

Ochrona danych osobowych (RODO)

- **Administrator danych:** Administratorem danych osobowych Pacjenta przekazanych w związku z korzystaniem z usługi jest Usługodawca – lek. Szymon Manasterski prowadzący działalność gospodarczą pod firmą Szymon Manasterski Ortopedia i Anty-Aging, z adresem do korespondencji: ul. Mikołaja Reja 82 lok. 2B, 50-343 Wrocław, e-mail: [email kontaktowy do ABI/IOD lub Usługodawcy].
- **Zakres zbieranych danych:** W celu realizacji usługi, Usługodawca przetwarza następujące kategorie danych osobowych Pacjenta:
 - **Dane identyfikacyjne i kontaktowe** – imię, nazwisko, adres e-mail, numer telefonu, adres do wysyłki (jeśli zamówiono wersję papierową), ewentualnie PESEL lub data urodzenia (jeśli wymagane do jednoznacznej identyfikacji Pacjenta w dokumentacji).
 - **Dane medyczne (szczególne kategorie danych)** – informacje o stanie zdrowia Pacjenta, przebiegu leczenia, diagnozach, wykonanych zabiegach, zażywanych lekach itp., zawarte w przekazanej dokumentacji medycznej oraz wynikające z opisu przypadku. Mogą to być m.in. historie choroby, epikryzy, wyniki badań diagnostycznych, konsultacje lekarskie, orzeczenia o niepełnosprawności lub uszczerbku na zdrowiu.
 - **Inne dane podane dobrowolnie** – np. dodatkowe wyjaśnienia czy informacje przekazane przez Pacjenta w korespondencji dotyczącej zlecenia, które mogą zawierać dane osobowe (w tym potencjalnie dane wrażliwe).
- **Cele przetwarzania:** Dane osobowe Pacjenta będą przetwarzane wyłącznie w następujących celach:
 - **Realizacja umowy o świadczenie usługi** – tj. w celu przyjęcia zamówienia, komunikacji z Pacjentem, sporządzenia opinii medycznej na zlecenie Pacjenta oraz dostarczenia jej Pacjentowi. Obejmuje to także podjęcie niezbędnych działań przed zawarciem umowy i w jej trakcie (np. wycena, weryfikacja dokumentów, obsługa płatności). Podanie danych osobowych jest dobrowolne, jednak **niezbędne do zawarcia i wykonania umowy** – ich niepodanie uniemożliwiłoby realizację usługi.
 - **Wypełnienie obowiązków prawnych ciążących na Usługodawcy** – np. obowiązek prowadzenia i przechowywania dokumentacji medycznej Pacjenta (wynikający z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta), obowiązki podatkowe i rachunkowe (wystawienie faktury, przechowywanie dokumentów księgowych), obowiązki archiwizacyjne.
 - **Ustalenie, dochodzenie lub obrona roszczeń prawnych** – przetwarzanie danych może być konieczne w celu ewentualnej obrony przed roszczeniami

Pacjenta lub dochodzenia roszczeń przez Usługodawcę (np. w przypadku sporu co do jakości usługi, konieczności wykazania należytego wykonania zobowiązania lub rozstrzygania reklamacji). Jest to tzw. prawnie uzasadniony interes administratora danych.

- **Cele kontaktowe związane z obsługą klienta** – dane kontaktowe (telefon, e-mail) mogą być wykorzystywane do przekazywania Pacjentowi informacji o statusie realizacji usługi, powiadomień o wysyłce, czy udzielenia odpowiedzi na pytania Pacjenta. (Usługodawca **nie** wykorzystuje danych Pacjenta do celów marketingowych ani nie wysyła niezamówionych treści marketingowych – kontakt odbywa się wyłącznie w związku z realizacją konkretnej usługi.)
- **Obsługa płatności elektronicznych** – dane osobowe niezbędne do realizacji płatności (w szczególności imię i nazwisko, adres e-mail, kwota transakcji, numer zamówienia oraz inne dane wymagane do realizacji płatności) mogą być przekazywane operatorowi płatności **Autopay S.A.** z siedzibą w Sopocie w celu obsługi płatności elektronicznych, weryfikacji transakcji, zapobiegania nadużyciom oraz realizacji obowiązków wynikających z przepisów prawa.
- **Podstawy prawne przetwarzania:** Przetwarzanie danych osobowych Pacjenta odbywa się zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (**RODO**) oraz polskimi przepisami o ochronie danych osobowych. W zależności od kategorii danych i celu, zastosowanie mają następujące podstawy prawne:
 - Art. 6 ust. 1 lit. b RODO – przetwarzanie jest niezbędne do **wykonania umowy**, której stroną jest Pacjent, lub do podjęcia działań na żądanie Pacjenta przed zawarciem umowy. Ta podstawa dotyczy wszelkich danych zwykłych potrzebnych do realizacji usługi (np. dane kontaktowe, identyfikacyjne).
 - Art. 9 ust. 2 lit. h RODO – przetwarzanie szczególnych kategorii danych (danych o zdrowiu) jest niezbędne do **celów diagnostyki medycznej, zapewnienia opieki zdrowotnej lub leczenia** lub zarządzania systemami opieki zdrowotnej – w zakresie, w jakim Usługodawca świadczy usługę medyczną (wydanie opinii stanowi formę działania medycznego w interesie Pacjenta). Alternatywnie lub dodatkowo może mieć zastosowanie art. 9 ust. 2 lit. a RODO – Pacjent **wyraża wyraźną zgodę** na przetwarzanie swoich danych medycznych w celu sporządzenia opinii (zgodę taką Pacjent wyraża poprzez dobrowolne przekazanie dokumentacji medycznej i zlecenie usługi; zgodę tę może w każdej chwili wycofać, jednak wycofanie zgody uniemożliwi dalszą realizację usługi).
 - Art. 6 ust. 1 lit. c RODO – przetwarzanie jest niezbędne do **wypełnienia obowiązku prawnego** ciążącego na administratorze (np. obowiązki przechowywania dokumentacji medycznej i udostępniania jej uprawnionym

osobom na podstawie ustawy o prawach pacjenta, obowiązki rachunkowe na podstawie ustawy o rachunkowości itp.).

- Art. 6 ust. 1 lit. f RODO – przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów** realizowanych przez administratora (Usługodawcę), takich jak obrona przed ewentualnymi roszczeniami, dochodzenie należności za wykonaną usługę czy zapewnienie bezpieczeństwa informacji. Tę podstawę stosuje się pomocniczo dla danych, które nie są objęte szczególnym obowiązkiem prawnym lub nie są ewidentnie niezbędne do wykonania umowy, ale ich przetwarzanie jest uzasadnione koniecznością ochrony praw Usługodawcy (np. przechowywanie dowodów korespondencji z Pacjentem na wypadek sporu).
- Art. 9 ust. 2 lit. f RODO – w zakresie danych medycznych może znaleźć zastosowanie podstawa przetwarzania **“w celu ustalenia, dochodzenia lub obrony roszczeń”** (np. gdyby dane zdrowotne musiały zostać wykorzystane w postępowaniu sądowym dotyczącym jakości usługi).
- **Okres przechowywania danych:** Dane osobowe Pacjenta będą przechowywane tylko przez okres niezbędny do realizacji wyżej wymienionych celów. W praktyce:
 - Dane zebrane w celu realizacji umowy (formularz zamówienia, treść opinii, dokumentacja medyczna) będą przechowywane przez czas wykonywania usługi, a następnie archiwizowane wraz z dokumentacją medyczną przez okres **20 lat** od końca roku kalendarzowego, w którym opinia została wydana, zgodnie z wymogami przechowywania dokumentacji medycznej. Po upływie tego okresu dokumentacja zostanie zniszczona w sposób gwarantujący ochronę danych (chyba że przepisy szczególne będą wymagały dłuższego przechowywania w określonych sytuacjach, np. 30 lat w razie zgonu Pacjenta na skutek uszczerbku na zdrowiu).
 - Dane potrzebne do celów podatkowych/księgowych (np. dane na fakturze) będą przechowywane przez okres wymagany przez przepisy podatkowe (obecnie 5 lat od końca roku podatkowego).
 - Dane kontaktowe (e-mail, telefon) oraz korespondencja będą przechowywane co najmniej do czasu dostarczenia usługi i zakończenia ewentualnej obsługi posprzedażowej (reklamacje), a po tym czasie mogą być przechowywane w celach archiwalnych (np. dowodowych) przez okres przedawnienia roszczeń cywilnoprawnych (co do zasady 6 lat, a w przypadku roszczeń konsumenckich 6 lat).
 - Jeśli przetwarzanie odbywa się na podstawie zgody Pacjenta (np. w zakresie danych medycznych wyłącznie na podstawie zgody), dane te będą przetwarzane do czasu wycofania zgody przez Pacjenta. Wycofanie zgody nie

wpływa na zgodność z prawem przetwarzania dokonanego wcześniej, ale może uniemożliwić dalszą realizację usługi (skutkując rozwiązaniem umowy).

- **Odbiorcy danych:** Dane osobowe Pacjenta mogą być przekazywane innym podmiotom wyłącznie w związku z realizacją powyższych celów i na podstawie stosownych umów lub przepisów prawa. Odbiorcami danych mogą być w szczególności:
 - **Podmioty uczestniczące w realizacji usługi** – np. firma kurierska lub poczta (dostawa przesyłki z opinią – przekazywane dane adresowe odbiorcy), dostawca hostingu lub usług IT obsługujący system informatyczny Usługodawcy (dostęp do danych w ramach utrzymania systemu), operator systemu płatności online (dane transakcyjne), księgowość Usługodawcy (dokumenty finansowe z danymi klienta). Wszystkie te podmioty przetwarzają dane na podstawie umowy z Usługodawcą i tylko zgodnie z jego poleceniami (umowy powierzenia przetwarzania danych) bądź jako niezależni administratorzy jeśli wynika to z ich roli (np. operator płatniczy). W przypadku **realizacji płatności elektronicznych** odbiorcą danych niezbędnych do przeprowadzenia transakcji jest **Autopay S.A.** z siedzibą w Sopocie, świadcząca usługi płatnicze. Autopay przetwarza dane jako odrębny administrator danych osobowych w zakresie niezbędnym do realizacji transakcji płatniczej, zgodnie z obowiązującymi przepisami prawa oraz własną polityką prywatności.
 - **Organy publiczne uprawnione z mocy prawa** – np. sądy, prokuratura, policja, rzecznik praw pacjenta, jeżeli zwrócą się o udostępnienie danych w oparciu o stosowne przepisy (np. w toku postępowania) – Usługodawca udostępni dane tylko w zakresie obowiązku prawnego.
 - **Personel medyczny lub konsultanci** – co do zasady opinię sporządza osobiście Usługodawca. W razie potrzeby może on jednak skonsultować się z innym lekarzem specjalistą (zwłaszcza gdy sprawa tego wymaga – np. opinia w zakresie innej specjalizacji medycznej). Taka konsultacja odbywać się będzie z poszanowaniem tajemnicy lekarskiej – jeśli zajdzie konieczność przekazania danych innemu lekarzowi, nastąpi to za zgodą Pacjenta albo w formie anonimizowanej (bez danych identyfikujących Pacjenta).
 - Inne podmioty mogące mieć dostęp do danych Pacjenta to np. dostawcy usług poczty elektronicznej (dane w wiadomościach e-mail), firmy serwisujące sprzęt lub oprogramowanie (incydentalny dostęp w razie awarii), przy czym w takich przypadkach dostęp jest jednorazowy i kontrolowany przez Usługodawcę. Dane Pacjenta **nie będą przekazywane** do państwa trzeciego (poza obszar EOG) ani do organizacji międzynarodowych, chyba że Pacjent

sam zażyczy sobie wysyłki dokumentów na adres poza EOG (wtedy nastąpi to na życzenie Pacjenta).

- **Prawa Pacjenta w odniesieniu do danych:** Pacjentowi, jako osobie, której dane dotyczą, przysługują następujące prawa:
 - **Prawo dostępu do danych** – Pacjent ma prawo uzyskać informację, czy Usługodawca przetwarza jego dane, a jeżeli tak, to jakie to są dane i w jakim celu, oraz otrzymać kopię swoich danych (w tym kopię dokumentacji medycznej przechowywanej przez Usługodawcę, zgodnie z prawem pacjenta do dokumentacji medycznej).
 - **Prawo sprostowania (poprawienia) danych** – jeśli dane posiadane przez Usługodawcę są nieprawidłowe lub niekompletne, Pacjent ma prawo żądać ich poprawienia lub uzupełnienia.
 - **Prawo usunięcia danych** (“prawo do bycia zapomnianym”) – w przypadkach przewidzianych przez RODO (art. 17), np. gdy dane nie są już potrzebne do celów, w których zostały zebrane, Pacjent może żądać usunięcia swoich danych osobowych. Należy jednak pamiętać, że uprawnienie to może zostać ograniczone przez przepisy zobowiązujące Usługodawcę do przechowywania dokumentacji medycznej przez określony czas – w takim zakresie żądanie usunięcia może zostać zrealizowane dopiero po upływie okresów archiwizacji wymaganych prawem.
 - **Prawo ograniczenia przetwarzania** – Pacjent może zażądać, by Usługodawca czasowo wstrzymał się z operacjami na danych (poza ich przechowywaniem) w sytuacjach, gdy np. kwestionuje prawidłowość danych lub wniósł sprzeciw (na czas rozpatrzenia).
 - **Prawo do przenoszenia danych** – w zakresie danych przetwarzanych na podstawie zgody lub umowy (art. 6 ust.1 lit. a lub b RODO) Pacjent ma prawo otrzymać od Usługodawcy swoje dane osobowe w ustrukturyzowanym formacie nadającym się do odczytu maszynowego lub zażądać przesłania tych danych innemu administratorowi (o ile jest to technicznie możliwe).
 - **Prawo sprzeciwu** – Pacjent ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania swoich danych opartego na prawie uzasadnionym interesie administratora (art. 6 ust.1 lit. f RODO), z przyczyn związanych z jego szczególną sytuacją. Wówczas Usługodawca oceni, czy – ze względu na ważne prawnie uzasadnione podstawy – może dalej przetwarzać te dane, czy też sprzeciw skutkuje zaprzestaniem przetwarzania. W przypadku danych przetwarzanych na potrzeby marketingu bezpośredniego sprzeciw jest skuteczny z chwilą jego wniesienia – jednak jak zaznaczono wyżej, Usługodawca nie prowadzi marketingu w oparciu o dane Pacjenta.

- **Prawo wycofania zgody** – w zakresie, w jakim przetwarzanie odbywa się na podstawie zgody (np. zgody na przetwarzanie danych medycznych, jeśli była wymagana), Pacjent ma prawo w dowolnym momencie wycofać swoją zgodę. Wycofanie zgody nie wpływa na legalność przetwarzania dokonanego przed wycofaniem. Należy jednak mieć na uwadze, że wycofanie zgody na przetwarzanie danych niezbędnych do wykonania usługi może skutkować niemożliwością jej dalszej realizacji (co jest równoznaczne z rozwiązaniem umowy na żądanie Pacjenta).
- **Realizacja praw:** W celu realizacji powyższych praw Pacjent może skontaktować się z Usługodawcą (Administratorem danych) – dane kontaktowe: [adres e-mail do spraw danych osobowych] lub pisemnie na adres siedziby. Usługodawca udzieli odpowiedzi na zgłoszenie bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania (termin może zostać przedłużony do 2 miesięcy w skomplikowanych przypadkach, o czym Pacjent zostanie poinformowany).
- **Prawo wniesienia skargi:** Jeżeli Pacjent uzna, że przetwarzanie jego danych osobowych narusza przepisy o ochronie danych, ma prawo wnieść **skargę do Prezesa Urzędu Ochrony Danych Osobowych** (adres: ul. Stawki 2, 00-193 Warszawa). Skarga może zostać złożona w trybie przewidzianym przepisami o postępowaniu przed UODO.
- **Bezpieczeństwo danych:** Usługodawca zapewnia, że wdrożył odpowiednie środki techniczne i organizacyjne, aby zabezpieczyć dane Pacjenta przed dostępem osób nieuprawnionych, utratą czy bezprawnym wykorzystaniem. Dane medyczne są objęte **tajemnicą lekarską**, której Usługodawca jako lekarz ma obowiązek przestrzegać zgodnie z art. 40 ustawy o zawodach lekarza oraz innymi przepisami. Wszyscy współpracownicy i podmioty, którym powierzane są dane, są również zobowiązani do zachowania poufności.