

Informace o zpracování osobních údajů Poskytovatelem

1. Právní základ zpracování dle GDPR

Zpracování údajů probíhá na základě plnění smlouvy podle čl. 6 odst. 1 písm. b) GDPR. Účelem zpracování osobních údajů je efektivní komunikace při poskytování zdravotních služeb s Uživateli - Pacienty nehovořících úředním jazykem ČR prostřednictvím Aplikace. Tyto údaje jsou dobrovolné a Aplikace je plně funkční i bez jejich zadání.

Vzájemné postavení stran při zpracování osobních údajů

Poskytovatel zdravotních služeb je v postavení Správce osobních údajů, který rozhoduje o účelu a prostředcích zpracování. Společnost Language solutions s.r.o. jako poskytovatel Aplikace Galenio je v postavení Zpracovatele osobních údajů, který pro Správce zpracovává osobní údaje na základě smlouvy o zpracování osobních údajů v souladu s GDPR.

2. Doba uchování údajů

Osobní údaje pacientů (včetně historie chatu) jsou uchovávány po dobu 24 hodin od poskytnutí dat pacientem a poté automaticky smazány. Data jsou smazána z Aplikace a také ze služeb třetích stran. Seznam třetích stran je dostupný níže. Údaje o uživatelských účtech lékařů jsou uchovávány po dobu trvání smluvního vztahu a dále dle zákonných archivačních povinností.

3. Subjekt zpracování

Osobní data pro správce zpracovává zpracovatel, podle článku 28 GDPR. Zpracovatelem je společnost Language solutions s.r.o. se sídlem Nové sady 988/2, 602 00 Brno, IČO: 19590024.

Zpracovatel zpracovává osobní údaje výhradně jménem a podle pokynů správce a nemůže s nimi nakládat pro vlastní účely.

Mezi hlavní povinnosti Poskytovatele jako zpracovatele patří:

- Zpracování osobních údajů pouze za účelem provozu Aplikace a poskytování jejích funkcí.
- Zajištění vysoké úrovně bezpečnosti osobních údajů, včetně šifrování dat a omezeného přístupu.
- Informování správce o bezpečnostních incidentech a poskytnutí součinnosti při jejich řešení.
- Vedení záznamů o činnostech zpracování a umožnění správci provádět kontroly.
- Po ukončení spolupráce vymazání nebo anonymizace osobních údajů dle pokynů správce.

4. Závazek zpracování pouze nezbytných údajů

Poskytovatel zpracovává pouze ty osobní údaje, které jsou nezbytné pro fungování aplikace a plnění smluvního účelu. Zpracování probíhá v minimálním rozsahu nezbytném pro dorozumění mezi pacientem a lékařem.

Minimalizace

- Poskytovatel zpracovává pouze osobní údaje nezbytné pro umožnění komunikace mezi lékaři a zahraničními pacienty, zajištění provozu aplikace a její bezpečnosti.
- Nebudou shromažďovány, zpracovávány ani uchovávány žádné údaje, které nejsou potřebné pro výše uvedené účely.

Typy zpracovávaných údajů

- **Identifikační údaje** – jméno pacienta, příjmení pacienta, datum narození, národnost, pohlaví, jméno a příjmení lékaře.
- **Kontaktní údaje** – e-mailová adresa lékaře.
- **Citlivé údaje (čl. 9 GDPR)** – údaje o zdravotním stavu pacienta, pokud je zadá do chatu nebo formulářů.

Omezení účelu

- Osobní údaje jsou zpracovávány výhradně za účelem umožnění komunikace mezi lékařem a pacientem a správy uživatelských účtů lékařů.
- Údaje nebudou použity k marketingovým ani analytickým účelům.

5. Způsob zpracování

Poskytovatel zpracovává osobní údaje výhradně elektronicky s důrazem na bezpečnost a ochranu soukromí. Použité technologie odpovídají požadavkům nařízení GDPR a zajišťují vysokou úroveň ochrany osobních údajů před neoprávněným přístupem, ztrátou nebo zneužitím.

Infrastruktura a úložiště dat

- Osobní údaje jsou uloženy v databázi hostované na serverech poskytovatele cloudových služeb HostArmada.com, přičemž servery se fyzicky nacházejí ve Frankfurtu nad Mohanem, Německo.
- Data jsou zpracovávána a ukládána výhradně v Evropské unii, čímž je zajištěna jejich ochrana dle GDPR.
- Servery jsou chráněny proti neoprávněnému přístupu víceúrovňovým zabezpečením, včetně firewallů a monitoringu síťového provozu.

Zabezpečení

Podrobné informace o zabezpečení a šifrování dat jsou uvedeny níže v sekci “**Zabezpečení údajů**”.

6. Povinnosti správce při správě osobních údajů

Nemocnice jako správce osobních údajů se zavazuje zajistit, že zpracování osobních údajů v rámci Aplikace probíhá v souladu s GDPR a dalšími relevantními právními předpisy. Mezi hlavní povinnosti správce patří:

Zajištění zákonnosti zpracování

- Správce odpovídá za to, že veškeré zpracování osobních údajů pacientů probíhá na právním základě, zejména podle čl. 6 a čl. 9 GDPR.
- Správce zajistí, že pacienti budou řádně informováni o zpracování osobních údajů, a pokud je to vyžadováno, bude od nich získán výslovný souhlas.

Využití Aplikace

- Správce je povinen využívat Aplikaci podle jejího účelu.

7. Povinnosti zpracovatele při správě osobních údajů

Poskytovatel jako zpracovatel osobních údajů jedná na základě pokynů správce a zavazuje se zajistit, že zpracování osobních údajů probíhá v souladu s GDPR. Mezi jeho hlavní povinnosti patří:

Zpracování údajů pouze na základě pokynů správce

- Zpracovatel smí zpracovávat osobní údaje pouze v rozsahu a pro účely, které budou uvedené ve smlouvě.
- Nesmí osobní údaje používat pro své vlastní účely.
- Pokud správce požádá o výmaz nebo úpravu osobních údajů, zpracovatel musí tuto žádost neprodleně splnit.

Zajištění bezpečnosti údajů

- Zpracovatel se zavazuje přijmout technická a organizační opatření k ochraně osobních údajů proti neoprávněnému přístupu, ztrátě, zneužití nebo úniku. Technická opatření jsou popsány v sekci “**Zabezpečení údajů**” níže.

Hlášení bezpečnostních incidentů

- Pokud zpracovatel zjistí narušení bezpečnosti osobních údajů, musí správce informovat nejpozději do 24 hodin od zjištění incidentu.
- Zpracovatel musí správci poskytnout veškeré dostupné informace o incidentu, včetně:
 - Povahy incidentu.
 - Dopadu na osobní údaje.
 - Opatření přijatých k nápravě a prevenci dalších incidentů.
- Zpracovatel se zavazuje spolupracovat se správcem na řešení incidentu a poskytovat součinnost při případném hlášení dozorovým orgánům.

Spolupráce při výkonu práv subjektů údajů

- Zpracovatel musí umožnit správci reagovat na žádosti pacientů týkající se výkonu jejich práv (např. výmaz údajů, přístup k údajům...).

Ukončení zpracování a výmaz údajů

- Po ukončení spolupráce nebo na žádost správce musí zpracovatel:
 - Bezodkladně vymazat nebo anonymizovat veškeré osobní údaje, které zpracovával jménem správce.

8. Povinnosti zpracovatele při porušení zabezpečení

V případě narušení zabezpečení osobních údajů, které by mohlo vést k náhodnému nebo neoprávněnému přístupu, ztrátě nebo úniku osobních údajů, se Poskytovatel (zpracovatel) zavazuje postupovat podle následujících pravidel:

Okamžité oznámení správci

- Poskytovatel musí bez zbytečného odkladu, nejpozději do 24 hodin od zjištění incidentu, informovat správce o jakémkoli porušení zabezpečení osobních údajů.
- Oznámení musí obsahovat:
 1. **Popis incidentu** – co se stalo a jaké údaje byly dotčeny.
 2. **Důsledky incidentu** – potenciální dopady na pacienty, lékaře nebo další osoby.
 3. **Přijatá opatření** – kroky podniknuté k nápravě a minimalizaci škod.

Spolupráce při řešení incidentu

- Zpracovatel je povinen plně spolupracovat se správcem na řešení incidentu a poskytnout veškeré potřebné informace.
- Na žádost správce musí zpracovatel provést interní audit a dodat správci zprávu o zjištěních a doporučeních pro zvýšení bezpečnosti.

Přijetí nápravných opatření

- Poskytovatel se zavazuje okamžitě přijmout vhodná technická a organizační opatření k zamezení opakování incidentu.
- Pokud je to nutné, Poskytovatel provede aktualizaci bezpečnostních protokolů a posílí ochranu přístupu k datům.

Povinnost vést evidenci incidentů

- Zpracovatel je povinen uchovávat záznamy o všech bezpečnostních incidentech, včetně jejich příčiny, dopadů a přijatých opatření, po dobu nejméně 5 let.
- Na žádost správce musí Zpracovatel poskytnout kopii těchto záznamů.

9. Odměna zpracovatele

Zpracování osobních údajů Poskytovatelem (zpracovatelem) je součástí poskytování služeb Aplikace a jeho náklady jsou plně zahrnuty v ceně předplatného hrazeného správcem.

Specifikace typů zpracovávaných dat, jejich zabezpečení a cyklus

Životní cyklus údajů

Uživatelské účty lékařů a údaje o nemocnicích

1. Data získáváme:
 - a) Od nemocnic při vytváření účtu nemocnice a lékařů
 - b) Od lékaře při změně hesla
2. Správa dat
 - a) Údaje jsou uloženy v databázi na serverech HostArmada.com. Servery společnosti HostArmada.com jsou fyzicky umístěny ve Frankfurtu nad Mohanem.
 - b) Ke smazání dat dojde po smazání nemocnice, či uživatelského účtu lékaře.

Údaje o pacientech a historie chatu

1. Data získáváme:
 - a) Pacienti mohou zadat své identifikační údaje a obecné informace do chatu a formuláře při připojování.
 - b) Pacienti následně přidávají zprávy do chatu, které obsahují obecné informace a Citlivé údaje.
 - c) Lékař do chatu píše zprávy, které obsahují obecné informace a Citlivé údaje.
 - d) Lékař má možnost stáhnout informace o komunikaci a údajích pacienta do PDF souboru.

Zabezpečení údajů

1. Technické zabezpečení
 - a) Údaje jsou zašifrované. Klíče pro rozšifrování jsou uloženy v prohlížečích pacienta a lékaře. Na serveru se tento klíč neukládá.
 - b) Funkce zabezpečení: Pokud pacient pošle zprávu, tak se odešle v plaintextu na server, kde se šifruje pomocí klíče, který je uložen v autentizačním tokenu chatu (RoomTokenu), kterým se pacient a lékař prokazují. Následně se zpráva v zašifrované podobě uloží do databáze a v nezašifrované podobě se posílá lékaři.
 - c) Zálohování databáze a kódu aplikace - každý den o půl páté ráno
 - d) logování přístupů - monitorujeme přístupy do aplikace a sledujeme podezřelá chování v aplikaci.
 - e) Specifikace hesel: Heslo musí být minimálně 6 znaků dlouhé a obsahovat alespoň: jedno malé a velké písmeno, jednu číslici a jeden speciální znak.
2. Personální zabezpečení
 - a) Uzavření dohody o mlčenlivosti se všemi zaměstnanci.
 - b) Proškolení všech zaměstnanců a spolupracovníků o problematice GDPR.
 - c) Všichni zaměstnanci používají hesla, která obsahují jedno malé a velké písmeno, jednu číslici a jeden speciální znak. Minimální délka hesla je 6 znaků
 - d) Zajištění evidence všech dodavatelů s přístupem k osobním údajům. S dodavateli v postavení zpracovatelů osobních údajů je uzavřena smlouva o zpracování osobních údajů v souladu s GDPR. Seznam třetích stran je dostupný níže.
3. Zabezpečení dodavatelského řetězce - Seznam třetích stran je dostupný níže v tomto dokumentu.
 - a) Zajištění evidence všech dodavatelů s přístupem k osobním údajům.
 - b) S dodavateli v postavení zpracovatelů osobních údajů je uzavřena smlouva o zpracování osobních údajů v souladu s GDPR.

4. Zabezpečené údaje obsahují:

- a) Identifikační údaje
- b) Obecné informace
- c) Kontaktní informace
- d) Citlivé údaje

Kategorie osobních údajů

Za účelem poskytování možnosti správné funkce webové aplikace Galenio zpracováváme tyto kategorie osobních údajů:

- 1. Identifikační údaje** - Jméno pacienta, příjmení pacienta, datum narození pacienta, národnost pacienta a pohlaví pacienta, jméno lékaře, příjmení lékaře
- 2. Kontaktní informace** - email lékaře
- 3. Obecné informace** - Informace, které se při komunikaci objeví v rozhraní chatu. Veškeré obecné informace, které se netýkají zdravotního stavu pacienta.
- 4. Citlivé údaje** - Informace, které se při komunikaci objeví v rozhraní chatu. Veškeré informace o zdravotním stavu, které pacient sdělí lékaři a na které se lékař zeptá.

Úroveň osobních údajů

Aplikace zpracovává obecné osobní údaje v kategoriích identifikační údaje a kontaktní informace. Aplikace dále zpracovává zvláštní kategorie osobních údajů podle článku 9 o Zpracování zvláštních kategorií osobních údajů citlivé údaje. Pro tuto zvláštní kategorii je v aplikaci nutné udělit výslovný **souhlas ze strany pacienta**. Pacient zaškrtnává tlačítko souhlasu poté, co má možnost si přečíst informace o zpracování jeho osobních údajů v rámci aplikace. Souhlas je informovaný a je ke konkrétnímu účelu - k použití aplikace a sdílení údajů s lékařem.

Operace zpracování

Veškeré informace o operacích zpracování jsou dostupné níže.

Seznam třetích stran

Seznam třetích stran:

1. OpenAI
 - a. Technologie pro překlady
 - b. Poskytovatel sídlí na adrese 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, Irsko
 - c. Pro případ sdílení informací se společnostmi ve skupině OpenAI jsou součástí zpracovatelských podmínek i standardní smluvní doložky pro předávání osobních údajů do třetích zemí schválené Evropskou komisí
2. HostArmada.com
 - a. Hosting serveru
 - b. Hosting databáze
 - c. Poskytovatel sídlí na adrese 501 Silverside Rd, Wilmington, Delaware, 19809, USA
 - d. Součástí zpracovatelských podmínek jsou standardní smluvní doložky pro předávání osobních údajů do třetích zemí schválené Evropskou komisí
 - e. Servery, na kterých se aplikace hostuje jsou umístěné ve Frankfurtu nad Mohanem v Německu
3. Google LLC IPA
 - a. Technologie pro speech to text a text to speech
 - b. Poskytovatel sídlí na adrese 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA
 - c. Poskytovatel je certifikovaným subjektem EU-US Rámce pro ochranu soukromí. Pro každý případ jsou součástí zpracovatelských podmínek i standardní smluvní doložky pro předávání osobních údajů do třetích zemí schválené Evropskou komisí.
4. Translated S.r.l.
 - a. Technologie pro překlady
 - b. Poskytovatel sídlí na adrese Via Indonesia 23, 00144 Roma, Italy
 - c. Pro případ sdílení informací jsou součástí zpracovatelských podmínek i standardní smluvní doložky pro předávání osobních údajů do třetích zemí schválené Evropskou komisí.

Tabulka s operacemi zpracování osobních údajů

Typ	Kategorie	Operace a účel zpracování	Kdo informace zpracovává	Zabezpečení	Mazání dat
Jméno pacienta	Identifikační údaje	Za účelem identifikace pacienta lékařem a umožnění použití aplikace	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Příjmení pacienta	Identifikační údaje	Za účelem identifikace pacienta lékařem a umožnění použití aplikace	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Datum narození pacienta	Identifikační údaje	Za účelem identifikace pacienta lékařem a umožnění použití aplikace	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Národnost pacienta	Identifikační údaje	Za účelem identifikace pacienta lékařem a umožnění použití aplikace	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Pohlaví pacienta	Identifikační údaje	Za účelem rozeznání pohlaví pacienta lékařem a jeho identifikaci	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Jméno lékaře	Identifikační údaje	Slouží pro možnost registrace lékaře do aplikace a k jeho identifikaci.	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách

Příjmení lékaře	Identifikační údaje	Slouží pro možnost registrace lékaře do aplikace a k jeho identifikaci.	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Email lékaře	Kontaktní informace	Za účelem vytvoření účtu lékaři v aplikaci.	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Po smazání účtu lékaře z aplikace galenio.cz
Informace zaznamenané v chatu, které nejsou citlivými údaji	Obecné informace	Za účelem poskytnutí obecných informací lékaři. Za účelem dorozumění.	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách
Informace zaznamenané v chatu, které jsou citlivé podle článku 9 GDPR a týkají se zdravotního stavu pacienta	Citlivé údaje	Za účelem umožnění léčby pacienta. Za účelem určení diagnózy. Za účelem dorozumění.	Společnost Language solutions s.r.o. provozující webovou aplikaci galenio.cz, Služby třetích stran.	Informace o zpracování osobních údajů Poskytovatelem sekce: Zabezpečení údajů	Automaticky po 24 hodinách