PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Poslední aktualizace: 20. dubna 2026

Identifikace poskytovatele: Citymind solutions s.r.o., IČO 19776438, se sídlem Pražákova 1008/69, Štýřice, 639 00 Brno, zapsána v obchodním rejstříku vedeném u Krajského soudu v Brně sp. zn. C 136031 („**Poskytovatel**“).

1. ÚVODNÍ USTANOVENÍ

1.1 Vztah ke smlouvě. Zákazník a Poskytovatel uzavřeli Smlouvu o poskytování software Citymind („**Smlouva**“), na základě které se Poskytovatel zavázal poskytovat služby spojené s produkty Citymind, jejichž cílem je, aby pomocí jazykových modelů zodpovídaly koncovým uživatelům jejich dotazy a řešily definované situace, na základě zvoleného datového základu a další činnosti a služby specifikované ve Smlouvě. Tyto podmínky zpracování osobních údajů („**Zpracovatelské podmínky**“) tvoří nedílnou součást Smlouvy.

1.2 Rozsah služeb. Na základě Smlouvy budou poskytovány služby jako například implementace, úpravy, personalizace, přípravy dat pro produkty Citymind na základě dat z webu formou web scrapingu ve sjednaném rozsahu, služby spojené s využíváním webové aplikace „Citymind Manager“, včetně následné údržby a podpory („**Služby**“). Konkrétní rozsah poskytovaných Služeb vyplývá z uzavřené Smlouvy, případně z dalších dílčích smluv či pokynů ze strany zákazníka dohodnutých v souladu se Smlouvou.

1.3 Vztah k právním předpisům. Vzhledem k tomu, že na základě poskytování Služeb může docházet ke zpracování osobních údajů Poskytovatelem pro zákazníka, vystupuje Poskytovatel v pozici zpracovatele osobních údajů vůči zákazníkovi. Nedílnou součástí Smlouvy jsou tak tyto podmínky zpracování osobních údajů ve smyslu čl. 28 odst. 3 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**“), a ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů.

1.4 Pověření ke zpracování. Zákazník tímto pověřuje Poskytovatele zpracováním osobních údajů subjektů údajů v rámci poskytování Služeb. Poskytovatel je povinen zpracovávat osobní údaje pro zákazníka na základě jeho doložených písemných pokynů a v rozsahu nezbytném k řádnému plnění povinností Poskytovatele vyplývajících ze Smlouvy. Písemné pokyny mohou být udělovány také prostřednictvím webové aplikace „Citymind Manager“ či pracovníků zákazníka, kteří komunikují s Poskytovatelem.

1.5 Odpovědnost zákazníka. Zákazník je odpovědný za plnění všech povinností ve vztahu ke zpracování osobních údajů, zejména za řádné informování subjektů údajů o zpracování osobních údajů, získání souhlasu se zpracováním osobních údajů, pokud je zapotřebí, vyřizování žádostí subjektů údajů, týkajících se realizace jejich práv (jako je právo na informace, přístup, opravu, výmaz, omezení zpracování, vznést námitku apod.) a plnění dalších povinností, které GDPR pro zákazníka jako správce osobních údajů stanovuje. Poskytovatel bude při plnění těchto povinností zákazníkovi nápomocný, a to v rozsahu těchto Zpracovatelských podmínek.

2. PŘEDMĚT ZPRACOVÁNÍ, KATEGORIE SUBJEKTŮ ÚDAJŮ A TYP OSOBNÍCH ÚDAJŮ

2.1 Předmět zpracování a typ osobních údajů. Předmětem zpracování jsou zejména následující osobní údaje:

a) uživatelské údaje a platební údaje zákazníků, kterým byl zřízen uživatelský účet pro poskytování Služeb Poskytovatelem,

b) identifikační údaje,

c) data získaná z webu formou scrapingu v souvislosti s poskytovanými Službami,

d) informace související s poskytováním aplikace Citymind, včetně záznamů komunikace prostřednictvím produktů Citymind, logů, statistik a dalších technických informací, včetně jakýchkoliv vstupních dat,

e) výstupy z jazykových modelů a další výstupní data,

f) informace získané v rámci poskytování technické podpory a údržby (reportované incidenty, obsahy těchto incidentů),

g) údaje subjektů údajů zákazníka, případně dalších subjektů údajů, které budou uloženy v jakémkoliv rozhraní poskytovaném při poskytování Služeb, budou zákazníkem předány Poskytovateli nebo které Poskytovatel získá při poskytování Služeb, a které budou zpracovávány při poskytování Služeb dle Smlouvy.

2.2 Kategorie subjektů údajů. Subjekty údajů jsou:

a) zaměstnanci a další pracovníci zákazníka,

b) další uživatelé, kteří využívají aplikaci Citymind,

c) osoby, kterým jsou poskytovány Služby a které jsou pověřeny zákazníkem komunikovat s Poskytovatelem,

d) návštěvníci webů zákazníka,

e) osoby, jejichž osobní údaje předal zákazník Poskytovateli za účelem zajištění Služeb,

f) další osoby, o kterých zákazník předá Poskytovateli osobní údaje, případně které budou předány, či jinak získány při poskytování Služeb v souladu s plněním Smlouvy.

3. POVAHA A ÚČEL ZPRACOVÁNÍ

3.1 Povaha zpracování. Poskytovatel bude zpracovávat osobní údaje elektronicky a automatizovaně, přičemž zpracování osobních údajů bude spočívat v uložení a zálohování osobních údajů na úložištích poskytovaných třetí stranou, konkrétně společností Microsoft, nahlížení na osobní údaje v rámci zajištění přizpůsobení a nastavení chatbota, činnosti a úpravy na míru, řešení požadavků zákazníka při poskytování Služeb, propojování osobních údajů a využívání umělé inteligence prostřednictvím jazykových modelů poskytovaných třetími stranami.

3.2 Automatizované rozhodování. Zákazník prohlašuje, že nebude využívat Služby pro automatizované rozhodování, včetně profilování subjektů údajů. V případě, že k tomuto bude ze strany zákazníka docházet, zavazuje se zákazník informovat subjekty údajů o této skutečnosti, přičemž je povinen samostatně zajistit plnění všech práv a povinností dle GDPR a Poskytovatel za to nenese žádnou odpovědnost.

3.3 Účel zpracování. Účel zpracování je definován účelem plnění Smlouvy, tedy zajištění poskytnutí Služeb, podpory a údržby.

4. DOBA ZPRACOVÁNÍ

4.1 Doba zpracování. Zpracování osobních údajů bude probíhat po dobu účinnosti Smlouvy, případně po dobu potřebnou pro poskytování Služeb. Povinnosti Poskytovatele týkající se ochrany osobních údajů se Poskytovatel zavazuje plnit po celou dobu účinnosti Smlouvy, pokud ze Zpracovatelských podmínek nevyplývá, že mají trvat i po zániku její účinnosti.

4.2 Skončení zpracování. V případě, že dojde k ukončení Smlouvy, dojde k uložení osobních údajů ve formě zálohy na servery MS Azure, ve které budou uloženy po dobu 6 měsíců od skončení Smlouvy. V této lhůtě může Zákazník požádat Poskytovatele o obnovení Služeb a uzavření nové Smlouvy, přičemž v takovém případě budou dané osobní údaje opět obnoveny pro poskytování Služeb. Po uplynutí 6 měsíců od skončení Smlouvy Poskytovatel osobní údaje vymaže.

5. DALŠÍ POVINNOSTI POSKYTOVATELE

5.1 Souhrn povinností. Poskytovatel je při zpracovávání osobních údajů povinen:

a) zpracovávat osobní údaje výlučně na základě doložených pokynů zákazníka; pro vyloučení pochybností, zpracovávání osobních údajů v souladu s povinnostmi Poskytovatele dohodnutými v rámci Smlouvy se považuje za prováděné v souladu s instrukcemi zákazníka; za pokyny pro zpracování osobních údajů se považují také pokyny učiněné prostřednictvím aplikace Citymind, případně jakéhokoliv jiného rozhraní využívaného při poskytování Služeb;

b) řídit se instrukcemi zákazníka v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Evropské unie nebo členského státu, které se na Poskytovatele vztahuje; v takovém případě Poskytovatel zákazníka informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

c) zajišťovat, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

d) při zohlednění povahy zpracování být zákazníkovi nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění zákazníkovy povinnosti reagovat na žádosti o výkon práv subjektů údajů;

e) při zajišťování souladu s povinnostmi zákazníka být zákazníkovi nápomocen (i) zajistit úroveň zabezpečení zpracování, (ii) ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a případně též subjektům údajů, (iii) posuzovat vliv na ochranu osobních údajů a (iv) realizovat předchozí konzultace s Úřadem pro ochranu osobních údajů, a to při zohlednění povahy zpracování a osobních údajů, jež má Poskytovatel k dispozici;

f) umožnit zákazníkovi či jím pověřené osobě kontrolu (včetně auditu či inspekce) dodržování těchto Zpracovatelských podmínek, zejména povinností pro zpracování osobních údajů z nich vyplývajících, a k těmto kontrolám přispět dle důvodných pokynů zákazníka či kontrolující osoby; konkrétní pravidla auditů jsou uvedena v čl. 5.2 a 5.3 těchto Zpracovatelských podmínek.

5.2 Audity. Jakoukoliv žádost o audit je zákazník povinen zaslat výhradně na e-mailovou adresu Poskytovatele hello@citymind.tech. Po obdržení žádosti o audit se Poskytovatel a zákazník dopředu dohodnou na: (a) možném termínu provedení auditu, bezpečnostních opatřeních a způsobu zajištění dodržení závazků mlčenlivosti během auditu, a (b) předpokládaném začátku, rozsahu a době trvání

auditu. V případě, že k dohodě nedojde ani do 30 dnů ode dne odeslání žádosti, určí podmínky auditu Poskytovatel.

5.3 Námitky proti auditorovi. Poskytovatel může vznést písemné námitky proti jakémukoliv auditorovi, který byl pověřen zákazníkem, pokud není auditor podle názoru Poskytovatele dostatečně kvalifikován, není nezávislý, je v soutěžním postavení vůči Poskytovateli nebo je jinak zjevně nevhodný. Na základě vznesené námitky má zákazník povinnost pověřit jiného auditora, nebo provést audit sám.

5.4 Žádosti subjektů. Poskytovatel se zavazuje, v případě přijetí jakékoliv žádosti třetí osoby, týkající se zpracování osobních údajů, zejména žádosti subjektu údajů (klientů zákazníka), týkající se výkonu jeho práv, zákazníka, nejpozději však do 14 dnů od přijetí, o takové skutečnosti informovat a poskytnout mu nezbytnou součinnost pro její vyřízení v souladu s GDPR. Tím není dotčeno ustanovení čl. 3.2. těchto Zpracovatelských podmínek.

5.5 Obecný souhlas se zapojením dalších zpracovatelů. Zákazník uděluje obecný souhlas se zapojením dalších zpracovatelů do zpracování osobních údajů Poskytovatelem. Zákazník tímto souhlasí s tím, že Poskytovatel zapojí dílčí zpracovatele, kterými jsou:

- Microsoft Ireland Operations Limited, který poskytuje služby jako Microsoft Azure, a také jazykový model. Osobní údaje jsou ukládány v EU – Polsko.
- OpenAI Ireland Ltd., která zajišťuje záložní jazykový model.
- Společnost Atlassian Pty Ltd a Trello, Inc., které zajišťují ticketovací systém Trello.
- Twilio, která zajišťuje spojení mezi telefonní bránou a systémem Citymind
- ElevenLabs, která zajišťuje řečové technologie

5.6 Zapojení dalších zpracovatelů. Poskytovatel před zapojením dalšího zpracovatele písemně informuje zákazníka (formou určenou Poskytovatelem) o tomto zapojení, přičemž zákazník může proti zapojení dalšího zpracovatele vznést námitky, a to do 10 dnů. Pokud se zákazník ve lhůtě nevyjádří, zapojí Poskytovatel tohoto dalšího zpracovatele. Pokud zákazník námitku vznese, Poskytovatel ji posoudí, a pokud ji shledá oprávněnou, dalšího zpracovatele nezapojí. V takovém případě je však Poskytovatel oprávněn ukončit poskytování Služeb v rozsahu navázaném na dalšího zpracovatele, přičemž zákazník nemá nárok na náhradu škody ani slevu z poskytovaných Služeb.

5.7 Závazek vůči dalším zpracovatelům. Pokud Poskytovatel zapojí do zpracování osobních údajů dalšího zpracovatele, musí tohoto dalšího zpracovatele smluvně zavázat k dodržování stejných povinností na ochranu osobních údajů, jako jsou dohodnuty mezi zákazníkem a Poskytovatelem v těchto Zpracovatelských podmínkách, a to zejména k zavedení vhodných technických a organizačních opatření.

6. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ A ZÁVĚREČNÁ USTANOVENÍ

6.1 Obecně k bezpečnostním opatřením. Poskytovatel přijal a udržuje taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

6.2 Konkrétní bezpečnostní opatření. Poskytovatel přijal a udržuje zejména následující opatření k zajištění přiměřené úrovně zabezpečení:

a) pseudonymizace a šifrování osobních údajů při uložení osobních údajů;

b) schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;

c) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Konkrétní opatření jsou uvedena v příloze č. 1 těchto Zpracovatelských podmínek.

6.3 Bezpečnostní incidenty. V případě, že Poskytovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu zákazníkovi, a to nejpozději do 48 hodin, přičemž Poskytovatel vynaloží přiměřené úsilí k tomu, aby zákazníkovi poskytl všechny informace, které k incidentu zná, maximálně však v rozsahu dle čl. 33 odst. 3 GDPR.

6.4 Náklady. Poskytovatel je oprávněn vyúčtovat zákazníkovi účelně vynaložené náklady spojené s vyřizováním jakékoliv žádosti, uvedené zejména v čl. 5 těchto Zpracovatelských podmínek (včetně vyřizování všech žádostí při zajišťování souladu, nápomoci při provádění dalších činností, auditů).

6.5 Odpovědnost. V případě, že zákazník udělí Poskytovateli pokyn, na základě kterého dojde k porušení povinností dle GDPR, přičemž Poskytovatel na základě tohoto pokynu bude sankcionován ze strany dozorového úřadu, či bude povinen nahradit škodu subjektům údajů, zavazuje se zákazník odškodnit Poskytovatele a uhradit mu veškerou prokazatelně vzniklou újmu.

6.6 Limitace odpovědnosti. V případě, že by Poskytovatel byl povinen uhradit zákazníkovi jakoukoliv náhradu škody, bude tato povinnost omezena maximálně do výše ceny, kterou zákazník zaplatil Poskytovateli na základě Smlouvy za uplynulých 12 měsíců před vznikem škody.

PŘÍLOHA Č. 1 – TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

OPATŘENÍ PRO PSEUDONYMIZACI

Opatření, která omezují přímé odkazy na fyzické osoby během zpracování, a to takovým způsobem, že údaje lze přiřadit ke konkrétní osobě pouze tehdy, pokud je k dispozici dodatečná informace. Tato dodatečná informace musí být uchovávána odděleně od pseudonymu pomocí vhodných technických a organizačních opatření.

OPATŘENÍ PRO ŠIFROVÁNÍ

- IT systémy zpracovávající naše data umožňují pouze bezpečné kanály či protokoly pro příchozí síťová připojení.
- Certifikáty a kryptografické klíče jsou bezpečně spravovány z hlediska:
    - vytváření, ukládání a odvolávání klíčů
    - sdílení nebo distribuce klíčů
    - nasazování klíčů do produkčního prostředí
    - rotace nebo obnovování klíčů

OPATŘENÍ K ZAJIŠTĚNÍ DŮVĚRNOSTI

- Logická kontrola přístupu:
    - Opatření k zabránění, aby neoprávněné osoby zpracovávaly či používaly data chráněná předpisy o ochraně osobních údajů nebo zákony o obchodním tajemství.
- Pokud je Poskytovatel odpovědný za správu a údržbu IT systémů ukládajících nebo zpracovávajících data, musí být minimálně přijata tato opatření pro logickou kontrolu přístupu:
    - Přístup je silně autentizován (např. pomocí zásad pro silná hesla v souladu s uznávanými osvědčenými postupy).
    - Přístupová práva k datům jsou udělována na základě zdokumentovaného procesu žádosti a schválení.
    - Odchody zaměstnanců, změny v týmu a neaktivní uživatelé (např. rodičovská dovolená) jsou včas zohledněny (uživatelské účty jsou odstraněny/zakázány/upraveny).
    - Přístupová práva k datům jsou pravidelně kontrolována (alespoň čtvrtletně).
    - Zaměstnanci, kteří mají přístup k datům, používají jedinečné a nesdílené osobní přihlašovací údaje. Používání obecných účtů je zakázáno.
    - Pokusy o přístup (úspěšné i neúspěšné) jsou zaznamenávány a monitorovány.
    - Přístup k pracovním stanicím používaným personálem Poskytovatele pracujícím pro zákazníka je autentizován (např. pomocí zásad pro silná hesla v souladu s uznávanými osvědčenými postupy).

- Síťová infrastruktura Poskytovatele je odpovídajícím způsobem chráněna.

- Popis opatření kontroly přístupu k datům:
  - Přístupová práva k datům zákazníka jsou udělována na základě zdokumentovaného procesu žádosti a schválení.
  - Přístup k datům zákazníka je omezen na princip minimálních oprávnění (least privilege).
  - Přístupová oprávnění jsou omezena na osoby, které je skutečně potřebují (např. mají roli vyžadující administrátorský přístup).
  - Přístupová práva k datům zákazníka jsou pravidelně kontrolována (alespoň čtvrtletně).

- Dodržování technická a další opatření (např. bezpečnostní a organizační pokyny a interní směrnice Klienta, pokud jsou mu známy) jejichž účelem je zajištění utajení Chráněných informací a bude je chránit způsobem určeným Klientem v rozsahu uzavřených smluv o mlčenlivosti.

OPATŘENÍ K ZAJIŠTĚNÍ INTEGRITY

- Popis opatření k zajištění integrity dat:
  - Opatření uvedená v jiných částech již řeší integritu dat.

- Kontrola přenosu:
  - Certifikáty a kryptografické klíče jsou bezpečně spravovány z hlediska:
    - vytváření, ukládání a odvolávání klíčů
    - sdílení nebo distribuce klíčů
    - nasazování klíčů do produkčního prostředí
    - rotace nebo obnovování klíčů
  - Přihlašovací údaje (hesla, OAuth 2 klienti, tokeny) používané k autentizaci vůči vzdáleným službám jsou bezpečně spravovány z hlediska:
    - vytváření, ukládání a odvolávání klíčů
    - sdílení nebo distribuce klíčů
    - nasazování klíčů do produkčního prostředí
    - rotace nebo obnovování klíčů
  - IT systémy zpracovávající data zákazníka umožňují pouze bezpečné kanály či protokoly pro příchozí síťová připojení.

- Události související s přístupem k systému jsou zaznamenávány (logovány).
  - Minimální rozsah zaznamenávaných údajů:
    - Časové razítko (Timestamp)

        - Zdrojová identita (Source Identity)
        - Úspěšná a neúspěšná autentizace
        - Úspěšná a neúspěšná autorizace
        - Detaily autorizace (co bylo autorizováno)
- Existuje proces pro pravidelnou kontrolu a vyhodnocování zaznamenaných událostí a reakci na ně.
- Logy jsou chráněny proti neoprávněnému přístupu.

OPATŘENÍ K ZAJIŠTĚNÍ DOSTUPNOSTI A ODOLNOSTI

Všechna opatření uvedená níže jsou zajišťována třetími stranami Poskytovatele

- Místnosti s umístěnými servery obsahujícími data zákazníka jsou řádně oddělené.
- Existují mechanismy ochrany proti požáru.
- Hořlavý materiál (např. papír, karton) se v místnostech s umístěnými servery obsahujícími data Klienta bez dozoru nenachází.
- Jsou zavedeny mechanismy pro kontrolu teploty a vlhkosti.
- Systémy chránící proti environmentálním rizikům jsou pravidelně kontrolovány a udržovány.
- Systémy jsou napájeny z nepřerušitelného zdroje energie (UPS).
- Systémy chránící proti výpadkům napájení (např. UPS) jsou pravidelně kontrolovány a udržovány.