

Smlouva o zpracování osobních údajů

Příloha ke smlouvě o poskytování služby GPcloud.app podle článku 28 GDPR

Tento dokument je pracovní návrh určený pro B2B poskytování služby GPcloud.app. Před použitím musí být doplněny zbývající provozní údaje a text musí zkontrolovat český advokát se zkušeností se SaaS a ochranou osobních údajů.

Smluvní strany

Role	Identifikační údaje
Zpracovatel	Jakub Jursík, IČO 73 860 701, se sídlem Litoměřická 405/9, 190 00 Praha, podnikající fyzická osoba evidovaná v Registru osob (ARES), zastoupený Jakubem Jursíkem
Správce	[DOPLNIT obchodní firma, IČO, DIČ, sídlo, zápis a zástupce Zákazníka]

Tato smlouva upravuje zpracování osobních údajů Poskytovatelem jako zpracovatelem jménem Zákazníka jako správce. Pojmy mají význam podle nařízení Evropského parlamentu a Rady EU 2016 679.

1 Předmět a doba zpracování

Zpracovatel zpracovává osobní údaje pouze za účelem zřízení, provozu, podpory, zabezpečení, zálohování a ukončení služby GPcloud.app a pouze po dobu smlouvy a následných retenčních lhůt. Zpracování probíhá na doložené pokyny Správce vyjádřené smlouvou, konfigurací služby nebo oprávněným požadavkem.

2 Povaha a účel zpracování

Oblast	Operace a účel
Správa uživatelů	Uložení identifikačních a kontaktních údajů, autentizace, role a audit přístupů.
HelpDesk	Příjem, uložení, třídění a vyřízení komunikace a příloh.
Docházka	Evidence příchoďů, odchodů, práce mimo pracoviště, oprav a výkazů.
Dovolené a absence	Evidence žádostí, schválení, termínů a zůstatků.
Obchodní moduly	Evidence zákazníků, zakázek, dokumentů, plateb a integrací podle aktivních modulů.
Zálohování	Šifrované kopie pro obnovu dostupnosti a integrity služby.

3 Kategorie subjektů a údajů

Subjekty údajů	Příklady údajů
Zaměstnanci a spolupracovníci Správce	Jméno, pracovní kontakt, osobní číslo, organizační zařazení, role, pracovní události, docházka a plánované absence.
Zákazníci a kontaktní osoby	Identifikační a kontaktní údaje, komunikace, objednávky, zakázky a fakturační údaje.

Subjekty údajů	Příklady údajů
Uživatelé služby	Identifikátory účtu, oprávnění, přihlašovací a auditní metadata, IP adresa a bezpečnostní události.
Řidiči a uživatelé vozidel	Údaje potřebné pro zápůjčku a předávací dokumentaci podle konfigurace modulu.

Zvláštní kategorie osobních údajů nejsou standardním účelem služby. Správce zejména nevkládá diagnózy nebo podrobné zdravotní informace do poznámek k absencím. Jejich zpracování vyžaduje samostatné posouzení, právní základ, minimalizaci a výslovné písemné nastavení.

4 Povinnosti Zpracovatele

1. Zpracovávat údaje pouze podle doložených pokynů Správce, ledaže zpracování vyžaduje právo Unie nebo členského státu.
2. Zajistit, aby osoby s přístupem byly vázány mlčenlivostí.
3. Přijmout technická a organizační opatření odpovídající rizikům.
4. Pomáhat Správci při vyřizování práv subjektů údajů, posuzování incidentů, DPIA a konzultacích s dozorovým úřadem v rozsahu dostupných informací.
5. Vést přiměřené záznamy a poskytnout informace potřebné k doložení souladu.
6. Umožnit audit v přiměřeném rozsahu po předchozí dohodě a při zachování bezpečnosti ostatních zákazníků.
7. Neprodleně upozornit na pokyn, který podle názoru Zpracovatele porušuje právní předpis o ochraně údajů.

5 Povinnosti Správce

1. Zajistit právní titul, informační povinnost a správnost pokynů.
2. Nastavit role a oprávnění podle zásady nejmenších oprávnění.
3. Nevkládat údaje, které nejsou potřebné pro sjednaný účel.
4. Spravovat životní cyklus uživatelských účtů a chránit přístupové údaje.
5. Informovat Zpracovatele o požadavcích, rizicích a zvláštních režimech zpracování.

6 Další zpracovatelé

Správce uděluje obecné písemné povolení k zapojení dalších zpracovatelů uvedených v aktuálním seznamu subzpracovatelů. Zpracovatel oznámí zamýšlenou změnu nejméně 30 dnů předem, není li naléhavá bezpečnostní potřeba. Správce může z vážných důvodů ochrany údajů vznést námitku.

Subzpracovatel	Účel	Umístění dat	Stav
OBSIDIAN, s.r.o., IČO 26 713 489	Hosting aplikace a databáze	Česká republika	W2 Hosting; ověřit podle smlouvy nebo faktury
Backblaze, Inc. B2 Cloud Storage	Externí zálohy pro obnovu	Region EU Central	AKTIVNÍ; doplnit právní posouzení případného přenosu
Poskytovatel transakčního e mailu	Odesílání systémové komunikace	[DOPLNIT]	DOPLNIT
iDoklad a další integrace	Pouze při aktivaci zákazníkem	Podle konkrétní služby	VOLITELNÉ

7 Bezpečnostní incidenty

Zpracovatel oznámí Správci porušení zabezpečení osobních údajů bez zbytečného odkladu poté, co se o něm dozví. První oznámení může být předběžné a bude postupně doplňováno. Obsahuje dostupný popis povahy incidentu, dotčených kategorií, pravděpodobných následků, přijatých opatření a kontaktní místo.

8 Předávání mimo Evropský hospodářský prostor

Zpracovatel bez předchozího právního posouzení a odpovídajícího mechanismu nepředává osobní údaje mimo Evropský hospodářský prostor. Je-li předání nezbytné, použije rozhodnutí o odpovídající ochraně, standardní smluvní doložky nebo jiný právně přípustný mechanismus a podle potřeby doplňující opatření.

9 Vrácení a odstranění údajů

Po ukončení služby Zpracovatel umožní Správci export po dobu 30 dnů, není-li sjednáno jinak. Následně odstraní údaje z aktivních systémů. Kopie v zálohách se odstraní uplynutím retenční doby, navrhované nejpozději do 12 měsíců, není-li právním předpisem nebo smlouvou vyžadováno jiné uchování. Po dobu retence nejsou záložní údaje používány k jinému účelu než obnově a zabezpečení.

10 Audity a součinnost

Správce může jednou ročně požádat o přiměřené doložení opatření nebo audit. Přednost mají dokumenty, protokoly a vzdálené ověření. Kontrola na místě vyžaduje přiměřené oznámení, mlčenlivost a nesmí narušit bezpečnost ani práva jiných zákazníků. Mimořádný audit po incidentu tím není dotčen.

Příloha A Technická a organizační opatření

Oblast	Navržená opatření	Stav před prodejem
Izolace	Samostatná instance, databáze, konfigurace, logy a zálohy každého zákazníka.	Implementováno architekturou
Přístupy	Role, oprávnění, audit a zákaz sdílení účtů.	Implementováno; MFA pro administrátory doplnit
Přenos	TLS pro web a integrační komunikaci.	Produkční certifikáty provozně ověřovat
Zálohy	Konzistentní dump, manifest, SHA 256, oddělené externí EU úložiště, omezený klíč a Object Lock.	Nasazeno na DEV, RG a AMR; nezměnitelná retence ověřena
Obnova	Ověření archivu, dry run, obnova souborů a databázový restore drill.	Ověřeno 9. 9. 2026 na chráněné externí kopii AMR
Monitoring	Zdravotní kontroly, logy scheduleru a upozornění při selhání.	Logování zavedeno; upozornění doplnit
Vývoj	Oddělené DEV a produkční prostředí, testy a řízené release.	Používáno
Minimalizace	Konfigurovatelné moduly, role a omezení nepotřebných údajů.	Průběžně
Likvidace	Export, deaktivace instance a odstranění podle retenčního cyklu.	Proces popsán v provozní příručce; ověřovat při ukončení

Příloha B Kontaktní údaje

Role	Kontakt
Kontakt Správce pro ochranu údajů	Doplň Zákazník
Kontakt Zpracovatele pro bezpečnost a incidenty	info@gpcloud.app
Provozní podpora	info@gpcloud.app

Právní zdroje pro revizi

- Nařízení Evropského parlamentu a Rady EU 2016 679, zejména články 28, 32 a 33.
- Úřad pro ochranu osobních údajů, metodické informace k postavení zpracovatele a cloudovým službám.
- Občanský zákoník, zejména pravidla smluvní odpovědnosti a omezení předchozího vzdání se náhrady újmy.