

ZÁSADY OCHRANY SÚKROMIA

digitálnej rehabilitačnej platformy Rehabot

Dátum účinnosti: [DÁTUM]

1. Účel dokumentu

1.1 Tieto Zásady ochrany súkromia (ďalej len „Zásady“) informujú dotknuté osoby o spôsobe, rozsahu a účele spracúvania osobných údajov v rámci digitálnej rehabilitačnej platformy Rehabot (ďalej len „Služba“) v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov (ďalej len „GDPR“) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 18/2018 Z. z.“).

1.2 Tieto Zásady sa vzťahujú na všetkých používateľov Služby – fyzioterapeutov aj pacientov.

2. Rozsah Služby

2.1 Služba pozostáva z:

- a) webového rozhrania (dashboard) pre fyzioterapeutov – správa pacientov, tvorba cvičebných plánov, sledovanie pokroku, poznámky, plánovanie stretnutí;
- b) mobilnej aplikácie pre pacientov – prístup k cvičebným plánom, domáce cvičenia, termíny stretnutí.

2.2 Služba nie je poskytovateľom zdravotnej starostlivosti; je výhradne softvérovým nástrojom na podporu rehabilitačného procesu.

3. Prevádzkovateľ, sprostredkovateľ a kontakt

3.1 Prevádzkovateľom Služby (vo vzťahu k údajom fyzioterapeutov a prevádzkovým údajom) je:

Tomáš Solár, IČO: 57 797 480, sídlo: 082 61 Ražňany, Surdok 67/3, e-mail: info@rehabot.sk (ďalej len „Poskytovateľ“).

3.2 Vo vzťahu k osobným údajom pacientov vystupuje Poskytovateľ ako sprostredkovateľ v zmysle čl. 28 GDPR a § 34 zákona č. 18/2018 Z. z. Prevádzkovateľom osobných údajov pacientov je príslušný fyzioterapeut.

3.3 Poskytovateľ v súčasnosti nemá určenú zodpovednú osobu (DPO) v zmysle čl. 37 GDPR. Kontaktným bodom pre otázky ochrany osobných údajov je: info@rehabot.sk.

4. Zdroj údajov

4.1 Osobné údaje fyzioterapeutov sú získavané priamo od fyzioterapeutov pri registrácii a používaní Služby.

4.2 Osobné údaje pacientov sú do Služby zadávané prevažne fyzioterapeutom (meno, kontaktné údaje, zdravotné údaje, rodné číslo). Pacient môže doplniť niektoré údaje priamo v mobilnej aplikácii.

4.3 Technické a diagnostické údaje (logy, IP adresy, informácie o zariadení) sú zbierané automaticky pri používaní Služby.

5. Kategórie spracúvaných údajov

5.1 Identifikačné údaje: meno, priezvisko, titul, rodné číslo (pacient).

5.2 Kontaktné údaje: e-mailová adresa, telefónne číslo.

5.3 Prihlasovacie údaje: e-mail, heslo (hashované), autentifikačné tokeny.

5.4 Zdravotné a rehabilitačné údaje (osobitná kategória): diagnóza, anamnéza, cvičebné plány, poznámky fyzioterapeuta, záznamy o pokroku, fotodokumentácia.

5.5 Údaje o stretnutiach: dátumy a časy plánovaných a absolvovaných stretnutí.

5.6 Technické údaje: IP adresa, typ a verzia prehliadača/zariadenia, operačný systém, logy prístupu, identifikátory relácie.

5.7 Fakturačné údaje (fyzioterapeut): obchodné meno, IČO, DIČ, fakturačná adresa.

6. Citlivé údaje

6.1 Služba spracúva údaje týkajúce sa zdravia pacientov, ktoré patria medzi osobitné kategórie osobných údajov podľa čl. 9 GDPR a § 16 zákona č. 18/2018 Z. z.

6.2 Rodné číslo pacienta je šifrované algoritmom AES-256-GCM a overované prostredníctvom jednosmerného hashu (one-way hash). V čitateľnej podobe nie je bežne prístupné; prístup k dešifrovanému rodnému číslu je obmedzený výhradne na oprávneného fyzioterapeuta.

6.3 Spracúvanie zdravotných údajov je nevyhnutné na účely poskytovania zdravotnej starostlivosti v zmysle čl. 9 ods. 2 písm. h) GDPR a § 16 ods. 2 písm. h) zákona č. 18/2018 Z. z.

7. Právne základy spracúvania

7.1 Spracúvanie osobných údajov fyzioterapeutov:

a) plnenie zmluvy (čl. 6 ods. 1 písm. b) GDPR, § 13 ods. 1 písm. b) zákona č. 18/2018 Z. z.) – poskytovanie Služby;

b) oprávnený záujem Poskytovateľa (čl. 6 ods. 1 písm. f) GDPR, § 13 ods. 1 písm. f) zákona č. 18/2018 Z. z.) – bezpečnosť, prevencia podvodov, zlepšovanie Služby;

c) plnenie zákonnej povinnosti (čl. 6 ods. 1 písm. c) GDPR, § 13 ods. 1 písm. c) zákona č. 18/2018 Z. z.) – účtovné a daňové povinnosti.

7.2 Spracúvanie osobných údajov pacientov (Poskytovateľ ako sprostredkovateľ):

a) právnym základom spracúvania je vzťah medzi fyzioterapeutom (prevádzkovateľom) a pacientom – typicky plnenie zmluvy o poskytovaní zdravotnej starostlivosti alebo výslovný súhlas pacienta;

b) pre zdravotné údaje: čl. 9 ods. 2 písm. h) GDPR – spracúvanie nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej schopnosti alebo zdravotnej starostlivosti;

c) fyzioterapeut ako prevádzkovateľ zodpovedá za existenciu platného právneho základu.

8. Účely spracúvania

8.1 Poskytovanie a prevádzka Služby (registrácia, autentifikácia, správa účtov).

8.2 Umožnenie rehabilitačného procesu (cvičebné plány, sledovanie pokroku, komunikácia).

8.3 Technická podpora a riešenie problémov.

8.4 Bezpečnosť a prevencia zneužitia (monitorovanie, logy).

8.5 Plnenie zákonných povinností (účtovníctvo, dane, uchovávanie dokumentácie).

8.6 Zlepšovanie Služby (analýza používania, diagnostika chýb).

8.7 Komunikácia s Používateľmi (notifikácie, e-maily, pripomienky).

9. Google Calendar a Google Meet integrácia

9.1 Služba umožňuje voliteľnú integráciu s Google Calendar a Google Meet na účely plánovania a realizácie online stretnutí.

9.2 Pri aktivácii integrácie Služba ukladá OAuth prístupové tokeny prepojené s Google účtom Fyzioterapeuta a zdieľa s Google nasledovné údaje: meno pacienta, dátum a čas stretnutia, e-mailová adresa. Do kalendárnej udalosti sa môžu preniesť aj poznámky zo sedenia, ak ich Fyzioterapeut do plánovania zahrnie.

9.3 Integrácia je dobrovoľná a Fyzioterapeut ju aktivuje vlastným rozhodnutím. Spracúvanie údajov spoločnosťou Google sa riadi podmienkami ochrany súkromia spoločnosti Google LLC.

10. Zdieľanie údajov a sprostredkovatelia

10.1 Poskytovateľ pri zabezpečovaní prevádzky Služby využíva ďalších sprostredkovateľov (subdodávateľov), najmä v oblasti databázových, hostingových, e-mailových a monitorovacích služieb. Aktuálny zoznam subdodávateľov poskytne Poskytovateľ Fyzioterapeutovi na základe písomnej žiadosti.

10.2 Poskytovateľ zdieľa osobné údaje s tretími stranami výhradne v rozsahu nevyhnutnom na poskytovanie Služby a na základe písomnej zmluvy zabezpečujúcej primeranú úroveň ochrany údajov.

10.3 Údaje nie sú predávané tretím stranám na marketingové účely.

11. Umiestnenie a prenos údajov

11.1 Údaje sú primárne uložené a spracúvané v rámci Európskeho hospodárskeho priestoru (EHP).

11.2 Niektorí subdodávatelia (Sentry, Resend) majú sídlo v USA. Prenos údajov do tretích krajín je zabezpečený prostredníctvom štandardných zmluvných doložiek (SCC) podľa čl. 46 ods. 2 písm. c) GDPR a § 48 ods. 2 písm. c) zákona č. 18/2018 Z. z.

11.3 Poskytovateľ pravidelne prehodnocuje primerané záruky prenosu údajov do tretích krajín.

12. Uchovávanie údajov

12.1 Osobné údaje sú uchovávané po dobu nevyhnutnú na dosiahnutie účelu spracúvania:

- a) údaje aktívneho účtu – po dobu trvania zmluvného vzťahu;
- b) údaje po zrušení účtu – 30 dní (na umožnenie obnovy), následne vymazané;
- c) účtovné a daňové doklady – 10 rokov podľa zákona č. 431/2002 Z. z. o účtovníctve;
- d) zdravotná dokumentácia – podľa lehôt stanovených zákonom č. 576/2004 Z. z. o zdravotnej starostlivosti (20 rokov od posledného poskytnutia zdravotnej starostlivosti);
- e) technické logy – maximálne 90 dní.

12.2 Po uplynutí doby uchovávania sú údaje bezpečne vymazané alebo anonymizované.

13. Bezpečnosť

13.1 Poskytovateľ prijíma primerané technické a organizačné opatrenia na ochranu osobných údajov podľa čl. 32 GDPR a § 39 zákona č. 18/2018 Z. z., najmä:

- a) šifrovanie dát pri prenose pomocou protokolu TLS;
- b) šifrovanie citlivých údajov (rodné číslo) algoritmom AES-256-GCM;
- c) prístup na základe rolí (Role-Based Access Control – RBAC);
- d) logovanie prístupov a bezpečnostných udalostí;
- e) pravidelné zálohovanie dát;
- f) hashované ukladanie hesiel;
- g) pravidelné bezpečnostné aktualizácie infraštruktúry.

13.2 Poskytovateľ uplatňuje zásadu ochrany údajov od návrhu a štandardne (data protection by design and by default) podľa čl. 25 GDPR a § 32 zákona č. 18/2018 Z. z. Bezpečnosť a minimalizácia údajov sú zohľadňované už pri návrhu nových funkcií Služby.

14. Monitorovanie a diagnostika chýb

14.1 Služba využíva nástroj Sentry na monitorovanie chýb a výkonu aplikácie.

14.2 Sentry môže spracúvať: informácie o chybe (stack trace), IP adresu, identifikátor používateľa, typ zariadenia a prehliadača, URL, na ktorej chyba nastala.

14.3 Údaje v Sentry sú uchovávané maximálne 90 dní a slúžia výhradne na diagnostiku a opravu chýb.

14.4 Zdravotné údaje pacientov nie sú zámerne odosielané do Sentry. V prípade neočakávanej chyby sa však minimálne kontextové údaje môžu zachytiť v rámci chybového hlásenia.

15. Cookies a lokálne úložisko

15.1 Služba využíva nevyhnutné cookies a lokálne úložisko prehliadača (localStorage) na zabezpečenie funkčnosti (autentifikácia, preferencie relácie).

15.2 Nevyhnutné cookies nevyžadujú súhlas podľa § 109 ods. 8 zákona č. 452/2021 Z. z. o elektronických komunikáciách.

15.3 Služba v súčasnosti nepoužíva marketingové cookies. Na meranie výkonu a analytiku návštevnosti webového rozhrania môžu byť využívané nástroje Vercel Analytics a Vercel Speed Insights, ktoré spracúvajú anonymizované technické údaje (čas načítania stránky, typ zariadenia) bez použitia cookies tretích strán. V prípade zavedenia analytických alebo marketingových cookies vyžadujúcich súhlas bude od Používateľa vyžiadaný predchádzajúci súhlas v súlade s § 109 ods. 8 zákona č. 452/2021 Z. z.

16. Práva dotknutých osôb

16.1 Dotknutá osoba má v súlade s čl. 15 – 22 GDPR a § 21 – 28 zákona č. 18/2018 Z. z. nasledovné práva:

- a) právo na prístup k údajom (čl. 15 GDPR, § 21 zákona č. 18/2018 Z. z.);
- b) právo na opravu (čl. 16 GDPR, § 22 zákona č. 18/2018 Z. z.);
- c) právo na výmaz („právo byť zabudnutý“) (čl. 17 GDPR, § 23 zákona č. 18/2018 Z. z.);
- d) právo na obmedzenie spracúvania (čl. 18 GDPR, § 24 zákona č. 18/2018 Z. z.);
- e) právo na prenosnosť údajov (čl. 20 GDPR, § 26 zákona č. 18/2018 Z. z.);
- f) právo namietat' proti spracúvaniu (čl. 21 GDPR, § 27 zákona č. 18/2018 Z. z.);
- g) právo nebyť predmetom automatizovaného individuálneho rozhodovania (čl. 22 GDPR, § 28 zákona č. 18/2018 Z. z.);
- h) právo odvolať súhlas (ak je spracúvanie založené na súhlase) kedykoľvek bez toho, aby to malo vplyv na zákonnosť predchádzajúceho spracúvania.

16.2 Žiadosť o uplatnenie práv je možné podať na: info@rehabot.sk. Poskytovateľ vybaví žiadosť bez zbytočného odkladu, najneskôr do 30 dní.

16.3 Ak sa žiadosť Pacienta týka údajov, ktorých prevádzkovateľom je Fyzioterapeut, Poskytovateľ postúpi žiadosť príslušnému Fyzioterapeutovi alebo odkáže dotknutú osobu na Fyzioterapeuta.

17. Prenositel'nosť údajov

17.1 Dotknutá osoba má právo na prenosnosť údajov podľa čl. 20 GDPR a § 26 zákona č. 18/2018 Z. z.

17.2 Služba v súčasnosti neposkytuje automatizovaný samoobslužný export údajov. Export údajov je možné vyžiadať na: info@rehabot.sk. Poskytovateľ zabezpečí export v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte.

18. Výmaz údajov

18.1 Dotknutá osoba má právo na výmaz údajov podľa čl. 17 GDPR a § 23 zákona č. 18/2018 Z. z., ak sú splnené podmienky stanovené v príslušnom právnom predpise.

18.2 Žiadosť o výmaz je možné podať na: info@rehabot.sk. Služba v súčasnosti neposkytuje samoobslužné tlačidlo na výmaz účtu.

18.3 Výmaz bude realizovaný bez zbytočného odkladu, najneskôr do 30 dní, pokiaľ neexistuje zákonný dôvod na ďalšie uchovávanie údajov.

19. Dozorný orgán

19.1 Dotknutá osoba má právo podať sťažnosť dozornému orgánu podľa čl. 77 GDPR a § 100 zákona č. 18/2018 Z. z.

19.2 Príslušným dozorným orgánom v Slovenskej republike je:

Úrad na ochranu osobných údajov Slovenskej republiky

Hraničná 12, 820 07 Bratislava 27

Tel.: +421 2 3231 3214

Web: <https://dataprotection.gov.sk>

20. Kontaktný formulár

20.1 Služba môže obsahovať kontaktný formulár. Údaje zadané do kontaktného formulára (meno, e-mail, text správy) sú spracúvané na účely vybavenia požiadavky.

20.2 E-maily z kontaktného formulára sú odosielané prostredníctvom služby Resend, Inc. (sprostredkovateľ).

20.3 Právnym základom je oprávnený záujem Poskytovateľa na komunikácii s používateľmi (čl. 6 ods. 1 písm. f) GDPR).

21. Deti a mladiství

21.1 Služba nie je určená pre osoby mladšie ako 16 rokov na samostatné používanie v zmysle § 15 zákona č. 18/2018 Z. z.

21.2 Ak je pacientom osoba mladšia ako 16 rokov, Fyzioterapeut je povinný zabezpečiť súhlas zákonného zástupcu so spracúvaním osobných údajov.

21.3 Poskytovateľ vedome nespracúva osobné údaje detí mladších ako 16 rokov bez súhlasu zákonného zástupcu.

22. Zmeny dokumentu

22.1 Poskytovateľ si vyhradzuje právo kedykoľvek aktualizovať tieto Zásady.

22.2 O podstatných zmenách bude Poskytovateľ informovať Používateľov prostredníctvom e-mailu alebo oznámenia v rámci Služby najmenej 30 dní pred nadobudnutím účinnosti zmeny.

22.3 Aktuálne znenie Zásad je vždy dostupné na webovom sídle Služby.

23. Kontakt

Tomáš Solár

IČO: 57 797 480

Sídlo: 082 61 Ražňany, Surdok 67/3

E-mail: info@rehabot.sk

Web: www.rehabot.sk