacjentów przy pierwszej wizycie o wskazanie, kogo ewentualnie upoważniają do dostępu do swojej dokumentacji lub informacji medycznych – imię i nazwisko oraz dane kontaktowe takiej osoby będą wówczas również przechowywane w Państwa kartotece. W dokumentacji mogą znaleźć się również dane takie jakinformacje o orzeczonym stopniu niepełnosprawności (jeśli ma to znaczenie dla procesu usprawniania) oraz inne informacje, które pacjent dobrowolnie przekaże personelowi w związku z leczeniem. Gromadzimy ponadto dane dotyczące płatności za usługi (np. odnotowanie faktu dokonania zapłaty, formy płatności, ewentualnie danych do faktury, itp.), jednak informacji tych nie zaliczamy co do zasady do dokumentacji medycznej a do dokumentacji finansowej.

Nie zbieramy żadnych danych, które nie są nam potrzebne – nie pytamy np. o sytuację rodzinną czy zawodową pacjenta, chyba że ma to bezpośredni związek ze stanem zdrowia (np. charakter pracy fizycznej przy rehabilitacji ortopedycznej). Nie prowadzimy również profilowania danych ani zautomatyzowanego podejmowania decyzji względem pacjentów w oparciu o ich dane osobowe – każdy plan terapii jest indywidualnie ustalany przez fizjoterapeutę.

Zgody pacjenta i klauzula informacyjna RODO

Actio przestrzega zasady, że pacjent powinien otrzymać pełną informację o przetwarzaniu jego danych osobowych przed rozpoczęciem udzielania świadczeń zdrowotnych. W związku z tym, podczas pierwszej wizyty przekazujemy pacjentowi do przeczytania niniejszą klauzulę informacyjną RODO i prosimy o podpisanie zgody/informacji. Dokument ten zawiera wszystkie wymagane informacje o celach, podstawach i zasadach przetwarzania danych, a podpis pacjenta potwierdza, że obowiązek informacyjny został zrealizowany we właściwym czasie (najpóźniej w momencie zbierania danych).

W praktyce, podczas pierwszej wizyty pacjent otrzymuje do wglądu i podpisu następujące formularze zgód:

1) Zgoda na udzielenie świadczenia zdrowotnego (zgoda na zabieg/terapię fizjoterapeutyczną): wymagana przepisami ustawy o prawach pacjenta w określonych sytuacjach (np. zabieg rehabilitacyjny wymaga zgody pacjenta – art. 16 ustawy o prawach pacjenta). Pacjent wyraża na piśmie zgodę na zaplanowaną terapię.

2) Potwierdzenie zapoznania się z niniejszą Polityką / klauzulą informacyjną RODO: pacjent swoim podpisem potwierdza, że został poinformowany o zasadach przetwarzania jego danych osobowych przez nasz podmiot leczniczy. Nie traktujemy tego jako odrębnej „zgody" na przetwarzanie danych (ponieważ, jak wyjaśniono, podstawą przetwarzania danych medycznych są głównie przepisy prawa i cele medyczne, a nie zgoda pacjenta), jednak podpis ten ma znaczenie dowodowe – pozwala nam wykazać, że dopełniliśmy obowiązku informacyjnego.

3) Zgoda na kontakt (opcjonalnie): na tym formularzu pacjent może wyrazić dobrowolnie zgodę na kontakt za pośrednictwem podanych danych (telefon, e-mail) w celach takich jak przypominanie o wizytach, informowanie o dostępności terminów, przekazywanie zaleceń w formie elektronicznej itp. (jeżeli nie chce opierać się wyłącznie na naszym uzasadnionym interesie). Brak zgody nie uniemożliwia korzystania z usług, a zgodę tę można w każdej chwili wycofać – służy ona jedynie ułatwieniu komunikacji zgodnie z preferencjami pacjenta. Uwaga: Zgoda na kontakt telefoniczny/mailowy nie jest wymagana, jeśli kontakt następuje w związku z koniecznością przekazania pacjentowi informacji dotyczących procesu leczenia (np. wyników badań) – taki kontakt mieści się w ramach udzielania świadczeń zdrowotnych i obowiązku lekarza/fizjoterapeuty, więc odrębna zgoda nie jest wymagana. Zgoda dotyczy więc raczej dodatkowej komunikacji wykraczającej poza niezbędne informacje medyczne.

Wymienione wyżej zgody i oświadczenia są gromadzone w formie papierowej i przechowywane w naszej siedzibie (ul. Słonecznikowa 4, Luboń) w sposób zapewniający ich poufność. Kopia podpisanej klauzuli informacyjnej RODO może być na życzenie wydana pacjentowi. Wycofanie zgody: Pacjent ma prawo w dowolnym momencie odwołać każdą udzieloną zgodę (np. zgodę na kontakt lub zgodę marketingową, jeśli była udzielona). Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej odwołaniem ani na przetwarzanie danych, które odbywa się na innej podstawie niż zgoda. Przykładowo, nawet po wycofaniu zgody na kontakt, nadal musimy – na podstawie przepisów prawa – prowadzić i przechowywać dokumentację medyczną Pani/Pana leczenia przez wymagany okres (patrz niżej). Nie jest zatem możliwe żądanie całkowitego usunięcia wszelkich danych medycznych przed upływem ustawowych okresów retencji, gdyż obowiązek ich dalszego przechowywania wynika z przepisów prawa i zasady ciągłości dokumentacji medycznej.

Odbiorcy danych – udostępnianie danych osobowych

Pani/Pana dane osobowe podlegają tajemnicy zawodowej i co do zasady nie są przekazywane osobom trzecim bez Pani/Pana zgody. W niektórych jednak sytuacjach jesteśmy zobowiązani lub uprawnieni udostępnić dane – zawsze w zgodzie z prawem i z zapewnieniem ich bezpieczeństwa. Potencjalni odbiorcy Pani/Pana danych osobowych to:

1) Podmioty przetwarzające dane w naszym imieniu (tzw. procesorzy): Są to zewnętrzne firmy lub osoby, którym powierzamy przetwarzanie danych na podstawie umowy, np.
2) dostawca i serwisant naszego systemu informatycznego do prowadzenia dokumentacji medycznej – obecnie korzystamy z platformy Finezjo, która służy do elektronicznej dokumentacji medycznej fizjoterapeuty. Finezjo jest aplikacją stworzoną w strukturach Krajowej Izby Fizjoterapeutów, utrzymywaną z funduszy samorządu fizjoterapeutów – dzięki temu jest bezpieczna i spełnia wszystkie wymogi prawne stawiane oprogramowaniu do dokumentacji medycznej. Firma obsługująca Finezjo (działająca na zlecenie KIF) ma dostęp do danych tylko w zakresie niezbędnym do zapewnienia działania systemu (np. wsparcie techniczne) i również jest zobowiązana do zachowania tajemnicy.
3) podmiot świadczący dla nas usługi księgowe – tj. biuro rachunkowe prowadzące naszą księgowość. Może ono mieć dostęp do danych na dokumentach finansowych (np. fakturach za usługi) w zakresie niezbędnym do realizacji obsługi księgowej. Biuro to działa na podstawie umowy powierzenia przetwarzania i ma obowiązek chronić powierzone dane.
4) ewentualnie inne firmy wspierające naszą działalność, którym zlecimy określone zadania wymagające przetwarzania danych. Każdorazowo zawieramy z takim podmiotem umowę powierzenia, która zobowiązuje go do przetwarzania danych wyłącznie w określonym celu i zgodnie z naszymi poleceniami oraz do zachowania standardów bezpieczeństwa wymaganych przez RODO.

5) Upoważniony personel medyczny: Dostęp do Pani/Pana danych (dokumentacji) mają wyłącznie osoby wykonujące u nas zawód medyczny (fizjoterapeuci) oraz ew. osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń, które zostały pisemnie upoważnione przez Administratora. Każda taka osoba działa z zachowaniem poufności – obowiązek ten utrzymuje się nawet po ustaniu współpracy. Osoby i podmioty uprawnione z mocy prawa: Na żądanie pacjenta lub jego przedstawiciela ustawowego udostępniamy kopię dokumentacji medycznej do wglądu lub wydajemy jej odpis – zgodnie z obowiązkiem prawnym (art. 27 ustawy o prawach pacjenta). Ponadto, jesteśmy zobowiązani udostępnić dokumentację lub informacje o stanie zdrowia innym podmiotom, jeżeli uprawnienie takie wynika z przepisów. Dotyczy to w szczególności:

6) innego podmiotu leczniczego lub lekarza – jeżeli pacjent zostanie tam skierowany lub gdy jest to niezbędne dla zapewnienia ciągłości leczenia bądź rehabilitacji (np. przekazanie informacji o dotychczasowym leczeniu nowemu specjaliście za zgodą pacjenta);
7) wskazanej przez pacjenta osoby upoważnionej – jeśli pacjent ustanowił taką osobę do dostępu do dokumentacji lub informacji (art. 26 ust. 1 ustawy o prawach pacjenta);
8) Narodowego Funduszu Zdrowia (NFZ) lub innego płatnika publicznego – o ile Actio współpracuje z NFZ (obecnie usługi świadczymy jako podmiot prywatny, więc NFZ nie finansuje naszych świadczeń; ten punkt ma zastosowanie, gdyby w przyszłości doszło do kontraktu z NFZ lub gdy pacjent korzysta z refundacji – wtedy NFZ może żądać danych potrzebnych do rozliczenia świadczeń);
9) organów władzy publicznej (np. Ministerstwo Zdrowia, organy nadzorcze) oraz samorządów zawodów medycznych – w zakresie niezbędnym do wykonywania przez nie ustawowych zadań, zwłaszcza nadzoru i kontroli (np. udostępnienie dokumentacji na żądanie Rzecznika Praw Pacjenta, konsultanta wojewódzkiego ds. fizjoterapii, w związku z postępowaniem wyjaśniającym lub kontrolą);
10) sądów, prokuratur oraz organów ścigania – na ich wiążące żądanie związane z toczącym się postępowaniem (np. postanowienie sądu o wydaniu dokumentacji w sprawie o odszkodowanie za błąd medyczny, postanowienie prokuratora w postępowaniu karnym, itp.);
11) organów rentowych (ZUS) oraz zespołów do spraw orzekania o niepełnosprawności – jeśli pacjent jest objęty takim postępowaniem, możemy zostać zobowiązani do przekazania danych o przebiegu rehabilitacji dla potrzeb orzeczenia rentowego lub o stopniu niepełnosprawności;
12) wojewódzkiej komisji do spraw orzekania o zdarzeniach medycznych – jeżeli pacjent złoży wniosek o odszkodowanie za tzw. zdarzenie medyczne, komisja ma prawo żądać dokumentacji dla oceny sprawy;
13) innych organów i instytucji wskazanych w odrębnych ustawach – o ile zgłoszą się do nas z podstawą prawną do uzyskania dokumentacji lub informacji (np. Policja na polecenie prokuratora, biegły sądowy za zgodą sądu, itd.).

W każdym przypadku udostępnienie odbywa się w granicach prawa – sprawdzamy podstawę prawną żądania oraz tożsamość wnioskodawcy. Dokumentacja medyczna udostępniana innym podmiotom może być przekazywana za pokwitowaniem odbioru i z zastrzeżeniem zwrotu (gdy przepisy tak przewidują). Podmioty lub osoby, którym udostępniamy dane na podstawie prawa, stają się niezależnymi administratorami tych danych (co oznacza, że ciąży na nich osobna odpowiedzialność za zgodne z prawem wykorzystanie tych informacji).

1) Podmioty realizujące płatności: Jeżeli za usługi rehabilitacyjne uiszczają Państwo opłatę przelewem bankowym lub kartą płatniczą, pewne dane (np. imię i nazwisko właściciela rachunku/karty, kwota i tytuł płatności) będą przetwarzane przez właściwe instytucje finansowe – banki, operatorów

płatności (np. firmę obsługującą terminal płatniczy w gabinecie). Są one odrębnymi administratorami tych danych, przetwarzającymi je w celu zrealizowania transakcji finansowej. Przykładowo, jeżeli pacjent płaci kartą, na wydruku terminala oraz w systemie rozliczeniowym znajdzie się część jego danych (choćby imię na karcie, jeśli jest spersonalizowana). Podobnie przy przelewie bankowym – na naszym wyciągu bankowym pojawi się imię i nazwisko nadawcy oraz ewentualnie adres, jeśli bank go dołącza. Dane te wykorzystujemy tylko do identyfikacji wpłaty. Uwaga: Administrator nie pobiera żadnych numerów kart ani innych wrażliwych danych finansowych – operacja płatnicza jest obsługiwana bezpośrednio przez bank/agentów rozliczeniowych, a my otrzymujemy jedynie potwierdzenie płatności.

2) Inne podmioty trzecie: Co do zasady nie przekazujemy danych osobowych pacjentów do państw trzecich (poza obszar EOG – Europejskiego Obszaru Gospodarczego) ani organizacjom międzynarodowym. Wszystkie nasze główne systemy (dokumentacja medyczna, poczta e-mail) są utrzymywane na serwerach zlokalizowanych w Polsce lub w Unii Europejskiej. W wyjątkowej sytuacji, gdy pacjent sam poprosi nas o przekazanie informacji np. lekarzowi za granicą lub gdy skontaktuje się z nami z zagranicznego adresu e-mail, takie przekazanie nastąpi wyłącznie na jego życzenie lub za zgodą. W razie ewentualnego wykorzystania narzędzi internetowych mogących skutkować transferem danych (np. komunikacja przez WhatsApp/Skype – której staramy się unikać w sprawach medycznych) uprzedzimy pacjenta o tym fakcie i uzyskamy akceptację.

Okres przechowywania danych (Polityka retencji)

Pani/Pana dane osobowe będą przechowywane przez okresy nie dłuższe niż konieczne do realizacji celów przetwarzania, z uwzględnieniem wymogów prawa dotyczących archiwizacji dokumentacji medycznej oraz dokumentów rozliczeniowych. Poniżej przedstawiamy kluczowe okresy retencji danych:

1) Dokumentacja medyczna pacjenta (historia choroby, karty zabiegów, wyniki badań, zgody, itp.) – przechowujemy przez 20 lat licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu w dokumentacji. Taki podstawowy okres archiwizacji wynika z art. 29 ust. 1 ustawy o prawach pacjenta. Przykład: jeśli ostatni wpis w dokumentacji miał miejsce w lipcu 2025 roku, dokumentacja będzie przechowywana do końca 2045 roku.

2) Dokumentacja medyczna dzieci małoletnich do 2. roku życia – jest przechowywana przez okres 22 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu. Ten wydłużony okres ma zabezpieczyć dostępność danych zdrowotnych dziecka na wypadek późniejszych potrzeb (np. oceny rozwoju). Przykład: dokumentacja niemowlęcia leczonego w 2025 roku będzie przechowywana do końca 2047 roku.

3) Wyjątkowe przypadki 30-letniego przechowywania: Jeżeli pacjent zmarł na skutek uszkodzenia ciała lub zatrucia, dokumentację medyczną związaną z jego leczeniem przechowujemy przez 30 lat od

końca roku, w którym nastąpił zgon. Również dokumentacja zawierająca dane niezbędne do monitorowania losów krwi i jej składników (nie dotyczy typowej działalności fizjoterapeutycznej, a raczej centrów krwiodawstwa) podlega 30-letniemu przechowywaniu. Nasza placówka co do zasady nie wchodzi w posiadanie takich danych, niemniej informujemy o tej regulacji dla pełności obrazu.

4) Badania obrazowe (RTG) wykonywane poza dokumentacją pisemną: W gabinecie fizjoterapii nie wykonujemy zdjęć rentgenowskich, jednak pacjenci często dostarczają nam płyty CD lub klisze z obrazami diagnostycznymi. Po wykorzystaniu ich do celów terapeutycznych zwracamy je pacjentowi, ewentualnie przechowując opis w dokumentacji. Gdyby jednak zdarzyło się, że posiadamy zdjęcie RTG poza dokumentacją medyczną pacjenta (np. pozostawione przypadkowo), mamy obowiązek przechowywać je 10 lat od końca roku, w którym wykonano zdjęcie, a następnie zniszczyć.

5) Skierowania na badania lub zlecenia lekarskie dot. pacjenta: Jeżeli pacjent przynosi skierowanie od lekarza (np. na zabiegi fizjoterapeutyczne), staje się ono częścią dokumentacji medycznej i będzie przechowywane tak długo, jak cała dokumentacja (20 lat). Jeśli jednak otrzymamy skierowanie, a pacjent nie podejmie u nas leczenia (nie zgłosi się), wówczas takie skierowanie (jako dokument zewnętrzny) możemy archiwizować przez okres 2 lat od końca roku, w którym miała być udzielona świadczenie, chyba że pacjent odbierze skierowanie wcześniej. Ta sytuacja jednak w praktyce nie występuje, bo skierowania niewykorzystane zwracamy pacjentowi lub odsyłamy do wystawcy.

6) Dane w dokumentacji finansowej (księgowej): Dokumenty zawierające dane osobowe związane z rozliczeniami (np. faktury imienne, ewidencja sprzedaży usług medycznych) przechowujemy 5 lat od końca roku podatkowego, którego dotyczą – zgodnie z wymogami prawa podatkowego. Przykład: faktura wystawiona w 2025 r. będzie przechowywana do końca 2030 r. W praktyce okres ten może być dłuższy niż 5 lat kalendarzowych, bo liczony jest od końca roku – np. faktury z początku 2025 r. przechowamy faktycznie prawie 6 lat. Po tym czasie dokumenty finansowe zostaną zniszczone, chyba że inne przepisy wymagałyby dłuższego przechowywania.

7) Okresy przedawnienia roszczeń: Dane potencjalnie potrzebne do obrony naszych praw lub dochodzenia roszczeń (np. w razie sporu sądowego) możemy zachować do czasu przedawnienia takich roszczeń. Zazwyczaj roszczenia pacjentów z tytułu udzielonych świadczeń zdrowotnych przedawniają się z upływem 3 lat od zdarzenia medycznego (lub od powzięcia o nim wiadomości), a w przypadku szkody na osobie – po 3 latach od dnia, w którym pacjent dowiedział się o szkodzie, nie dłużej jednak niż 10 lat od zdarzenia. Jeśli jednak roszczenie dotyczy małoletniego pacjenta, termin przedawnienia nie może skończyć się wcześniej niż z upływem 2 lat od uzyskania przez niego pełnoletności. W praktyce nasze 20-letnie przechowywanie dokumentacji medycznej w pełni pokrywa te potencjalne wydłużone terminy. Ewentualne kopie dokumentów dotyczących roszczeń (np. pisma procesowe) przechowujemy do czasu prawomocnego zakończenia sprawy i upływu terminów archiwizacji akt sprawy.

Po upływie wyżej wskazanych okresów dane osobowe zostaną trwale usunięte lub zanonimizowane. W przypadku dokumentacji medycznej – po upływie okresu archiwizacji niszczymy ją w sposób uniemożliwiający identyfikację pacjenta (np. poprzez profesjonalne spalanie lub rozdrobnienie). Zgodnie z przepisami, przed zniszczeniem dokumentacji medycznej możemy wydać ją pacjentowi, jego przedstawicielowi ustawowemu lub osobie przez niego upoważnionej – jeśli zainteresowana osoba zgłosi nam chęć odbioru starej dokumentacji, poinformujemy o terminie jej planowanego zniszczenia i umożliwimy odbiór oryginałów. W przypadku, gdyby nasza placówka zakończyła działalność, zapewnimy przekazanie dokumentacji medycznej podmiotowi przejmującemu nasze obowiązki lub właściwym organom, zgodnie z art. 30a ustawy o prawach pacjenta.

Prawa osoby, której dane dotyczą (prawa pacjenta w zakresie danych osobowych)

W związku z przetwarzaniem Pani/Pana danych osobowych, przysługują następujące prawa wynikające z RODO oraz innych przepisów o ochronie danych. Każde z tych praw można wykonać, kontaktując się z Administratorem (dane kontaktowe podano wyżej). Należy jednak pamiętać, że charakter świadczeń zdrowotnych i przepisy szczególne mogą w pewnych sytuacjach te prawa ograniczać. Prawa pacjenta dotyczące danych to:

1) Prawo dostępu do danych – ma Pani/Pan prawo uzyskać informację, czy przetwarzamy Pani/Pana dane, a jeśli tak, to jakie to dane, w jakim celu, jak długo będziemy je przechowywać, komu zostały ujawnione itp. (są to informacje zawarte w niniejszej polityce). Ma też Pan/Pani prawo otrzymać kopię swoich danych. Najczęściej realizuje się to poprzez wydanie kopii dokumentacji medycznej na żądanie, co jest również odrębnym prawem pacjenta wynikającym z ustawy o prawach pacjenta (art. 23 – prawo dostępu do dokumentacji). Kopia dokumentacji udostępniana jest bezpłatnie.

2) Prawo sprostowania danych – ma Pani/Pan prawo żądać poprawienia swoich danych, jeśli są nieaktualne, nieścisłe lub niekompletne. W kontekście dokumentacji medycznej prawo to podlega ograniczeniom: dokumentacja odzwierciedla stan faktyczny w chwili wpisu, więc co do zasady nie zmieniamy retrospektywnie wpisów medycznych (błędne wpisy koryguje się poprzez adnotacje, a nie poprzez usuwanie). Możemy natomiast sprostować dane administracyjne, np. błędny adres czy literówkę w nazwisku.

3) Prawo do usunięcia danych („prawo do bycia zapomnianym") – prawo to nie ma bezwzględnego zastosowania do danych medycznych. Zgodnie z art. 17 RODO może Pani/Pan zażądać usunięcia danych, jeśli np. cofnięto zgodę i brak innej podstawy przetwarzania lub dane nie są już potrzebne do celów, dla których zostały zebrane. Należy jednak podkreślić, że w przypadku dokumentacji medycznej istnieje odrębny obowiązek prawny jej przechowywania przez określony czas i żądanie usunięcia nie może zostać uwzględnione w odniesieniu do danych, które musimy zachować na mocy prawa. Innymi słowy, nie można domagać się wcześniejszego usunięcia (zniszczenia) dokumentacji

medycznej przed upływem wymaganego 20-letniego okresu, nawet jeśli pacjent przestał korzystać z naszych usług. Prawo do usunięcia może mieć zastosowanie np. do danych przetwarzanych na podstawie zgody w celach marketingowych – takich danych na żądanie już nie będziemy wykorzystywać. Podsumowując, prawo do usunięcia nie dotyczy danych przetwarzanych na podstawie obowiązku prawnego lub w ramach sprawowania opieki zdrowotnej. Gdy tylko ustawowy czas przechowywania minie – dane zostaną usunięte zgodnie z przyjętymi procedurami.

4) Prawo do ograniczenia przetwarzania – w pewnych sytuacjach ma Pani/Pan prawo zażądać, abyśmy tymczasowo wstrzymali się z aktywnym przetwarzaniem danych (np. ich wykorzystaniem), poza ich przechowywaniem. Takie sytuacje to np.: kwestionowanie prawidłowości danych (na czas sprawdzenia można żądać ograniczenia), przetwarzanie jest niezgodne z prawem, ale pacjent nie chce usunięcia tylko ograniczenia, lub Administrator nie potrzebuje już danych, ale pacjent potrzebuje ich do ustalenia lub obrony roszczeń. W praktyce w ochronie zdrowia prawo to ma ograniczone zastosowanie, ale np. jeśli pacjent zakwestionuje poprawność danych kontaktowych i zażąda zaprzestania ich używania, dostosujemy się do tego.

5) Prawo do przenoszenia danych – przysługuje w odniesieniu do takich danych, które pacjent sam dostarczył Administratorowi, są przetwarzane na podstawie zgody lub umowy oraz w sposób zautomatyzowany (art. 20 RODO). Może Pan/Pani zażądać, abyśmy wydali w ustrukturyzowanym formacie (np. CSV) dane osobowe, które spełniają te kryteria – albo przekazali te dane bezpośrednio innemu wskazanemu administratorowi, o ile jest to technicznie możliwe. Należy zaznaczyć, że dane medyczne w dokumentacji nie podlegają przenoszeniu na żądanie pacjenta, ponieważ podstawą ich przetwarzania nie jest zgoda ani umowa, tylko obowiązek prawny i przepisy szczególne. Natomiast dane kontaktowe podane przy rejestracji wizyty, dane podane w formularzu zgody RODO czy dane potrzebne do wystawienia faktury – mogą podlegać przeniesieniu (możemy je udostępnić w formie elektronicznej na życzenie). W praktyce jednak częściej realizuje się prawo dostępu do dokumentacji medycznej niż prawo do przeniesienia, które dotyczy głównie sektora usług cyfrowych.

6) Prawo do sprzeciwu – ma Pani/Pan prawo wnieść sprzeciw wobec przetwarzania swoich danych, *jeśli odbywa się ono na podstawie naszego prawnie uzasadnionego interesu lub w interesie publicznym* (art. 21 RODO). Sprzeciw musi być uzasadniony Pani/Pana szczególną sytuacją. Wówczas my musimy uwzględnić sprzeciw, chyba że wykażemy istnienie ważnych, prawnie uzasadnionych podstaw nadrzędnych wobec Pani/Pana interesów, praw i wolności (co w kontekście danych medycznych może oznaczać np. obowiązek dalszego przetwarzania ze względu na zdrowie publiczne). Uwaga: Prawo sprzeciwu nie przysługuje wobec przetwarzania, które jest niezbędne do wykonania świadczenia zdrowotnego czy obowiązku prawnego (czyli nie można sprzeciwić się przetwarzaniu danych w dokumentacji medycznej, gdyż bez tego nie da się kontynuować leczenia i spełnić wymogów prawa). Natomiast sprzeciw może dotyczyć np. wykorzystania danych kontaktowych na

podstawie naszego uzasadnionego interesu – jeśli pacjent uzna, że nie życzy sobie żadnego kontaktu z naszej strony poza absolutnie koniecznym, może zgłosić sprzeciw, a my rozpatrzymy, czy możemy zaprzestać takiego przetwarzania (co do przypomnień o wizytach opieraliśmy się na naszym interesie, ale jeśli pacjent sobie nie życzy, uszanujemy to i nie będziemy wysyłać przypomnień). Sprzeciw może dotyczyć też przetwarzania danych w celach ewentualnego ustalania roszczeń – pacjent może np. sprzeciwić się, byśmy przechowywali jego dane dłużej w celu naszej ochrony prawnej. Jeśli nie wykażemy nadrzędnych podstaw (a zwykle po zakończeniu leczenia i upływie wymaganego okresu nie będziemy mieli już silnych podstaw), takie żądanie uwzględnimy.

7) Prawo wycofania zgody – jeśli jakiekolwiek Pani/Pana dane są przetwarzane na podstawie zgody, ma Pani/Pan prawo tę zgodę w dowolnym momencie wycofać (patrz wyżej punkt Zgody pacjenta). Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano wcześniej na jej podstawie, ale zobowiązuje nas do zaprzestania dalszego przetwarzania danych w zakresie objętym tą zgodą. W szczególności, jeśli pacjent wycofa zgodę na kontakt telefoniczny/mailowy, zaprzestaniemy używania tych kanałów komunikacji (chyba że istnieje inna podstawa prawna, np. powiadomienie o zagrożeniu zdrowia pacjenta – wówczas i tak będziemy uprawnieni skontaktować się, ale to wynika z przepisów, nie z zgody). Wycofanie zgody nie skutkuje usunięciem danych, które przetwarzamy na innych podstawach prawnych – np. nie powoduje to wykreślenia pacjenta z dokumentacji medycznej, gdyż obowiązek jej prowadzenia nadal trwa.

8) Prawo do wniesienia skargi do organu nadzorczego – jeśli uważa Pani/Pan, że przetwarzamy dane niezgodnie z prawem, ma Pani/Pan prawo złożyć skargę do organu nadzorującego przestrzeganie przepisów o ochronie danych osobowych. W Polsce organem tym jest Prezes Urzędu Ochrony Danych Osobowych (PUODO). Aktualne dane kontaktowe Urzędu: ul. Stawki 2, 00-193 Warszawa; infolinia: 606-950-000; email: kancelaria@uodo.gov.pl. Zachęcamy jednak w pierwszej kolejności do kontaktu z nami – postaramy się wyjaśnić wszelkie wątpliwości i rozwiązać problem polubownie.

Chcemy podkreślić, że szanujemy prawa pacjentów wynikające z RODO i dokładamy starań, aby ułatwić ich realizację. Niemniej, musimy przy tym przestrzegać przepisów szczególnych dotyczących dokumentacji medycznej oraz praw pacjenta, które czasem zawężają możliwość spełnienia pewnych żądań (jak wyjaśniono powyżej). Każdy wniosek w sprawie Pani/Pana danych rozpatrzymy indywidualnie i udzielimy odpowiedzi bez zbędnej zwłoki – najpóźniej w terminie miesiąca od otrzymania żądania.

Zabezpieczenia i procedury ochrony danych

W Actio wdrożyliśmy odpowiednie techniczne i organizacyjne środki bezpieczeństwa danych osobowych, zgodnie z art. 32 RODO oraz wytycznymi branżowymi. Chronimy zarówno papierową dokumentację medyczną, jak i dane przechowywane w systemach informatycznych. Najważniejsze elementy naszego systemu ochrony danych to:

1) Dostęp do danych pacjentów mają wyłącznie osoby upoważnione – zatrudniony personel medyczny Actio oraz ewentualnie upoważnieni pracownicy pomocniczy. Każda osoba dopuszczona do danych jest zobowiązana do zachowania poufności (podpisuje stosowne oświadczenie) i przechodzi szkolenie z ochrony danych. Nadawanie i odbieranie uprawnień odbywa się na podstawie pisemnych upoważnień Administratora i jest odnotowywane w prowadzonym przez nas rejestrze osób upoważnionych. W przypadku systemu informatycznego Finezjo – każdy użytkownik posiada indywidualne konto chronione hasłem, a dostęp do systemu jest zabezpieczony certyfikatem i szyfrowanym połączeniem SSL. Administrator Systemu Informatycznego (ASI) dba o bieżące utrzymanie bezpieczeństwa systemu – w naszym przypadku rolę tę pełnią specjaliści techniczni platformy Finezjo we współpracy z KIF.

2) Używamy sprzętu komputerowego zabezpieczonego hasłami oraz aktualnym oprogramowaniem antywirusowym i firewall. System Finezjo działa w chmurze, ale dostęp do niego wymaga uwierzytelnienia i jest monitorowany. Regularnie aktualizujemy oprogramowanie systemowe i medyczne do najnowszych wersji w celu eliminacji znanych podatności. Wykonujemy również okresowe kopie zapasowe kluczowych danych (baza dokumentacji medycznej jest zabezpieczana przez Finezjo – platforma ta gwarantuje tworzenie backupów zgodnie z wymogami KIF). Nasze komputery i urządzenia mobilne wykorzystywane do pracy z danymi pacjentów są zabezpieczone przed dostępem osób trzecich (hasła, szyfrowanie dysków). Nie przechowujemy danych medycznych na prywatnych nośnikach lub w niezabezpieczonych aplikacjach.

3) Dokumentacja papierowa (np. zgoda pacjenta) jest przechowywana w zamkniętych szafach w pomieszczeniach dostępnych wyłącznie dla personelu.. Dokumenty zawierające dane osobowe nie są pozostawiane na widoku osób postronnych – np. podczas wizyty tylko terapeuta ma wgląd do karty pacjenta. Stosujemy zasadę czystego biurka – po zakończonej pracy dokumenty są chowane do szaf, a nośniki elektroniczne wyjmowane z komputerów.

4) Każde podejrzenie naruszenia bezpieczeństwa danych niezwłocznie zgłaszamy Administratorowi, który dokonuje analizy ryzyka. W razie potrzeby informujemy również właściwy organ nadzorczy (PUODO) o naruszeniu – jeśli istnieje taka ustawowa konieczność (np. gdy doszło do utraty danych medycznych). Jeżeli charakter naruszenia mógłby powodować wysokie ryzyko dla praw lub wolności pacjenta – poinformujemy także Pacjenta o zaistniałym incydencie i o podjętych działaniach ochronnych. Wszystkie zdarzenia i podjęte czynności dokumentujemy, zgodnie z zasadą rozliczalności RODO.

5) Polityka ochrony danych jest okresowo przeglądana i w razie potrzeby aktualizowana, aby spełniać zmieniające się wymogi prawne i technologiczne.

6) Prowadzimy też rejestr upoważnień i ewidencję osób uprawnionych do przetwarzania danych, rejestr zgód pacjentów (w dokumentacji pacjenta odnotowujemy fakt podpisania zgody na świadczenie i klauzuli informacyjnej), a także rejestr ewentualnych naruszeń ochrony danych. Taka dokumentacja wewnętrzna pozwala nam wykazać spełnienie obowiązków RODO i szybko reagować na wszelkie zdarzenia.

Postanowienia końcowe

Niniejsza Polityka obowiązuje w Actio od dnia podpisania i publikacji na stronie internetowej. Zastrzegamy sobie prawo do wprowadzania zmian w treści Polityki, jeśli będzie to konieczne ze względu na zmiany przepisów lub naszych procesów – o każdej istotnej zmianie poinformujemy pacjentów poprzez ogłoszenie w naszej siedzibie oraz aktualizację informacji na stronie www.

Polityka została przyjęta i ogłoszona dnia 19.09.2025r. Aktualna wersja dokumentu jest zawsze dostępna w siedzibie Actio oraz na naszej stronie internetowej.