

Smlouva o zpracování osobních údajů (DPA)

1. Smluvní strany

Zpracovatel: Ing. Radim Strejček IČO: 01944525 sídlem Kozmice 1, 256 01 Kozmice e-mail: info@automatigo.cz (dále jen „**Zpracovatel**“)

Správce: Podnikající fyzická nebo právnická osoba, která uzavřela se Zpracovatelem Smlouvu o poskytování služby Automatigo dle Obchodních podmínek (dále jen „**Smlouva**“). Identifikační údaje Správce jsou uvedeny v jeho uživatelském účtu v Administraci Služby. (dále jen „**Správce**“) (společně jen „**smluvní strany**“, samostatně též „**strana**“)

2. Úvodní ustanovení

2.1 Tato DPA upravuje zpracování osobních údajů, které Zpracovatel zpracovává **jménem Správce** v rámci poskytování Služby Automatigo (zejména provozu Modulů na webových stránkách / e-shopu Správce).

2.2 Tato DPA tvoří nedílnou součást Smlouvy uzavřené mezi Zpracovatelem a Správce. V případě rozporu mezi DPA a Obchodními podmínkami má pro otázky zpracování osobních údajů přednost DPA.

2.3 Smluvní strany prohlašují, že:

- **Správce** je správcem osobních údajů ve smyslu čl. 4 odst. 7 GDPR — určuje účel a prostředky zpracování osobních údajů svých koncových zákazníků,
- **Zpracovatel** je zpracovatelem ve smyslu čl. 4 odst. 8 GDPR — zpracovává osobní údaje jménem Správce dle jeho pokynů.

2.4 Tato DPA se vztahuje **pouze** na zpracování, při kterém Zpracovatel vystupuje jako zpracovatel jménem Správce. Nevztahuje se na zpracování, při kterém je Zpracovatel sám správcem (např. fakturace, podpora vůči Správci, marketing služby Automatigo) — toto upravují **Zásady ochrany osobních údajů** Zpracovatele.

3. Definice

Pojmy s velkým písmenem mají stejný význam jako v Obchodních podmínkách (zejména **Modul, Služba, Administrace, Externí poskytovatelé**). Dále:

3.1 GDPR — nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

3.2 Osobní údaj — jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě ve smyslu čl. 4 odst. 1 GDPR.

3.3 Zpracování — operace nebo soubor operací s osobními údaji ve smyslu čl. 4 odst. 2 GDPR.

3.4 Subjekt údajů — fyzická osoba, jejíž osobní údaje jsou zpracovávány. Pro účely této DPA zejména koncoví zákazníci, návštěvníci nebo registrovaní uživatelé webových stránek / e-shopu Správce.

3.5 Porušení zabezpečení — porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 GDPR (zejména náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předávaných nebo zpracovávaných osobních údajů).

3.6 Podzpracovatel — třetí strana, kterou Zpracovatel zapojuje do zpracování osobních údajů na základě této DPA.

4. Předmět, doba, povaha a účel zpracování

4.1 Předmět zpracování: osobní údaje koncových zákazníků, návštěvníků nebo registrovaných uživatelů webových stránek / e-shopu Správce zpracovávané Moduly Automatigo aktivovanými Správcem.

4.2 Doba zpracování: po dobu trvání Smlouvy o poskytování Služby Automatigo. Po jejím ukončení postupuje Zpracovatel dle čl. 14.

4.3 Povaha zpracování: automatizované zpracování zahrnující zejména sběr, ukládání, agregaci, analýzu, vyhodnocování interakcí a zobrazování personalizovaného obsahu.

4.4 Účel zpracování: plnění Smlouvy mezi Zpracovatelem a Správcem — zejména provoz Modulů (popup formuláře, cart upsell, exit intent, cart reminder, tracking událostí, AI funkcionality apod.), sběr analytických dat pro Správce a poskytování statistik využití Modulů.

4.5 Druh osobních údajů a kategorie subjektů údajů jsou specifikovány v Příloze A.

5. Povinnosti Zpracovatele

Zpracovatel se zavazuje, že:

5.1 Pokyny Správce. Bude zpracovávat osobní údaje **pouze na základě doložených pokynů** Správce — uzavření této DPA, Smlouvy a nastavení Modulů v Administraci se považuje za doložený pokyn. Pokud bude Zpracovatel ze zákona EU nebo členského státu povinen zpracovat údaje nad rámec pokynů, informuje o tom Správce před zpracováním (ledaže to právní předpis zakazuje).

5.2 Mlčenlivost. Zajistí, že osoby oprávněné zpracovávat osobní údaje (zaměstnanci, spolupracovníci, případně podzpracovatelé) jsou vázány **povinností mlčenlivosti** nebo se na ně vztahuje zákonná povinnost mlčenlivosti.

5.3 Bezpečnost. Přijme všechna **technická a organizační opatření** vyžadovaná čl. 32 GDPR. Souhrn opatření je v **Příloze B**.

5.4 Podzpracovatelé. Zapojuje další zpracovatele pouze za podmínek čl. 8 a Přílohy C.

5.5 Práva subjektů údajů. S přihlédnutím k povaze zpracování poskytne Správci v přiměřeném rozsahu **technickou součinnost** při výkonu práv subjektů údajů dle GDPR čl. 12–22 (přístup, oprava, výmaz, omezení, přenositelnost, námitka).

5.6 Bezpečnostní incidenty. Postupuje dle čl. 9.

5.7 DPIA. S přihlédnutím k povaze zpracování a jemu dostupným informacím **pomáhá** Správci s plněním povinností dle čl. 32–36 GDPR (zabezpečení, oznamování porušení, posouzení vlivu na ochranu osobních údajů, předchozí konzultace).

5.8 Vrácení nebo výmaz. Po skončení poskytování Služby naloží s osobními údaji dle čl. 14.

5.9 Spolupráce při auditu. Poskytne Správci v přiměřeném rozsahu informace nezbytné k prokázání souladu s povinnostmi dle této DPA a GDPR čl. 28; postup auditu upravuje čl. 12.

5.10 Upozornění na nesoulad. Pokud se Zpracovatel domnívá, že pokyn Správce porušuje GDPR nebo jiné předpisy o ochraně osobních údajů, **bez zbytečného odkladu o tom Správce informuje**.

6. Povinnosti Správce

Správce se zavazuje, že:

- 6.1** Bude zpracovávat osobní údaje v souladu s GDPR a platnými právními předpisy a bude mít pro každé předání osobních údajů Zpracovateli platný **právní titul** (zejména souhlas subjektů údajů, oprávněný zájem, plnění smlouvy s koncovým zákazníkem).
- 6.2** Bude poskytovat subjektům údajů odpovídající **informace o zpracování** (zejména informace dle čl. 13 a 14 GDPR — kdo zpracovává, za jakým účelem, kdo jsou příjemci včetně Zpracovatele Automatigo a jeho podzpracovatelů).
- 6.3** Bude nastavovat Moduly a jejich konfiguraci tak, aby zpracování bylo **přiměřené účelu** a v souladu se zásadami GDPR (minimalizace údajů, omezení účelu, přesnost, omezení doby uložení).
- 6.4** Bude **bez zbytečného odkladu** informovat Zpracovatele o žádostech subjektů údajů, které vyžadují technickou součinnost Zpracovatele (zejména žádost o výmaz, přenos údajů, omezení zpracování).
- 6.5** Neposkytne Zpracovateli **citlivé osobní údaje** ve smyslu čl. 9 a 10 GDPR (zvláštní kategorie, údaje o trestných činech), pokud k tomu Zpracovatel nedal výslovný předchozí souhlas — Služba Automatigo není designována pro zpracování takových údajů.
- 6.6** Odpovídá za **zákonost** instrukcí, které dává Zpracovateli, a za nastavení Modulů.

7. Bezpečnost zpracování

- 7.1** Zpracovatel přijímá vhodná technická a organizační opatření dle čl. 32 GDPR k zajištění úrovně zabezpečení odpovídající danému riziku, s ohledem na stav techniky, náklady, povahu, rozsah, kontext a účely zpracování i pravděpodobnosti a závažnosti rizik pro práva a svobody subjektů údajů.
- 7.2** Souhrn aktuálních bezpečnostních opatření je uveden v **Příloze B**. Zpracovatel je oprávněn opatření v čase měnit, pokud nová opatření poskytují **alespoň stejnou** úroveň ochrany.

8. Podzpracovatelé

- 8.1 Obecný souhlas.** Správce uděluje Zpracovateli **obecný souhlas** se zapojením podzpracovatelů uvedených v **Příloze C** pro účely poskytování Služby (zejména Google / Firebase, OpenAI, Anthropic, Make.com, Comgate, případně další Externí poskytovatelé).
- 8.2 Nový nebo nahrazený podzpracovatel.** Pokud Zpracovatel zamýšlí zapojit dalšího podzpracovatele nebo nahradit stávajícího, oznámí to Správci **alespoň 30 dnů předem** prostřednictvím Administrace, e-mailem nebo aktualizací této DPA na webu Zpracovatele. Správce má právo proti změně podzpracovatele vznést **odůvodněnou písemnou námitku** ve lhůtě 30 dnů od oznámení. V takovém případě smluvní strany v dobré víře jednají o řešení; pokud k dohodě nedojde, Správce je oprávněn ukončit Smlouvu výpovědí s 30denní výpovědní dobou.
- 8.3 Smluvní povinnosti podzpracovatele.** Zpracovatel uloží každému podzpracovateli **stejně povinnosti** v oblasti ochrany osobních údajů, jaké má sám podle této DPA, zejména povinnost přijmout opatření dle čl. 32 GDPR a omezení podzpracování.
- 8.4 Odpovědnost.** Pokud podzpracovatel nesplní své povinnosti v oblasti ochrany osobních údajů, **odpovídá Správci za plnění povinností tohoto podzpracovatele** Zpracovatel.

9. Porušení zabezpečení osobních údajů

- 9.1 Oznámení Správci.** Pokud Zpracovatel zjistí Porušení zabezpečení osobních údajů, oznámí to Správci **bez zbytečného odkladu**, zpravidla do **72 hodin** od zjištění, a to e-mailem na kontaktní adresu Správce uvedenou v Administraci.
- 9.2 Obsah oznámení.** Oznámení obsahuje, je-li to možné, alespoň:

- popis povahy porušení (kategorie a přibližný počet dotčených subjektů a záznamů),
- jméno a kontakt na osobu schopnou poskytnout další informace,
- popis pravděpodobných důsledků,
- popis opatření přijatých nebo navrhovaných k řešení a zmírnění následků.

Pokud nelze informace poskytnout najednou, Zpracovatel je doplní postupně bez zbytečného odkladu.

9.3 Zpracovatel vede evidenci Porušení zabezpečení a poskytne ji Správci na vyžádání.

9.4 Povinnost ohlásit Porušení zabezpečení **dozorovému úřadu** (ÚOOÚ) a případně subjektům údajů zůstává na Správci dle čl. 33 a 34 GDPR; Zpracovatel poskytuje Správci součinnost.

10. Mezinárodní přenosy

10.1 Někteří podzpracovatelé (zejména Google v rámci některých služeb, OpenAI, Anthropic) mohou zpracovávat osobní údaje mimo Evropskou unii nebo Evropský hospodářský prostor, typicky ve **Spojených státech amerických**.

10.2 Pro takové přenosy zajišťuje Zpracovatel **přiměřené záruky dle čl. 44 a násl. GDPR**, zejména:

- Standardní smluvní doložky (SCC) schválené Evropskou komisí, nebo
- **EU-US Data Privacy Framework (DPF)**, pokud je daný podzpracovatel certifikován.

10.3 Konkrétní mechanismus přenosu pro jednotlivé podzpracovatele je uveden v **Příloze C** nebo bude Správci poskytnut na vyžádání.

11. Práva subjektů údajů

11.1 Pokud subjekt údajů uplatní svá práva přímo u Zpracovatele, Zpracovatel jej **odkáže na Správce** jako primárně odpovědný subjekt a o této skutečnosti **bez zbytečného odkladu informuje Správce**.

11.2 Zpracovatel poskytuje Správci přiměřenou technickou součinnost při výkonu práv subjektů údajů – zejména:

- **přístup** – export dat ve strojově čitelném formátu,
- **oprava** – možnost úpravy prostřednictvím Administrace,
- **výmaz** – odstranění údajů Subjektu na pokyn Správce,
- **omezení zpracování** – zablokování dalšího zpracování konkrétních záznamů,
- **přenositelnost** – strukturovaný, běžně používaný a strojově čitelný formát.

11.3 Zpracovatel je oprávněn Správci přiměřeně účtovat administrativní náklady na rozsáhlou součinnost (nad rámec standardních operací Administrace).

12. Audit

12.1 Zpracovatel poskytne Správci na žádost informace nezbytné k prokázání splnění povinností dle této DPA a GDPR čl. 28, a to v rozsahu, který je přiměřený.

12.2 Zpracovatel umožňuje audit prováděný Správcem nebo jím pověřeným auditorem **maximálně 1x ročně**, není-li dán závažný důvod pro vyšší frekvenci (např. zjištěné porušení). Správce oznámí audit Zpracovateli **alespoň 30 dnů předem**.

12.3 Audit probíhá způsobem, který **nenarušuje běžný provoz** Služby ani bezpečnost údajů dalších klientů Zpracovatele. Zpracovatel může požadovat uzavření dohody o mlčenlivosti s auditorem.

12.4 Náklady auditu nese Správce, ledaže audit prokáže podstatné porušení povinností Zpracovatele.

12.5 Zpracovatel je oprávněn auditní požadavky splnit poskytnutím **certifikací třetích stran** (např. SOC 2, ISO 27001) nebo auditních zpráv svých podzpracovatelů, pokud pokrývají předmět auditu.

13. Odpovědnost

13.1 Smluvní strany odpovídají subjektům údajů za škody způsobené porušením GDPR podle čl. 82 GDPR.

13.2 Vzájemná odpovědnost mezi Správce a Zpracovatelem se řídí Smlouvou a Obchodními podmínkami (zejména čl. 7.5 – limit odpovědnosti) v rozsahu, ve kterém to GDPR nebrání.

13.3 Zpracovatel není odpovědný za škody vzniklé v důsledku:

- pokynů Správce v rozporu s GDPR,
- nesprávné konfigurace Modulů Správce,
- absence právního titulu pro zpracování,
- porušení povinností Správce dle čl. 6.

14. Ukončení a osud osobních údajů

14.1 Po skončení Smlouvy o poskytování Služby Zpracovatel **dle volby Správce** sdělené nejpozději do 30 dnů od ukončení Smlouvy:

- **vrátí** osobní údaje Správci ve strojově čitelném formátu (CSV/JSON), **nebo**
- údaje **vymaže** a smaže všechny existující kopie.

14.2 Pokud Správce neudělí pokyn ve lhůtě dle čl. 14.1, je Zpracovatel oprávněn osobní údaje **vymazat**.

14.3 Zpracovatel je oprávněn údaje uchovávat **i po skončení Smlouvy**, pokud to vyžaduje právo EU nebo členského státu (zejména účetní a daňové předpisy – viz Zásady ochrany osobních údajů čl. 7). Po dobu uchování se nadále aplikují bezpečnostní opatření dle této DPA.

14.4 Logy a zálohy. Údaje obsažené v rotujících bezpečnostních zálohách a logách budou postupně **přepsány nebo smazány** v rámci běžných retenčních cyklů (typicky do 90 dnů).

15. Závěrečná ustanovení

15.1 Tato DPA nabývá účinnosti uzavřením Smlouvy mezi Správce a Zpracovatelem a trvá po celou dobu jejího trvání. Ustanovení o zachování důvěrnosti, vrácení / výmazu údajů a odpovědnosti zůstávají v platnosti i po skončení DPA.

15.2 Změny DPA. Zpracovatel je oprávněn DPA jednostranně změnit, zejména pokud to vyžaduje změna právních předpisů, rozhodnutí dozorového úřadu, technologická změna Služby nebo přidání podzpracovatele. Změny se oznamují alespoň **30 dnů předem** prostřednictvím Administrace, e-mailem nebo zveřejněním na webu. Pokud Správce s podstatnou změnou nesouhlasí, je oprávněn ukončit Smlouvu výpovědí dle čl. 8.2.

15.3 Rozhodné právo a soudní příslušnost. Tato DPA se řídí právním řádem **České republiky** a předpisy EU o ochraně osobních údajů. Případné spory rozhodují příslušné soudy České republiky.

15.4 Vztah k jiným dokumentům. Pro otázky neupravené touto DPA platí Obchodní podmínky a Zásady ochrany osobních údajů Zpracovatele.

15.5 Salvatorská klauzule. Pokud se některé ustanovení této DPA stane neplatným nebo nevymahatelným, nemá to vliv na platnost ostatních ustanovení.

15.6 Účinnost. Tato DPA nabývá účinnosti dne **13. 5. 2026**.

Příloha A – Předmět zpracování, kategorie údajů a subjektů údajů

A.1 Druh osobních údajů

V závislosti na konkrétních Modulech aktivovaných Správcem mohou být zpracovávány:

- **Identifikátory online:** cookies, identifikátor relace (session), identifikátor zařízení / prohlížeče, IP adresa
- **Technické údaje:** typ a verze prohlížeče, operační systém, jazyk, časová zóna, rozlišení obrazovky, doména
- **Údaje o chování na webu:** navštívené stránky, doba na stránce, kliknutí, otevření popupu, opuštění košíku, scroll depth, časové známky interakcí
- **Údaje vložené koncovým zákazníkem do formulářů Modulů:** zejména e-mailová adresa (newsletter, cart reminder), případně jméno, telefon, údaje o objednavce (pouze pokud konkrétní Modul tyto údaje vyžaduje)
- **Údaje o produktech v košíku** (pro Moduly cart upsell, cart reminder): identifikátory produktů, množství, ceny, varianty
- **Informace o transakci** (pouze pokud Modul vyžaduje): stav objednávky, identifikátor objednávky

A.2 Kategorie subjektů údajů

- **Návštěvníci** webových stránek / e-shopu Správce (anonymní zákazníci)
- Registrovaní zákazníci e-shopu Správce
- **Odběratelé newsletteru** Správce (z formulářů Modulů Automatigo)

A.3 Účel zpracování

- Provoz Modulů (popup formuláře, exit-intent, cart upsell, cart reminder, atd.)
- Sběr a vyhodnocení analytických údajů pro Správce (kliknutí, konverze, retence)
- Personalizace obsahu zobrazovaného Modulem koncovému zákazníkovi
- AI funkcionality (pokud Správce aktivuje příslušné Moduly)

A.4 Doba zpracování

- Po dobu trvání Smlouvy
- Údaje pro export 30 dnů po ukončení (viz čl. 14)
- Účetní a obdobné údaje dle zákonných retenčních lhůt

Příloha B – Bezpečnostní opatření

Zpracovatel přijímá zejména následující technická a organizační opatření:

B.1 Technická opatření

- **Šifrování přenosu:** veškerá komunikace HTTPS / TLS 1.2+
- **Šifrování dat v klidu:** Firebase / Google Cloud at-rest encryption
- **Bezpečnostní pravidla:** Firestore Rules a Storage Rules s ověřením autentizace a oprávnění
- **Autentizace:** Firebase Authentication s povinným ověřením e-mailu pro administrátorské účty; podpora vícefaktorové autentizace
- **Firestore App Check** (až bude plně aktivováno): ochrana proti neoprávněnému použití API
- **Logování přístupů** k systému a auditní záznamy
- **Pravidelné aktualizace** softwaru a bezpečnostních knihoven
- Hodinové automatizované zálohování databáze Firestore; denní snapshot s retencí 30 dnů
- **Oddělení dat klientů** logickou izolací na úrovni databáze (každý Správce má vlastní namespace v kolekci)
- Monitorování a logování abnormálního provozu

B.2 Organizační opatření

- **Omezený přístup** pouze pro nezbytný personál (princip "least privilege" / "need-to-know")
- **Mlčenlivost** zaměstnanců a spolupracovníků
- Smluvní zajištění podzpracovatelů
- Pravidelná interní revize bezpečnostních postupů
- **Plán reakce** na bezpečnostní incidenty (incident response)
- **Procesy** pro vyřízení žádostí subjektů údajů

B.3 Opatření k zajištění důvěrnosti, integrity, dostupnosti a odolnosti

- **Důvěrnost:** šifrování, řízení přístupu
- **Integrita:** ověření autentizace u zápisů, validace dat
- **Dostupnost:** redundantní hosting (Firestore / Google Cloud), automatické failover
- **Obnova po výpadku:** zálohy a testování restore procedur

Příloha C – Schválení podzpracovatelé

Tabulka schválených podzpracovatelů ke dni účinnosti DPA. Aktuální verze v Administraci nebo na webu Zpracovatele.

Podzpracovatel	Účel zpracování	Region zpracování	Mechanismus přenosu
Google Ireland Ltd. / Google LLC (Firebase, Google Cloud, Cloud Functions, Cloud Storage, Authentication, Firestore)	Hosting Služby, databáze, autentizace, výpočet, úložiště	EU (Irsko) + USA	SCC + EU-US DPF
Google Ireland Ltd. (Google Analytics 4 – pokud Správce aktivuje)	Webová analytika	EU + USA	SCC + EU-US DPF
Anthropic, PBC	AI funkcionality (Claude API)	USA	SCC
OpenAI, OpenAI Ireland Ltd.	AI funkcionality (GPT API)	EU (Irsko) + USA	SCC + EU-US DPF
Make.com (Make.com s.r.o. / Celonis SE)	Automatizační workflow (pokud Modul vyžaduje)	EU	– (EU)
Comgate, a.s.	Platební brána (pouze pro platby v rámci Modulů, pokud Správce aktivuje)	Česká republika	– (EU)
Shoptet a.s.	Integrace s e-shop platformou Správce (jen čtení konfigurace e-shopu, pokud Správce povolí)	Česká republika	– (EU)

Zpracovatel může seznam podzpracovatelů aktualizovat dle čl. 8.2 DPA.

Podpisy

Tato DPA je uzavírána v elektronické podobě a vstupuje v platnost okamžikem uzavření Smlouvy o poskytování Služby (potvrzení objednávky, aktivace Modulu, zahájení využívání Služby).

V případě potřeby písemného potvrzení může kterákoli strana požádat o vyhotovení podepsané verze; Zpracovatel takovou žádost vyřídí bez zbytečného odkladu na adrese info@automatigo.cz.