Přehled zabezpečení služby bim-pulse CDE connector

Verze 1.0 · účinnost od 1. 9. 2026 · vydáno 3. 8. 2026 · provozovatel Buildify Digital s.r.o., https://b-pulse.buildify.cz

Tento dokument popisuje, jak je bim-pulse zabezpečen. Je určen zákazníkům a jejich IT a bezpečnostním útvarům a nahrazuje vyplňování bezpečnostních dotazníků. Uvádíme jen to, co skutečně máme zavedeno; co nemáme, je uvedeno v článku 2. Otázky posílejte na kluch@buildify.cz.

---

1. Jak zabezpečení řešíme

Oblast	Jak to řešíme
Hosting a lokalita dat	Google Cloud Platform, region **europe-west3 (Frankfurt, Německo)** — aplikace i databáze jsou v Evropské unii. Frontend je doručován přes Firebase Hosting z globální sítě CDN; jde pouze o statické soubory aplikace, žádná data zákazníka.
Šifrování při přenosu	Veškerá komunikace přes **TLS/HTTPS** — mezi prohlížečem, aplikací i rozhraními CDE. Nešifrovaný přenos není podporován.
Šifrování v klidu	Databáze, registr obrazů a úložiště tajemství jsou šifrovány **AES-256** klíči spravovanými poskytovatelem infrastruktury. Přístupové tokeny ke CDE navíc šifrujeme na aplikační úrovni, hesla ukládáme jako **BCrypt** hash a tokeny sdílených odkazů a pozvánek jen jako otisk.
Řízení přístupů a 2FA	Role **Owner / Admin / Member** v rámci organizace, přidání uživatele pouze pozvánkou na e-mail s platností 7 dní. **Dvoufaktorové ověření (TOTP) je povinné pro všechny superadministrátory provozovatele** včetně ochrany proti opakovanému použití kódu a zamčení účtu po neúspěšných pokusech. Administrátorská oprávnění nejsou trvalá — vyžadují elevaci platnou **30 minut**. Pro uživatele zákazníků dvoufaktor zatím nevynucujeme.
Oddělení dat mezi zákazníky	Multi-tenant databáze; každý záznam nese identifikátor organizace a všechny dotazy jsou podle něj filtrovány. Organizaci nelze zadat z klienta jako parametr. Oddělení je zajištěno na úrovni aplikace, nikoli databáze.
Správa tajemství	Připojovací řetězec, podpisový klíč a přístupové údaje jsou v **Google Secret Manager** a vkládají se do běžících služeb až za běhu. **V repozitáři nejsou žádná produkční tajemství.** Rotace se provádí novou verzí tajemství a nasazením.
Zálohy a obnova	Databáze metadat je zálohována automatickými zálohami Google Cloud SQL; parametry záloh a výsledek posledního testu obnovy sdělíme na vyžádání. Obsah dokumentů zůstává v obou CDE zákazníka — **bim-pulse není jejich jediným úložištěm**. Nedokončené úlohy se po výpadku au-

Oblast	Jak to řešíme
	tomaticky obnoví a idempotenční klíče brání duplicitám.
Logování a monitoring	Aplikační a provozní záznamy v Cloud Logging, aktivita uživatele v aplikaci v samostatné evidenci. Databáze **nemá veřejnou IP adresu** a je dostupná jen ze služeb přes Unix socket; rozhraní používá allowlist povolených domén (CORS).
Vývoj a nasazování	Zdrojový kód a pipeline v Azure DevOps, sestavení a nasazení přes Cloud Build do Cloud Run a Firebase Hosting. **Produkční data zákazníků se ve vývoji a testování nepoužívají.** Služební účty mají pouze nejnutnější oprávnění (přístup k databázi a ke čtení tajemství).
Subdodavatelé	Uzavřený seznam: Google Cloud a Firebase (hosting), Stripe (platby), Brevo (transakční e-maily), sdílená identity služba Buildify (přihlašování), Microsoft Azure DevOps (pouze vývojová data). Helpdesk, CRM ani webová analytika nasazeny nejsou.
Ochrana osobních údajů	Provozovatel je zpracovatelem, zákazník správcem; podmínky upravuje dokument „Smlouva o zpracování osobních údajů". Neukládáme obsah souborů, IP adresy, identifikátory prohlížeče, čísla platebních karet ani zvláštní kategorie údajů. Automatické mazání běží denně: protokol souborů a odeslaných e-mailů **30 dní**, záznamy úloh a aktivita v aplikaci **400 dní**.
Ohlašování incidentů	Porušení zabezpečení oznámíme zákazníkovi jako správci **bez zbytečného odkladu, nejpozději do 24 hodin** od zjištění, a poskytneme podklady pro jeho ohlášení dozorovému úřadu. Dozorový úřad ani subjekty údajů neinformujeme jménem zákazníka bez jeho pokynu. Hlášení přijímáme na kluch@buildify.cz v pracovních dnech.

2. Co zatím nemáme

Jsme malý tým a k některým opatřením jsme se zatím nedostali. Uvádíme to raději otevřeně, než abychom na dotazník odpověděli nepřesně.

- **Nemáme certifikaci ISO/IEC 27001 ani zprávu SOC 2.** Popsaná opatření jsou zavedena, ale nejsou nezávisle auditována.
- **Neproběhl penetrační test** ani externí bezpečnostní audit aplikace.
- **Nemáme pojištění odpovědnosti** za škodu způsobenou poskytováním služby.
- **Databáze běží v zonální konfiguraci**, nikoli regionální — výpadek celé zóny znamená nedostupnost služby do jejího obnovení.

- **Neprovozujeme nepřetržitý bezpečnostní dohled (SOC)** ani pohotovost mimo pracovní dobu.

Prioritou pro nejbližší období je penetrační test aplikace a přechod databáze na regionální konfiguraci s automatickým převzetím do druhé zóny; o certifikaci uvažujeme až po nich a termín zatím neslibujeme.

---

3. Nejčastější dotazy

Kde jsou naše data uložena? V Evropské unii — aplikace i databáze v regionu europe-west3 (Frankfurt). Statické soubory frontendu jsou doručovány z globální CDN, data zákazníka se přes ni nepřenášejí. Data mohou mimo EU procházet infrastrukturou poskytovatelů CDE, které si zvolíte vy — to je vaše rozhodnutí a váš vztah s daným poskytovatelem.

Ukládáte obsah našich souborů? Ne. bim-pulse je přenosová služba, nikoli úložiště. Soubor se během přenosu stáhne do dočasného souboru na disku pracovní instance, ověří se jeho velikost a otisk SHA-256, nahraje se do cílového CDE a **okamžitě se smaže**, a to i při chybě přenosu; instance je dočasná a po skončení úlohy zaniká i s diskem. Trvale ukládáme jen metadata — názvy souborů, velikosti, identifikátory, cesty ke složkám, otisky, časy a chybové hlášky. Z otisků nelze obsah rekonstruovat.

Pozor: názvy souborů a struktura složek ve stavebních projektech běžně obsahují osobní údaje. Nakládáme s nimi jako s osobními údaji a totéž doporučujeme vám.

Kdo k našim datům může přistupovat? Uživatelé vaší organizace podle přidělené role. Na naší straně superadministrátor, a to jen pro řešení požadavku podpory, diagnostiku chyby, vyšetření incidentu nebo splnění právní povinnosti. Takový přístup vyžaduje dvoufaktorové ověření, je časově omezen na 30 minut a je protokolován. K obsahu vašich souborů se tímto přístupem dostat nelze — trvale jej neukládáme.

Co se stane při bezpečnostním incidentu? Incident vyhodnotíme, zamezíme jeho šíření a vy jako správce dostanete oznámení nejpozději do 24 hodin od zjištění, s popisem incidentu, dotčených dat a přijatých opatření. Poskytneme vám podklady pro ohlášení dozorovému úřadu a u závažných incidentů shrnutí následné analýzy.

Jak dlouho data držíte? Podle typu záznamu: protokol jednotlivých souborů a odeslaných e-mailů 30 dní, záznamy úloh a aktivitu v aplikaci 400 dní. Po ukončení smlouvy máte **14 dní** přístup pouze pro čtení k exportu a data trvale mažeme **do 30 dnů**; výjimkou jsou účetní a daňové doklady, které musíme uchovat 10 let.

Jak se bim-pulse připojuje k našemu CDE? Buď přes OAuth 2.0, kdy oprávnění udělíte vy a my ukládáme jen šifrované tokeny a obnovujeme je automaticky na pozadí, aby synchronizace běžela podle plánu, nebo jménem a heslem či API klíčem, které nám svěříte. Ve druhém případě doporučujeme zřídit **samostatný servisní účet s minimálními oprávněními** omezenými na synchronizované složky.