POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejsza polityka ochrony danych określa zasady przetwarzania Danych Osobowych przez Marcin Maksymiec („**Administrator**").
2. Administrator przetwarza Dane Osobowe z zachowaniem zasad zgodności z prawem, rzetelności i przejrzystości, w tym w szczególności zgodnie z przepisami Rozporządzenia 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 („RODO") oraz przepisami prawa krajowego.
3. Administrator wykonuje działalność leczniczą na podstawie ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej i przetwarza Dane Osobowe:
    1) Pacjentów:
        a. w celach zdrowotnych, związanych z udzielaniem świadczeń zdrowotnych, w tym prowadzeniem i udostępnianiem dokumentacji medycznej – na podstawie art. 9 ust. 2 lit h RODO oraz art. 6 ust. 1 lit. b i c RODO;
        b. w celach związanych ze zrealizowaniem ciążących na nim obowiązków związanych z prowadzeniem, przechowywaniem i udostępnianiem dokumentacji medycznej – na podstawie ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta oraz art. 6 ust. 1 lit. c RODO;
        c. w celu dochodzenia zapłaty na usługi, jeśli taka zapłata nie zostanie uiszczona – na podstawie art. 6 ust. 1 lit. f RODO;
        d. w celu ochrony przed roszczeniami oraz w celu dochodzenia innych roszczeń niewskazanych w punkcie c) powyżej, a także w celu zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;
        e. w celu ochrony przed roszczeniami oraz w celu dochodzenia roszczeń oraz zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;
        f. w celach marketingowych oraz innych niewymienionych w lit. a i b – na podstawie zgody Pacjenta, zgodnie z art. 6 ust 1 lit. a RODO;
    2) innych osób:
        a. w zakresie zawartych umów, w celu zapewnienia ich realizacji – na podstawie art. 6 ust. 1 lit. b RODO;
        b. w celu zapewnienia procesu zarządzania przedsiębiorstwem Administratora oraz zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;
        c. w pozostałych celach – na podstawie zgody osoby, której dane dotyczą, zgodnie z art. 6 ust 1 lit. a RODO, o ile nie zachodzą inne podstawy przetwarzania Danych Osobowych, o których mowa w art. 6 oraz art. 9 RODO.
4. Administrator zapewnia bezpieczeństwo Danych Osobowych w tym ochronę przed ich niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez:
    1) stosowanie właściwej dokumentacji przetwarzania danych osobowych;
    2) dopuszczenie do przetwarzania Danych Osobowych wyłącznie osób upoważnionych przez Administratora na piśmie oraz osób zobowiązanych do zachowania tajemnicy zawodowej w związku z wykonywanym zawodem

medycznym (fizjoterapeuci, lekarze) chyba, że upoważnienie do przetwarzania danych osobowych wynika wprost z przepisów prawa powszechnie obowiązującego;

3) powierzanie przetwarzania Danych Osobowych wyłącznie na podstawie odrębnych umów o powierzenie Przetwarzania Danych Osobowych;
4) prowadzenie i udostępnianie dokumentacji medycznej zgodnie z przepisami prawa powszechnie obowiązującego w tym m.in. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania;
5) szkolenia Personelu z zakresu zasad Przetwarzania Danych Osobowych;
6) prowadzenie rejestru czynności przetwarzania Danych Osobowych;
7) monitorowanie naruszeń ochrony Danych Osobowych i prowadzenie rejestru naruszeń;
8) stosowanie środków technicznych ochrony Danych Osobowych, w szczególności:
    a. ochrony budynku i systemu alarmowego;
    b. zabezpieczeń antywłamaniowych w stolarce drzwiowej i okiennej;
    c. stosowanie szaf i pojemników zapewniających należyty poziom bezpieczeństwa Danych Osobowych;
    d. zabezpieczeń teleinformatycznych (m.in. ograniczony dostęp do systemów, oprogramowanie antywirusowe, firewall, certyfikaty SSL na stronie internetowej).

5. Administrator nie jest zobowiązany do przeprowadzenia oceny skutków dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO.
6. Administrator nie jest zobowiązany do wyznaczenia inspektora ochrony danych, o którym mowa w art. 37 ust. 1 RODO.
7. Administrator zobowiązany jest do:
    1) prowadzenia i udostępniania dokumentacji medycznej Pacjentów zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz jej zabezpieczenia przed utratą lub zniszczeniem;
    2) w przypadku udostępniania dokumentacji medycznej – do rzetelnej weryfikacji tożsamości osoby, której dane są udostępniane;
    3) w przypadku udostępniania dokumentacji medycznej w formie elektronicznej – do jej uprzedniego zaszyfrowania lub innego zabezpieczenia przed dostępem osób nieuprawnionych;
    4) korzystania z urządzeń oraz systemów teleinformatycznych w sposób zapewniający ochronę Danych Osobowych przed dostępem osób nieuprawnionych m.in. poprzez:
        a. stosowanie indywidualnych, niepowtarzalnych haseł dostępu,
        b. niepozostawianie urządzeń bez nadzoru,
        c. zamykanie pomieszczeń, w których pracują urządzenia, na których przetwarzane są Dane Osobowe,
        d. wyłączanie urządzeń po zakończeniu użytkowania,
        e. nieudostępniania danych dostępowych (loginów i haseł) osobom nieuprawnionym,
        f. stosowanie oprogramowania antywirusowego oraz oprogramowania typu *firewall.*
    5) zamykania na klucz pomieszczeń, w których przechowywane są Dane Osobowe;

6) przechowywania w miejscu pracy (gabinet, recepcja itp.) dokumentów i innych nośników zawierających Dane Osobowe wyłącznie w przeznaczonych do tego pojemnikach/szafach/biurkach;
7) stosowania zasady „czystego biurka";
8) nieudostępniania Danych Osobowych osobom, których tożsamości nie można zweryfikować, lub co do której istnieją uzasadnione wątpliwości;
9) nieujawniania Danych Osobowych Pacjentów w pomieszczeniach ogólnodostępnych lokalu Administratora.

8. W przypadku podejrzenia naruszenia ochrony Danych Osobowych Administrator niezwłocznie weryfikuje, czy doszło do naruszenia i czy naruszenie mogło spowodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. W przypadku stwierdzenia naruszenia, Administrator niezwłocznie, nie później jednak niż w terminie 72 godzin o stwierdzeniu naruszenia zawiadamia Prezesa UODO.
9. Jeżeli naruszenie ochrony Danych Osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki powiadamia osobę, której dane dotyczą, o takim naruszeniu, chyba, że zachodzą okoliczności wskazane w art. 34 ust. 3 RODO.

Warszawa, dnia 27.09.2025 r.

Marcin Maksymiec

Podpis Administratora