

Smlouva o zpracování osobních údajů

Salesbot.cz · verze 2026-10.1 · účinnost od 16. 10. 2026; vůči Správci od jejího přijetí v aplikaci

Tato smlouva o zpracování osobních údajů („DPA“) je součástí [obchodních podmínek](#) služby Salesbot.cz. Uzavírají ji společnost **Sales Robots s.r.o.**, IČ 09586563, Generála Šišky 2082/26, 143 00 Praha, e-mail info@salesbot.cz („Zpracovatel“), a zákazník služby, který ji přijme za sebe nebo za společnost, kterou je oprávněn zastupovat („Správce“). DPA se použije pouze na osobní údaje, které Sales Robots zpracovává pro zákazníka na jeho pokyn. U údajů o uživatelském účtu, platbách a provozní komunikaci vystupuje Sales Robots jako samostatný správce podle [zásad ochrany osobních údajů](#).

DPA vzniká elektronickým přijetím při registraci nebo následným potvrzením v aplikaci. Záznam o přijetí identifikuje jednatelkou osobu, zastupovanou společnost, čas a přesné verze dokumentů. Samotné zveřejnění návrhu na webu nebo pouhé používání služby bez tohoto kroku nepředstavuje přijetí nové verze DPA. DPA trvá po dobu, kdy Zpracovatel pro Správce zpracovává osobní údaje; ustanovení o mlčenlivosti, výmazu, odpovědnosti a součinnosti trvají po potřebnou dobu i poté. V otázkách zpracování osobních údajů má DPA přednost před obchodními podmínkami.

1. Předmět, rozsah a pokyny

Zpracovatel zpracovává údaje pouze pro účely, v rozsahu a po dobu uvedenou v **příloze 1** a výhradně na doložené pokyny Správce. Za pokyny se považují zejména nastavení a akce oprávněných uživatelů v aplikaci, požadavky přes jimi připojené MCP aplikace a písemné pokyny zaslané na info@salesbot.cz. Přístup připojené aplikace zřízený Správcem je jeho pokynem; poskytovatel takové aplikace se řídí vlastními podmínkami Správce.

Jiný účel nebo předání do třetí země Zpracovatel nepřidá bez pokynu Správce, ledaže mu to ukládá právo EU nebo členského státu. V takovém případě Správce předem informuje, pokud to zákon nezakazuje z důležitého veřejného zájmu. Má-li Zpracovatel za to, že pokyn porušuje GDPR nebo jiný předpis o ochraně údajů, bez zbytečného odkladu to Správci oznámí a dotčený krok odloží, dokud nebude pokyn vyjasněn.

Správce určuje právní základ zpracování, rozsah údajů a pravidla oslovení. Odpovídá za informační povinnost vůči dotčeným osobám, vyřízení jejich námitek a soulad obchodních sdělení s právem, včetně zákona č. 480/2004 Sb. Veřejná dostupnost údajů sama o sobě nedává souhlas s oslovením. Správce nevkládá zvláštní kategorie údajů podle čl. 9 GDPR ani údaje o trestních věcech, pokud k tomu nemá výslovně sjednaný režim.

Vznikne-li Zpracovateli újma v příčinné souvislosti s protiprávním pokynem nebo porušením povinností Správce, zejména chybějícím právním titulem ke zpracování nebo oslovení, nahradí ji Správce v rozsahu, v němž je přičitatelná jeho porušení a její náhradu právo připouští. Náhrada zahrnuje také přiměřené náklady řízení a právního zastoupení, náhrady vyplacené subjektům údajů nebo třetím osobám a pravomocně uložené pokuty, pokud a v rozsahu, v jakém jejich náhradu nevylučuje kogentní právo. Zpracovatel vznik, výši a souvislost nároku doloží a učiní přiměřená opatření k omezení újmy. Správce nehradí část újmy přičitatelnou vlastnímu porušení povinností Zpracovatele. Tím nejsou dotčena práva subjektů údajů, pravomoci dozorových úřadů ani vlastní odpovědnost Zpracovatele podle GDPR; ujednání nepřenáší veřejnoprávní odpovědnost za pokutu na jinou osobu.

2. Mlčenlivost, zabezpečení a AI

Přístup k osobním údajům mají jen osoby, které jej potřebují k poskytování služby a jsou vázány mlčenlivostí nebo zákonnou povinností mlčenlivosti. Zpracovatel zavede a pravidelně přezkoumává přiměřená technická a organizační opatření podle čl. 32 GDPR uvedená v **příloze 2**. Správce odpovídá za správu přístupů svých uživatelů, připojených účtů a MCP klíčů.

Zpracovatel nepoužije osobní údaje Správce k tréninku nebo vylepšování obecných AI modelů a zapojí pro práci s takovými údaji jen režimy podzpracovatelů, které to smluvně vylučují. Ze zpracování může vytvořit pouze nevratně anonymizované souhrny pro vlastní statistiky a zlepšování služby; výstup nesmí umožnit zpětnou identifikaci osob ani Správce. Dokud lze osobu nebo Správce určit, jde dál o údaje zpracovávané výhradně na pokyn Správce. Tento odstavec nedává oprávnění k využití identifikovatelných dat pro vlastní marketing ani k tréninku modelů.

3. Další zpracovatelé a předání mimo EHP

Správce uděluje obecné písemné povolení zapojit podzpracovatele uvedené v **příloze 3** pro tam popsané činnosti. Zpracovatel jim smluvně uloží povinnosti ochrany údajů alespoň ve stejném rozsahu, v jakém je sám zavázán touto DPA, a za jejich plnění vůči Správci nadále odpovídá. Zamýšlené přidání nebo nahrazení podzpracovatele oznámí e-mailem nebo v aplikaci nejméně **15 dní předem**. Správce může v této lhůtě vznést odůvodněnou námitku. Strany se pokusí nalézt přiměřené řešení; není-li možné, Správce může dotčenou službu před změnou ukončit bez sankce.

Přenosy osobních údajů mimo Evropský hospodářský prostor musí splňovat kapitulu V GDPR. Podle konkrétního příjemce se použije rozhodnutí Evropské komise o odpovídající ochraně (u USA EU–US Data Privacy Framework pouze pro aktuálně certifikovaného příjemce), nebo standardní smluvní doložky Evropské komise a potřebná doplňující opatření. Umístění serveru samo o sobě nevylučuje přístup ze třetí země. Mechanismus předání u jednotlivých podzpracovatelů je uveden v příloze 3.

4. Součinnost a incidenty

Zpracovatel s ohledem na povahu zpracování a dostupné informace pomáhá Správci vyřizovat žádosti o přístup, opravu, výmaz, omezení, přenositelnost a námitky. Žádost doručenou Zpracovateli postoupí Správci bez zbytečného odkladu a bez jeho pokynu na ni věcně neodpoví, pokud to nevyžaduje zákon. Na žádost poskytne přiměřenou součinnost pro posouzení vlivu na ochranu údajů, případnou předchozí konzultaci s úřadem a splnění oznamovacích povinností podle čl. 32–36 GDPR.

O porušení zabezpečení osobních údajů Správce, o kterém se Zpracovatel dozví, jej informuje bez zbytečného odkladu, nejpozději do **48 hodin** od zjištění. Oznámení obsahuje dostupné informace o povaze incidentu, dotčených údajích a osobách, pravděpodobných následcích a přijatých nebo navržených opatřeních; chybějící informace doplní postupně. Lhůta pro případné oznámení dozorovému úřadu podle čl. 33 GDPR zůstává povinností Správce.

Zpracovatel poskytne informace nezbytné k doložení plnění čl. 28 GDPR a umožní přiměřený audit Správcem nebo jím pověřeným nezávislým auditorem. Běžný audit lze provést nejvýše jednou za 12 měsíců na základě písemného oznámení doručeného nejméně 30 dní předem, způsobem chránícím údaje ostatních zákazníků a bezpečnost systému; doložení certifikací a dokumentace může předcházet místní kontrole. Mimořádný audit při důvodném podezření na závažné porušení, incidentu nebo požadavku dozorového úřadu tím není omezen. Každá strana nese své běžné náklady, není-li sjednáno jinak; zákonná práva Správce tím nejsou dotčena.

5. Konec zpracování, odpovědnost a změny

Po ukončení placeného předplatného nebo na výslovnou žádost Správce o smazání účtu Zpracovatel podle jeho volby osobní údaje vrátí nebo vymaže a odstraní jejich kopie, pokud právní předpis nevyžaduje další uchování. Správce může dostupná data exportovat před ukončením. Pokud si nevyžádá vrácení, použije se výmaz; produkční údaje zpracovávané pro Správce se vymažou nejpozději do **14 dní** od ukončení placeného předplatného nebo od žádosti o smazání. Pouhé skončení nezaplaceného zkušebního období tuto lhůtu nespouští; na takový účet se použije retenční doba podle přílohy 1 a zásad ochrany osobních údajů. Zálohy se odstraní v nejbližším přiměřeném retenčním cyklu, jsou mezitím izolovány od běžného použití a přístup k nim je omezen; konkrétní cyklus musí Zpracovatel Správci na vyžádání sdělit. Záznamy, které musí uchovat zákon (zejména účetní doklady), vede ve své samostatné roli správce pouze po zákonnou dobu.

Celková povinnost Zpracovatele nahradit Správci újmu podle této DPA je omezena částkou odpovídající platbám přijatým od Správce za službu Salesbot.cz za 12 měsíců před vznikem škodní události. Omezení se nevztahuje na újmu způsobenou úmyslně nebo z hrubé nedbalosti, na práva subjektů údajů podle čl. 82 GDPR ani na další odpovědnost, kterou podle kogentního práva nelze omezit, včetně ochrany přirozených práv člověka a práv slabší strany podle § 2898 občanského zákoníku. Tím nejsou omezeny pravomoci dozorových úřadů ani zákonné regresní nároky v rozsahu, v němž je nelze smluvně omezit. Toto ujednání se použije i přes přednost DPA před obchodními podmínkami.

Změny DPA, které vyžadují nové přijetí, Zpracovatel oznámí nejméně **15 dní před účinností**. Nová verze začne vůči Správci platit až po jejím doložitelném přijetí v aplikaci nebo jiným písemným způsobem. Dřívější verze zůstávají dostupné v

archivu právních dokumentů. Rozhodným jazykem je čeština; anglické znění slouží jako překlad. DPA se řídí českým právem, aniž jsou dotčena kogentní pravidla GDPR.

Příloha 1 — Popis zpracování

- **Předmět a účel:** provoz aplikace Salesbot.cz pro správu firem a obchodních kontaktů, vyhledávání na pokyn Správce, vedení CRM, návrhy a odesílání komunikace přes účty připojené Správcem, synchronizace zpráv, obohacení firemních údajů z ARES a veřejných firemních webů, zabezpečení a technická podpora.
- **Povaha operací:** získání, přenos, uložení, uspořádání, vyhledání, zobrazení, úprava, vyhodnocení, zpřístupnění oprávněným uživatelům a podzpracovatelům, omezení a výmaz.
- **Kategorie osob:** zaměstnanci a zástupci obchodních partnerů a potenciálních zákazníků Správce, osoby uvedené ve veřejných rejstřících, odesílatelé a příjemci zpráv a osoby přidané Správcem do CRM.
- **Kategorie údajů:** jméno, pracovní role a firma, lokalita, odkaz na LinkedIn profil, zdroj a datum získání, firemní či Správcem vložený e-mail a telefon, zprávy, poznámky, úkoly, stav obchodního vztahu, identifikátory účtů a záznam námitek. Volný text komunikace může obsahovat další údaje vložené Správcem nebo odesílatelem; zvláštní kategorie údajů nejsou zamýšleny.
- **Doba:** po dobu účtu a podle pravidel služby; záznam konkrétní osoby se běžně smaže po 12 měsících bez aktivity, s výjimkou obchodu ve fázi „Vyhráno“. Identifikátor na seznamu „Nekontaktovat“ se uchovává po dobu účtu, aby Správce neopakoval oslovení. Seznam platí v rámci zákaznického účtu nebo firmy, ke které Správce patří, nikoli napříč všemi zákazníky Salesbotu. Po skončení se použije článek 5.
- **Právní titul:** určuje Správce. Zpracovatel jej sám nestanoví a žádný výstup služby nepředstavuje potvrzení zákonnosti oslovení.

Příloha 2 — Technická a organizační bezpečnostní opatření

Stav opatření k 16. 10. 2026. Databázové zálohy se pořizují denně a uchovává se sedm posledních denních záloh. Přístupy podzpracovatelů a režimy dalších kopií a provozních záznamů se řídí článkem 3 a přílohou 3. Zpracovatel udržuje přiměřenou úroveň ochrany i při změně technického řešení.

2.1 Umístění a šifrování

- Databáze, autentizace, soubory a zálohy služby jsou v projektu Supabase v regionu **EU Stockholm (eu-north-1)**. Serverové funkce používají platformu Supabase; místo vykonávání jednotlivých funkcí závisí na jejich konfiguraci. Webová aplikace je hostována na Vercelu. Umístění hlavní databáze samo o sobě nevylučuje přístup dodavatelů ze třetích zemí; platí článek 3.
- Komunikace s aplikací, API a MCP serverem používá HTTPS/TLS. Databáze a zálohy jsou šifrovány na úrovni úložiště Supabase.
- Osobní MCP API klíče jsou v databázi uloženy jako otisk SHA-256, nikoli v čitelné podobě. Hesla spravuje Supabase Auth jako hash. Připojení LinkedInu a e-mailových schránek probíhá přes hostované přihlášení Unipile; Salesbot drží identifikátor propojeného účtu a neukládá přihlašovací hesla ani cookies těchto služeb.
- Tajné klíče interních služeb jsou drženy v zabezpečeném úložišti platformy, nikoli ve zdrojovém kódu aplikace.

2.2 Řízení přístupu

- Ve všech **tabulkách veřejného databázového schématu** je zapnuto zabezpečení na úrovni řádků (Row Level Security). Přístup zákazníků je oddělen podle účtu nebo firmy a rolí; oprávnění serverových funkcí se kontrolují samostatně.
- Služba rozlišuje běžného uživatele, administrátora firmy a správce služby. Privilegovaný přístup je omezen na oprávněné osoby podle jejich úkolů.
- Serverové funkce ověřují přihlášeného uživatele, interní tajný klíč plánovaných úloh nebo podpis či tajemství příchozího webhooku podle typu funkce. Klíč s plným přístupem k databázi je pouze na serveru, nikoli v prohlížeči.

- AI asistenti se připojují přes OAuth 2.1 nebo odvolatelný osobní API klíč. Akce podléhají hodinovým limitům; u jednorázových akcí přes MCP je schválení člověkem ve výchozím nastavení zapnuté. Nastavení kampaní a e-mailových schránek mohou mít vlastní pravidla schvalování.
- Registrace je chráněna reCAPTCHA. Blokováný uživatel nemá přístup k datům služby.

2.3 Zálohy, záznamy a výmaz

- Fyzická záloha databáze se pořizuje **jednou denně** a uchovává se **sedm posledních denních záloh** v regionu EU Stockholm. Tento sedmidenní cyklus se vztahuje na projektové databázové zálohy; provozní a bezpečnostní záznamy a další dodavatelské kopie podléhají pravidlům přílohy 3.
- Aplikace zaznamenává s časem a účtem provedené akce na LinkedInu, akce AI asistentů přes MCP, automatické odpovědi a odeslané e-maily. Provozní logy serverových funkcí a databáze vede Supabase; přístup k nim je omezen na oprávněné osoby.
- U CRM kontaktů se ukládají údaje nutné pro obchodní práci: jméno, profesní titulek, aktuální firma a role, lokalita, odkaz na profil, zdroj a datum získání, komunikace a poznámky uživatele. Profilové fotografie, texty „O mně“, vzdělání a starší pozice se v trvalém profilu kontaktu neukládají; vstupní data se při zápisu filtrují.
- Kontakty bez aktivity se po 12 měsících automaticky mažou podle přílohy 1. Námitka proti oslovení vede k výmazu běžných údajů a uchování nezbytného identifikátoru v seznamu „Nekontaktovat“ v rámci účtu nebo firmy Správce. Zrušení účtu spouští pozastavení a následný výmaz podle článku 5.

2.4 Ochrana provozu a incidenty

- Služba uplatňuje denní a hodinové limity LinkedIn akcí, postupný náběh nových účtů, nastavené pracovní hodiny, pauzy mezi vyhledáváními a možnost nouzového zastavení akcí účtu.
- Při incidentu se zaznamená čas zjištění, rozsah, dotčené účty, nápravná opatření a komunikace se Správcem. Osoby s přístupem k údajům jsou poučeny o mlčenlivosti a bezpečném nakládání s daty.

Příloha 3 — Schválení podzpracovatelé

Při poskytování služby Správci Zpracovatel využije níže uvedené smluvní režimy, a to pouze pro skutečně aktivované funkce a na základě smlouvy podle čl. 28 GDPR s příslušným podzpracovatelem. U Vercelu je pro zpracování podle této DPA smluvně požadován tarif Pro; Zpracovatel tento tarif zajistí před zahájením zákaznického zpracování prostřednictvím Vercelu. Údaje o oblastech, retenci a předání vycházejí z veřejných podmínek dodavatelů k 16. 10. 2026. Retence provozních a bezpečnostních záznamů se řídí uvedenou službou a její smlouvou; Zpracovatel poskytne aktuální přehled na vyžádání.

Supabase Pte. Ltd. (Singapur) — Databáze, autentizace, úložiště a serverové funkce; kontakty a CRM záznamy. Jádru projektu a zálohy EU Stockholm; podpora může mít přístup i mimo EHP. Přenosy do Singapur a USA kryjí SCC. Retence projektu do smazání, po smazání projektu odstranění dat do 30 dnů; zálohy podle tarifu. [DPA](#)

Vercel Inc. (USA), Pro — Hosting aplikace, MCP a OAuth proxy, technické logy; předávané požadavky a odpovědi mohou obsahovat údaje kontaktů a zpráv. Primární zpracování v USA, možné i jinde. [DPA](#) pro Pro obsahuje SCC, včetně modulu zpracovatel–podzpracovatel. Po ukončení výmaz v přiměřené době bez pevné lhůty. Pro je smluvně požadovaný tarif pro zákaznické zpracování podle této DPA.

Unipile SAS (Francie), API V1 — Připojení LinkedIn a e-mailových účtů, zprávy. Podle dodavatele jsou čitelná data zpracovávána ve Francii (Scaleway a OVHcloud). U V1 zprávy a konverzace do smazání připojeného účtu; u Microsoft/IMAP jen e-mailová metadata do smazání účtu, nikoli těla e-mailů; Gmail bez ukládání. Profily a metadata konverzací bez trvalého ukládání nebo cache podle [zásad dodavatele](#). Volitelné proxy mimo EU pouze směrují šifrovaný provoz bez dešifrovacích klíčů; případné předání podléhá článku 3. Smluvním podkladem je [DPA poskytovaná na vyžádání](#); bez jejího sjednání je zákaznické zpracování přes Unipile podle této DPA vyloučeno.

Google Cloud EMEA Limited (Irsko) — Placené Gemini API pro návrhy textů; omezené vstupy. Možné zpracování mimo EHP; SCC nebo rozhodnutí o odpovídající ochraně/DPF podle příjemce. Bez tréninku na vstupech v placeném režimu; bezpečnostní uchování promptů a výstupů 55 dní. [Podmínky](#) a [DPA](#).

OpenAI Ireland Ltd. — Placené API pro kontrolu a návrhy zpráv; omezené vstupy. Možné zpracování mimo EHP na základě SCC nebo odpovídající ochrany. API bez tréninku ve výchozím režimu; bezpečnostní logy běžně až 30 dní, další retence podle endpointu. [DPA](#).

Plus Five Five, Inc. (Resend; USA) — Odesílání servisních e-mailů a případné údaje příjemců. Uložená data v USA i při evropském odesílání; SCC, DPF jako další mechanismus. Běžné e-mailové logy 30 dní u Free/Pro/Scale, po ukončení účtu zbývající data do 90 dní. [DPA](#).

Entita Google: uvedená entita odpovídá české fakturační adrese podle veřejného seznamu Google, není-li smluvně sjednáno jinak. **Poznámka k rolím:** Stripe zajišťuje platby a předplatné, v kontrolovaném platebním toku získává údaje plátce a identifikátor uživatele, nikoli CRM kontakty Správce; proto zde není uveden jako jejich podzpracovatel. Analytické služby se týkají údajů, u nichž je Sales Robots samostatným správcem. Google Analytics se spouští pouze podle nastavení souhlasu s cookies a neslouží k práci s kontakty Správce.