

Bezpečnost a ochrana dat: přehled pro zákazníky

Vydává	Buildify Digital s.r.o.
IČO / sídlo	29541743 · Korunní 2569/108, Vinohrady, 101 00 Praha 10
Zápis	Městský soud v Praze, sp. zn. C 447453
Verze / účinnost	1.0 · účinné od 1. září 2026
Kontakt	kluch@buildify.cz

Buildify CDE je společné datové prostředí pro stavební projekty. Víme, že do něj dáváte projektovou dokumentaci, modely i fotografie ze stavby. Tady je přehled toho, jak s vašimi daty zacházíme. Bez právníčiny a bez slibů, které bychom nesplnili.

1. Kde jsou data

- Všechna data zpracováváme **v Evropské unii**.
- Produkce běží na Google Cloud v regionu **europe-west3 (Frankfurt)** — aplikace, databáze, úložiště souborů i logy.
- Transakční e-maily posíláme přes poskytovatele v EU (Brevo, MailerSend). Volitelné přihlášení účtem Microsoft nebo Google běží přes jejich irské entity.
- Jedinou výjimkou je platební brána Stripe. Ta může data o platbách předat uvnitř své skupiny mimo EU, a to na základě **standardních smluvních doložek** schválených Evropskou komisí.
- Editaci dokumentů v prohlížeči provozujeme sami na vlastní infrastruktuře. Vaše soubory kvůli ní neopouštějí naše prostředí.

2. Oddělení zákazníků a přístupy

- Data každého zákazníka jsou oddělená už na úrovni databáze. Každý záznam nese identifikátor tenanta a filtr se uplatní automaticky u každého dotazu. Je nastavený jako **fail-closed**: když by chyběl, dotaz nevrátí nic — místo aby vrátil cizí data.
- Oprávnění nastavujete **granulárně na jednotlivé složky**, nejen na celý projekt.
- Uživatelé sdružujete do **skupin**, takže práva nastavujete jednou pro celý tým.
- U každého požadavku se navíc kontroluje **členství v projektu** na úrovni rozhraní. Bez členství se k projektu nedostane nikdo, ani s odkazem.
- Super-admini mají povinné **dvoufaktorové ověření (TOTP)**.
- Každý uživatel si musí **ověřit e-mail**, jinak se nepřihlásí.
- Přihlášení lze **okamžitě zneplatnit**. Odhlášení nebo zablokování účtu zneplatní vydané tokeny hned, nečeká se na jejich vypršení. Odejde vám člověk z týmu — přístup končí ve stejnou minutu.
- Rozhraní je chráněné omezením počtu požadavků.

3. Šifrování, zálohy, dohledatelnost

- Přenos dat je vždy šifrovaný přes **TLS**. Data uložená na disku jsou šifrovaná v klidu.
- **Zálohy děláme denně** a držíme je **30 dní**.
- **Audit log** zaznamenává, kdo, kdy a co udělal, včetně staré a nové hodnoty, IP adresy a projektu. Držíme ho **24 měsíců**.

- **Verzování dokumentů** podle ISO 19650: každá revize zůstává dohledatelná, včetně revizních kódů a metadat. Tiskové razítko s QR kódem umožní ověřit, jestli je výtisk stále platný.
- Smazané položky jdou vrátit z **koše po dobu 30 dní**. Mazání je měkké a s auditem, takže je vždy vidět, kdo co odstranil.
- Souběžné úpravy hlídá optimistické zamykání, takže si dva lidé navzájem nepřepíší práci.
- **Zpracování dokumentů včetně extrakce textu (OCR) běží lokálně na našich serverech.** Vaše výkresy ani PDF neposíláme žádné externí službě na rozpoznávání obsahu.
- ZIP exporty jsou dostupné jen 3 dny, pak odkaz expiruje.

4. Dostupnost a co slibujeme

- Pro placené tarify garantujeme dostupnost **99 % měsíčně** v rámci samostatné dohody o úrovni služeb (SLA).
- Když dostupnost nedodržíme, máte nárok na **servisní kredit** — 10 %, 20 % nebo 30 % měsíčního poplatku podle toho, jak hluboko jsme spadli. Uplatníte ho e-mailem do 30 dnů.
- Plánovanou údržbu děláme mimo 8:00 až 18:00 v pracovní dny a oznamujeme ji 48 hodin předem. Nepřesáhne 8 hodin měsíčně.
- Podporu poskytujeme e-mailem v pracovní dny 9:00 až 17:00. Na kritický incident reagujeme do 8 hodin.
- Tarif Free je bez SLA.

5. Data po ukončení a dokumenty na vyžádání

- Data jsou vaše. My je jen hostujeme.
- Po ukončení předplatného máte **30 dní přístup jen pro čtení a export**. Stihnete si všechno stáhnout.
- Další **60 dní** data držíme v záloze. Pak je **nevratně smažeme**.
- **Zpracovatelskou smlouvu i aktuální seznam sub-zpracovatelů** vám pošleme na vyžádání na kluch@buildify.cz.
- Změnu sub-zpracovatele oznamujeme **30 dní předem**, takže máte čas se k ní vyjádřit.
- Porušení zabezpečení vašich osobních údajů vám oznámíme do 48 hodin od zjištění.

6. Co zatím nemáme

Jsme mladá firma a raději vám rovnou řekneme, co u nás nenajdete, než abyste to zjistili až při bezpečnostním dotazníku. Tenhle seznam je otevřený a budeme ho zkracovat, jak porosteme.

- Nemáme certifikaci **ISO 27001**, **SOC 2** ani **ISAE** a neprošli jsme auditem podle nich.
- Nemáme nezávislý **penetrační test se zprávou**, kterou bychom vám mohli poslat.
- Neprovozujeme program **odměn za hlášení zranitelností**. Hlášení ale vítáme a máme pro ně jasná pravidla v samostatném dokumentu.
- Nemáme **geograficky redundantní řešení** a negarantujeme dobu obnovení provozu ani maximální ztrátu dat (RTO/RPO). Běžíme v jednom regionu ve Frankfurtu.
- Podporu provozujeme **v pracovní dny, ne nepřetržitě**.

Máte dotaz, na který tenhle přehled neodpovídá? Napište na kluch@buildify.cz. Odpovíme konkrétně, i když bude odpověď „tohle zatím neděláme“.