Smlouva o zpracování osobních údajů služby bim-pulse CDE connector

Verze 1.0 · účinnost od 1. 9. 2026 · vydáno 3. 8. 2026 · příloha „Všeobecných obchodních podmínek” — uzavírá se jejich akceptací, samostatný podpis se nevyžaduje

---

1. Strany, předmět a postavení

1.1 **Zpracovatelem** je Buildify Digital s.r.o., IČO 295 41 743, se sídlem Korunní 2569/108, Vinohrady, 101 00 Praha 10, zapsaná v obchodním rejstříku pod C 447453 vedená u Městského soudu v Praze (dále jen „**provozovatel**”); e-mail kluch@buildify.cz, který je zároveň kontaktním místem pro ochranu osobních údajů, další údaje v dokumentu „Údaje o provozovateli”. **Správcem** je zákazník — podnikatel, kterému byla podle „Všeobecných obchodních podmínek” (dále jen „**VOP**”) zřízena Organizace ve službě bim-pulse.

1.2 Tato smlouva je přílohou VOP, uzavírá se jejich akceptací a upravuje práva a povinnosti stran podle čl. 28 odst. 3 nařízení (EU) 2016/679 („**GDPR**”). Nedílnou součástí jsou **Příloha 1** (popis zpracování), **Příloha 2** (opatření podle čl. 32 GDPR) a **Příloha 3** (další zpracovatelé); pojmy zde nedefinované mají význam podle VOP.

1.3 V otázkách ochrany osobních údajů má tato smlouva přednost před VOP, v ostatním platí VOP; individuálním ujednáním nelze omezit kogentní požadavky čl. 28 GDPR.

1.4 Vystupuje-li zákazník sám jako zpracovatel pro investora nebo jiného účastníka výstavby, použije se tato smlouva obdobně a provozovatel je dalším zpracovatelem podle čl. 28 odst. 4 GDPR. Zákazník prohlašuje, že je oprávněn provozovatele zapojit a že jeho pokyny odpovídají pokynům, které sám obdržel.

1.5 **Poskytovatelé CDE zvolení zákazníkem nejsou dalšími zpracovateli provozovatele** — jsou samostatnými správci nebo zpracovateli zákazníka. Provozovatel k nim přistupuje výhradně jménem zákazníka na základě přístupových údajů nebo souhlasu OAuth, které zákazník poskytl.

1.6 U fakturačních a účetních údajů, provozních a bezpečnostních záznamů a údajů pro obhajobu právních nároků je provozovatel **samostatným správcem**; toto zpracování upravují „Zásady ochrany osobních údajů”.

---

2. Pokyny správce

2.1 Provozovatel zpracovává osobní údaje **výhradně na základě doložených pokynů zákazníka**, včetně pokynů k předání do třetí země, ledaže mu zpracování ukládá právo Evropské unie nebo České republiky; v takovém případě zákazníka předem informuje, nezakazuje-li to daný předpis.

2.2 Doloženým pokynem jsou tato smlouva a VOP, individuální písemné ujednání, potvrzený požadavek z kontaktní adresy uvedené v účtu, volání rozhraní API a zejména **konfigurace provedená v aplikaci** — účty a role, Páry a přístupové údaje k CDE, Mapování složek, plán synchronizace, sdílené odkazy včetně volby zobrazovat názvy souborů, pozvánky, reporty a funkce exportu a výmazu. Konfigurace provedená uživatelem zákazníka je pokynem zákazníka bez ohledu na jeho vnitřní rozdělení oprávnění; systém ji zaznamenává, což strany považují za dostatečné doložení.

2.3 **Předání mimo EU a EHP.** Provozovatel zpracovává osobní údaje v Evropské unii (region europe-west3, Frankfurt). Mimo EU/EHP je předá jen na pokyn zákazníka — zejména jeho volbou poskytovatele CDE —, předvídá-li to Příloha 3, nebo ukládá-li to právní předpis, a vždy jen se zárukou podle kapitoly V GDPR, tedy s rozhodnutím o odpovídající ochraně nebo se standardními smluvními doložkami podle rozhodnutí Komise (EU) 2021/914. **Za právní titul předání vyvolaného volbou poskytovatele CDE odpovídá zákazník.**

2.4 Je-li rozpor pokynu s předpisy o ochraně osobních údajů zjevný, provozovatel na to zákazníka neprodleně upozorní a může provedení pozastavit do potvrzení, změny nebo odvolání pokynu. Pokyn nad rámec funkcí služby splní jen po dohodě o podmínkách a odměně.

2.5 Zákazník odpovídá za právní základ zpracování a za informační povinnost podle čl. 13 a 14 GDPR, zejména u osobních údajů vkládaných do názvů souborů a cest, u zveřejnění názvů souborů sdíleným odkazem a u pozvánek zasílaných třetím osobám. **Zvláštní kategorie údajů podle čl. 9 a údaje podle čl. 10 GDPR** — typicky dokumentaci BOZP — **nesmí do služby vkládat bez předchozí písemné dohody**.

---

3. Mlčenlivost

3.1 Provozovatel zajistí, aby se osoby oprávněné zpracovávat osobní údaje písemně zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti; závazek trvá i po skončení jejich poměru k provozovateli. Stejný standard uloží dalším zpracovatelům.

3.2 Přístup k údajům mají jen osoby, které jej potřebují ke své práci. Zvýšená oprávnění superadministrátora jsou chráněna povinným dvoufaktorovým ověřením, **časově omezena na 30 minut** a využívají se jen při řešení hlášeného problému, incidentu nebo na žádost zákazníka.

---

4. Zabezpečení zpracování

4.1 Provozovatel přijal opatření podle čl. 32 GDPR, jejichž výčet obsahuje **Příloha 2**, a zavazuje se popsanou úroveň udržovat; podrobnosti obsahuje dokument „Přehled zabezpečení". Opatření může rozvíjet, nesmí však bez souhlasu zákazníka snížit jejich celkovou úroveň.

4.2 Zákazník odpovídá za opatření na své straně, zejména za nakládání s přihlašovacími údaji a s tokeny sdílených odkazů, za včasné odebrání přístupu uživatelům, kteří jej nepotřebují, za obměnu přístupových údajů k CDE a za volbu poskytovatele CDE s odpovídající úrovní zabezpečení.

---

5. Další zpracovatelé

5.1 Zákazník uděluje provozovateli **obecné písemné povolení** zapojit další zpracovatele podle čl. 28 odst. 2 GDPR. Ke dni účinnosti smlouvy jsou schváleni ti, kteří jsou uvedeni v **Příloze 3**; seznam je uzavřený.

5.2 Zapojení nového nebo nahrazení stávajícího dalšího zpracovatele oznámí provozovatel **nejméně 30 dní předem** e-mailem na kontaktní adresu v účtu a zveřejněním nové Přílohy 3; uvede firmu a sídlo zpracovatele, jeho činnost, kategorie údajů, umístění zpracování a případný titul pro předání mimo EU/EHP.

5.3 Zákazník může vznést **odůvodněnou písemnou námitku do 15 dnů** od oznámení; odůvodněná je námitka opřená o konkrétní důvody týkající se ochrany osobních údajů, nikoli o důvody obchodní. Nevznese-li ji, má se za to, že se změnou souhlasí.

5.4 Po námitce strany jednají o řešení — jiném zpracovateli, dodatečných opatřeních nebo poskytování dotčené části služby bez něj. Nedohodnou-li se **do 30 dnů**, může zákazník dotčenou část služby nebo celou smlouvu vypovědět bez sankce a bez výpovědní doby a provozovatel vrátí poměrnou část předplatného.

5.5 Provozovatel uloží každému dalšímu zpracovateli smlouvou stejné povinnosti, jaké má sám podle této smlouvy, a před zapojením ověří jeho záruky. Neplní-li další zpracovatel své povinnosti, odpovídá zákazníkovi nadále provozovatel.

5.6 Je-li změna nezbytná k odvrácení bezprostředního ohrožení bezpečnosti služby, provede ji provozovatel ihned a vyrozumí zákazníka do 5 pracovních dnů; právo námitky tím není dotčeno.

---

6. Součinnost správci

6.1 Práva subjektů údajů vyřizuje zákazník; přednostně k tomu využije funkce aplikace — opravu údajů uživatele, zrušení účtu, pozvánek a sdílených odkazů, odpojení Páru CDE včetně smazání uložených přístupových údajů, export dat a smazání Organizace.

6.2 Žádost subjektu údajů provozovatel věcně nevyřizuje a **do 3 pracovních dnů** ji předá zákazníkovi. Nepostačují-li funkce aplikace, poskytne součinnost **do 10 pracovních dnů**, aby zákazník stihl lhůtu podle čl. 12 odst. 3 GDPR; do 2 člověkohodin měsíčně bezplatně, nad tento rámec podle ceníku.

6.3 Provozovatel je zákazníkovi nápomocen při plnění povinností podle **čl. 32 až 36 GDPR** v rozsahu informací, které má k dispozici: Přílohou 2 a dokumentem „Přehled zabezpečení", ohlašováním porušení podle článku 7 a podklady pro posouzení vlivu (DPIA) a předchozí konzultaci s dozorovým úřadem — popisem toků dat, retenčních lhůt a opatření. DPIA za zákazníka neprovádí.

6.4 Provozovatel vede záznamy podle čl. 30 odst. 2 GDPR a na žádost je zpřístupní; Příloha 1 je zpracována tak, aby ji zákazník mohl použít pro svou evidenci podle čl. 30 odst. 1 GDPR.

6.5 Žádost orgánu veřejné moci o údaje zpracovávané pro zákazníka provozovatel posoudí, zákazníka o ní neprodleně informuje — ledaže je to zakázáno — a poskytne údaje v nejmenším nezbytném rozsahu.

---

7. Porušení zabezpečení osobních údajů

7.1 Provozovatel ohlásí zákazníkovi porušení zabezpečení osobních údajů zpracovávaných pro zákazníka **bez zbytečného odkladu, nejpozději do 48 hodin od zjištění**, e-mailem na kontaktní adresu v účtu a u závažného porušení navíc telefonicky. Zjištěním je okamžik, kdy provozovatel nabyl přiměřenou jistotu, že k porušení došlo, nikoli pouhá detekce anomálie.

7.2 Oznámení obsahuje v rozsahu, v jakém jsou informace známy: povahu porušení; kategorie a přibližný počet dotčených subjektů údajů a záznamů; čas zjištění a vzniku; pravděpodobné důsledky; přijatá nebo navržená opatření ke zmírnění dopadů; doporučení pro zákazníka; a kontakt kluch@buildify.cz. Chybějící informace provozovatel doplní průběžně; neúplnost prvotního oznámení není porušením lhůty.

7.3 **Ohlášení dozorovému úřadu podle čl. 33 GDPR a informování subjektů údajů podle čl. 34 GDPR provádí zákazník**; provozovatel mu poskytne součinnost, každé porušení dokumentuje a dokumentaci na žádost zpřístupní.

---

8. Výmaz a vrácení údajů po skončení zpracování

8.1 Po ukončení smlouvy zpřístupní provozovatel zákazníkovi jeho data v režimu **read-only po dobu 14 dnů** pro export; synchronizace v této době neběží a nové pokyny se nepřijímají. Nerozhodne-li zákazník o vrácení údajů jinak, postupuje se podle článků 8.2 a 8.3.

8.2 **Trvalý výmaz** provede provozovatel **nejpozději do 30 dnů** od ukončení smlouvy, resp. od uplynutí lhůty pro export. Soft-delete, který systém používá kvůli integritě dat, není výmazem podle GDPR — tr-

valý výmaz probíhá samostatným procesem. V zálohách mohou data přetrvat do konce jejich retenční doby; po obnově ze zálohy provozovatel výmaz bez zbytečného odkladu zopakuje.

8.3 Déle je provozovatel oprávněn uchovat pouze údaje, jejichž uchování ukládá právo — zejména **účetní a daňové doklady po dobu 10 let** —, dále údaje nezbytné pro obhajobu právních nároků a dokumentaci bezpečnostních incidentů; ty jsou vyloučeny z běžného provozu a provozovatel je u nich samostatným správcem.

8.4 Po celou dobu trvání smlouvy probíhá automatizované denní mazání: protokol jednotlivých souborů a odeslaných e-mailů po **30 dnech**, záznamy Úloh a události užívání aplikace po **400 dnech**. Na žádost vystaví provozovatel potvrzení o provedeném výmazu.

---

9. Doložení souladu a kontrola

9.1 Povinnost podle čl. 28 odst. 3 písm. h) GDPR plní provozovatel **primárně doložením dokumentů** — této smlouvy s přílohami a aktuálního dokumentu „Přehled zabezpečení" — a **vyplněním bezpečnostního dotazníku** zákazníka v přiměřeném rozsahu, jednou ročně bezplatně. Zákazník je povinen využít nejprve tyto podklady.

9.2 Nepostačují-li a odůvodní-li to zákazník písemně, může provést **kontrolu na místě po předchozí dohodě obou stran, nejvýše jednou za kalendářní rok**, oznámenou 30 dní předem, v pracovní době, způsobem nenarušujícím provoz služby, **na náklady zákazníka** a po uzavření dohody o mlčenlivosti. Kontrolující osobu, která je přímým konkurentem provozovatele, může provozovatel odmítnout.

9.3 Provozovatel nezpřístupní data jiných zákazníků, zdrojový kód, obchodní tajemství nepotřebné k posouzení souladu, zásah do produkčního prostředí ani infrastrukturu dalších zpracovatelů; u ní se použijí jejich certifikace a auditní zprávy.

9.4 Po porušení zabezpečení dotýkajícím se dat zákazníka nebo na příkaz dozorového úřadu lze kontrolu provést i mimo uvedenou četnost, s oznámením 10 dní předem; nedostatky vzniklé porušením povinností provozovatele odstraní provozovatel na vlastní náklady a nese i náklady kontroly. S dozorovým úřadem spolupracuje podle čl. 31 GDPR.

---

10. Odpovědnost

10.1 Odpovědnost stran se řídí čl. 13 VOP: **souhrnná odpovědnost provozovatele je omezena částkou odpovídající 50 % souhrnu plateb, které zákazník skutečně uhradil za 12 měsíců bezprostředně předcházejících škodné události**, resp. za dosavadní dobu trvání smlouvy, byla-li kratší; vyloučena je náhrada nepřímé újmy, ušlého zisku a ztráty dat. Omezení se neuplatní tam, kde to zakazuje § 2898 OZ.

10.2 **Omezením podle článku 10.1 nejsou dotčena práva subjektů údajů na náhradu újmy podle čl. 82 GDPR** ani odpovědnost stran vůči subjektům údajů a dozorovým úřadům; platí výhradně mezi stranami. Uhradila-li jedna strana celou újmu podle čl. 82 odst. 4 GDPR, může po druhé požadovat část odpovídající její míře odpovědnosti (čl. 82 odst. 5 GDPR); regres vůči provozovateli podléhá článku 10.1.

10.3 Provozovatel odpovídá za újmu způsobenou zpracováním jen tehdy, nesplnil-li povinnosti stanovené GDPR výslovně pro zpracovatele, nebo jednal-li nad rámec pokynů zákazníka či v rozporu s nimi (čl. 82 odst. 2 GDPR). Zákazník odpovídá provozovateli za újmu vzniklou protiprávním pokynem, chybějícím právním základem, porušením prohlášení podle článku 1.4 a vložením zvláštních kategorií údajů v rozporu s článkem 2.5.

---

11. Trvání, změny a závěrečná ustanovení

11.1 Smlouva nabývá účinnosti současně se smlouvou o poskytování služby a zaniká s ní; i poté trvají článek 3 (mlčenlivost), článek 8 (výmaz), článek 9 po dobu 12 měsíců a článek 10 (odpovědnost).

11.2 Provozovatel může smlouvu jednostranně změnit v rozsahu nezbytném pro soulad se změnou předpisů či rozhodnutím dozorového úřadu, pro změnu opatření nesnižující úroveň zabezpečení a pro aktualizaci Přílohy 3 postupem podle článku 5. O změně informuje e-mailem a zveřejněním **30 dní předem**; zhoršuje-li změna podstatně postavení zákazníka, může zákazník smlouvu do 30 dnů vypovědět a obdrží poměrnou část předplatného zpět.

11.3 Provozovatel může odstoupit, trvá-li zákazník na pokynu zjevně porušujícím předpisy o ochraně osobních údajů; zákazník může odstoupit, poruší-li provozovatel podstatně povinnosti podle čl. 28 GDPR a nezjedná-li nápravu do 30 dnů od výzvy.

11.4 Smlouva se řídí právem České republiky a spory rozhodují soudy určené podle sídla provozovatele; práva subjektů údajů podle čl. 79 GDPR ani pravomoc dozorových úřadů tím nejsou dotčeny.

Příloha 1 — Popis zpracování

(čl. 28 odst. 3 a čl. 30 odst. 2 GDPR)

Předmět a povaha. Plně automatizovaný obousměrný přenos souborů a jejich metadat mezi dvěma systémy CDE podle konfigurace zákazníka. Automatizované rozhodování ani profilování podle čl. 22 GDPR se neprovádí.

Účel. Poskytování služby bim-pulse podle VOP: správa Organizace, účtů a rolí, ověřování totožnosti a řízení přístupu, připojení k CDE a správa přístupových údajů a tokenů OAuth, plánování a provádění přenosů, provozní a chybové záznamy, měření spotřeby a vynucení limitů tarifu, transakční e-maily a reporty, sdílené odkazy, podpora a zajištění bezpečnosti a dostupnosti služby.

Doba. Po dobu trvání smlouvy o poskytování služby; poté 14 dní v režimu read-only pro export a nejdéle 30 dní do výmazu, s výjimkami podle článku 8.3.

Kategorie subjektů údajů

1. **Uživatelé aplikace** — osoby s účtem v Organizaci zákazníka (Owner, Admin, Member).
2. **Osoby uvedené v názvech souborů, cestách složek a metadatech dokumentů** — projektanti, autoři a schvalovatelé dokumentace, stavbyvedoucí, technický dozor, koordinátoři BOZP, zástupci investora, subdodavatelé a další účastníci výstavby.
3. **Osoby zvané do Organizace** — adresáti pozvánek zadaní uživatelem zákazníka.
4. **Držitelé přístupu k CDE zákazníka** — osoby, jejichž přihlašovací údaje nebo souhlas OAuth zákazník do služby vložil.

5. **Příjemci sdílených odkazů** — osoby bez účtu; zpracovává se pouze agregovaný počet zobrazení odkazu.

Typy osobních údajů

- **Údaje uživatelů:** jméno a příjmení, e-mail, role, identifikátor ve sdílené identitní službě Buildify, stav účtu.
- **Autentizační údaje:** hash hesla (BCrypt), TOTP secret a stav dvoufaktorového ověření, hash pozvánkového tokenu, hash a náhled tokenu sdíleného odkazu.
- **Přístupové údaje k CDE:** šifrované tokeny OAuth; u připojení bez OAuth uživatelská jména, hesla nebo API klíče a base URL zadané zákazníkem, včetně šablon připojení.
- **Metadata souborů a přenosů:** názvy souborů, cesty a struktura složek, identifikátory souborů a verzí v obou CDE, velikosti, otisky SHA-256 a MD5, ETagy, časy modifikace a metadata dokumentů z CDE.
- **Provozní záznamy:** stav a průběh Úloh, počty souborů a bajtů, denní spotřeba kvót, chybové hlášky, události užívání aplikace a protokol odeslaných e-mailů.
- **Údaje o Organizaci:** název a slug, identifikátory u Stripe, měna, stav a konec předplatného, historie změn tarifu včetně e-mailu osoby, která změnu provedla.

Obsah souborů se trvale neukládá. Soubor se během přenosu stáhne do dočasného souboru na efemérním disku pracovního kontejneru, ihned nahraje do cílového CDE a smaže — i při chybě přenosu; kontejner po skončení Úlohy zaniká i se svým diskem. Trvale se z obsahu ukládají jen otisky SHA-256 a MD5 a velikost, z nichž obsah nelze rekonstruovat. **Názvy souborů, cesty ve stavebních projektech, metadata dokumentů a chybové hlášky však osobní údaje obsahovat mohou** a nakládá se s nimi jako s osobními údaji.

Nezpracovává se: trvale obsah souborů, IP adresy a user-agent (aplikace je nečte; vznikají jen v infrastrukturních logách Google Cloud a Firebase Hosting), čísla platebních karet, biometrické údaje, reklamní identifikátory, zvláštní kategorie údajů podle čl. 9 a údaje podle čl. 10 GDPR.

Místo zpracování. Aplikace, databáze, logy, buildy a tajemství v Google Cloud, europe-west3 (Frankfurt, Německo); frontend na Firebase Hosting (globální CDN); transakční e-maily u Brevo (EU); systémy CDE podle volby zákazníka, i mimo EU. Podrobnosti v Příloze 3.

Příloha 2 — Opatření podle čl. 32 GDPR

- **Šifrování při přenosu** — veškerá komunikace uživatelů, API i propojení na CDE probíhá výhradně přes TLS/HTTPS.
- **Šifrování v klidu** — databáze a registr kontejnerů šifrovány AES-256, hesla uložena jen jako hash BCrypt se solí, tokeny OAuth k CDE v šifrované podobě.
- **Databáze bez veřejné IP adresy** — dostupná pouze z aplikačních služeb, nikoli z internetu.
- **Řízení přístupů** — ověřování tokenem JWT, role Owner/Admin/Member, minimální oprávnění služebních účtů a allowlist CORS.
- **Dvoufaktorové ověření (2FA)** — povinné TOTP pro superadministrátory, se zamčením účtu po neúspěšných pokusech; zvýšená oprávnění platí nejvýše 30 minut.
- **Oddělení tenantů** — každý záznam nese identifikátor Organizace a filtruje se podle něj; data zákazníků se nemísí.
- **Logování** — provozní záznamy v Cloud Logging, evidence Úloh a jednotlivých přenosů a historie změn tarifu s identifikací osoby, která je provedla.
- **Správa tajemství** — connection string a klíče v Google Secret Manager, injektované do běhového prostředí, nikoli v repozitáři.
- **Zálohy** — automatické zálohy databáze s definovanou retencí a obnovou k bodu v čase; k aktivnímu zpracování se nepoužívají.
- **Integrita přenosu** — idempotenční klíč u každého přenosu, ověření velikosti a otisku SHA-256 na obou stranách, limity souběžných Úloh.
- **Organizační opatření** — mlčenlivost všech osob s přístupem k údajům, automatizované denní mazání podle retenčních lhůt a oddělení vývoje od produkce; ve vývojovém prostředí se produkční data nezpracovávají.

Příloha 3 — Další zpracovatelé

Seznam je **úplný a uzavřený**; provozovatel nemá nasazen helpdesk, CRM ani nástroj webové analytiky.

Subjekt	Role	Umístění zpracování
Google Cloud EMEA Limited / Google Ireland Limited	hosting aplikace a databáze, provozní logy, buildy, správa tajemství	europe-west3 (Frankfurt, Německo)
Google (Firebase Hosting)	doručování frontendové aplikace, přístupové logy s IP adresami	globální CDN
Stripe Payments Europe, Ltd. / Stripe, Inc.	platební údaje, fakturační identita, e-mail; u platebních údajů zároveň samostatný správce	EU / USA — standardní smluvní doložky a EU-US Data Privacy Framework
Brevo (Sendinblue SAS)	transakční e-maily: adresy příjemců, názvy projektů, statistiky v reportech	Francie / EU
Buildify identity service	ověřování uživatelů, e-mailové adresy, potvrzování e-mailů (sdílená komponenta skupiny)	Google Cloud, europe-west3
Microsoft (Azure DevOps)	zdrojový kód a CI/CD; **žádná produkční data zákazníků**	EU

Poskytovatelé CDE zvolení zákazníkem (Autodesk Construction Cloud / BIM 360, Microsoft SharePoint a OneDrive, Google Drive, Trimble Connect, PlanRadar, Fieldwire, Stavario, Buildify CDE, Proconom, AspeHub, Dalux Build, Bentley Infrastructure Cloud a ProjectWise, Procore) **nejsou dalšími zpracovateli provozovatele** — jsou samostatnými správci nebo zpracovateli zákazníka podle článku 1.5 a data u nich mohou být zpracovávána i mimo EU.