Smlouva o zpracování osobních údajů BIM Harness

Buildify Digital s.r.o., IČO 29541743, Korunní 2569/108, Vinohrady, 101 00 Praha 10, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. C 447453.
Verze 1.0 · účinné od 4. listopadu 2026 · kontakt kluch@buildify.cz

1. Strany a k čemu tahle smlouva je

1.1 **Poskytovatel, v roli zpracovatele:** Buildify Digital s.r.o., IČO 29541743, se sídlem Korunní 2569/108, Vinohrady, 101 00 Praha 10, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. C 447453, zastoupená jednatelem Lukášem Kluchem. Kontakt pro cokoli kolem ochrany údajů: kluch@buildify.cz.

1.2 **Zákazník, v roli správce:**

Obchodní firma nebo jméno: .....

Sídlo nebo adresa: .....

IČO: .....

Zastoupen: .....

Kontaktní e-mail: .....

1.3 Tahle smlouva upravuje zpracování osobních údajů podle článku 28 GDPR, ke kterému dochází při užívání služby BIM Harness (dále „Služba“) v rámci podnikání Zákazníka. Řídí se českým právem.

1.4 Smlouvu lze použít dvěma způsoby: jako samostatný podepsaný dokument, nebo jako přílohu obchodních podmínek BIM Harness. V druhém případě se podpisová doložka nepoužije a platí článek 15.5.

1.5 Pro službu Buildify CDE platí samostatná zpracovatelská smlouva. Tahle smlouva se na ni nevztahuje.

2. Kdo je tady kým

2.1 U obsahu, který do Služby vložíte - zadání, konverzace s AI asistentem, fotografie, výkresy, modely a další soubory - jste **správcem vy**. My jsme **zpracovatel** a řídíme se vašimi pokyny.

2.2 U uživatelských účtů, přihlašování, fakturace, provozních logů, podpory, čekací listiny a poptávek z webu jsme **správcem my**. Tam neplatí tahle smlouva, ale naše zásady ochrany osobních údajů.

2.3 Používáte-li Službu jako spotřebitel pro své osobní potřeby, tahle smlouva se nepoužije. Údaje ve vašem obsahu pak zpracováváme jako správce podle zásad ochrany osobních údajů.

2.4 Společnými správci nejsme a nechceme být. Žádná strana nerozhoduje o účelech zpracování té druhé.

> **Prostou řečí:** Co do BIM Harness nahrajete, je vaše a rozhodujete o tom vy. My to jen zpracujeme, aby vám editor a AI fungovaly. Za seznam uživatelů a fakturaci odpovídáme my.

3. Předmět, doba, povaha a účel zpracování

3.1 **Předmět:** osobní údaje obsažené v datech, která do Služby vložíte vy nebo vaši uživatelé.

3.2 **Povaha zpracování:** ukládání, hosting, zálohování, zobrazení a úpravy v prohlížeči, **zpracování modely umělé inteligence** (čtení zadání a příloh, navrhování modelu, odpovědi asistenta, AI rendery), vyhledání místa stavby v mapových službách, zpřístupnění přes sdílecí odkazy a klientské stránky, exporty, **anonymizace pro ladění podle článku 6.3** a mazání.

3.3 **Účel:** výhradně poskytování Služby vám podle smlouvy a dokumentace. Vaše data nepoužíváme pro vlastní účely, neprodáváme je, nepůjčujeme a **nepoužíváme k trénování modelů umělé inteligence**.

3.4 **Doba:** po dobu trvání smlouvy o Službě a dále po dobu podle článku 13.

4. Koho a jakých údajů se to týká

4.1 Kategorie subjektů údajů:

- zaměstnanci a spolupracovníci Zákazníka
- klienti, investoři a další účastníci projektu Zákazníka
- vlastníci a uživatelé staveb a pozemků, kterých se zadání týká
- osoby zachycené na fotografiích fasád, staveb a okolí
- autoři výkresů a podkladů a osoby v nich uvedené
- osoby, o kterých uživatelé píší v zadání a v konverzaci s AI asistentem

4.2 Kategorie osobních údajů:

- identifikační a kontaktní údaje: jméno, příjmení, e-mail, telefon, firma
- adresa stavby, číslo parcely a souřadnice, pokud je lze spojit s konkrétním člověkem
- **fotografie fasád a staveb**, včetně obličejů osob a registračních značek vozidel, které na nich náhodou jsou
- **výkresy a podklady** se jmény, razítky a podpisy
- **text zadání a konverzace s AI asistentem** a cokoli, co do nich uživatel napíše
- údaje v klientských stránkách a prezentacích

4.3 Nad rozsahem údajů v textu zadání, v konverzaci a na fotografiích nemáme kontrolu. Co do nich napíšete nebo nahrajete, určujete vy.

5. Zvláštní kategorie údajů

5.1 Služba není určená ke zpracování zvláštních kategorií údajů podle článku 9 GDPR ani údajů o trestných činech. Záměrně je nezpracováváme a nemáme pro ně zvláštní funkce.

5.2 Nesmíte je do Služby vkládat, pokud pro to sami nemáte právní důvod a nevyhodnotíte, že je to přiměřené. Pozor na ně hlavně u zadání pro zdravotnické a sociální stavby: jméno konkrétního pacienta nebo klienta do zadání nepatří.

6. Pokyny

6.1 Osobní údaje zpracováváme jen podle vašich doložených pokynů.

6.2 Za pokyn se považuje samotné užívání Služby v souladu s dokumentací a nastavení, které si zvolíte ve své Organizaci - kdo má přístup, sdílecí odkazy, klientské stránky, exporty, mazání. Další pokyny nám posílejte e-mailem.

6.3 **Anonymizace pro ladění.** Dáváte nám pokyn, abychom vaše data mohli v **anonymizované podobě** použít k hledání a opravě chyb výpočetního jádra Služby a k jeho testování. Před takovým použitím z dat odstraníme jména, kontakty, adresy, souřadnice, fotografie osob a další údaje, podle kterých by šlo poznat

konkrétního člověka. Anonymizovaná data už nejsou osobními údaji. K trénování modelů umělé inteligence je nepoužíváme.

6.4 Pokyn, který by šel nad rámec Služby a vyžadoval vývoj nebo ruční práci, můžeme odmítnout, nebo ho provést za úhradu po dohodě.

6.5 Pokud bude pokyn podle nás v rozporu s právem, řekneme vám to a jeho provedení odložíme do vyjasnění. Zpracování na základě práva Unie nebo České republiky vám oznámíme předem, ledaže to zákon zakazuje.

7. Mlčenlivost

7.1 K vašim datům pouštíme jen osoby, které je potřebují znát pro provoz nebo podporu. Tyto osoby jsou vázány mlčenlivostí, která trvá i po skončení spolupráce.

7.2 Poskytovatel je malá firma. Přístup k produkčním datům má jen jednatel a jednotliví spolupracovníci, kteří s námi mají uzavřenou písemnou mlčenlivost.

8. Zabezpečení

8.1 Zavedli jsme technická a organizační opatření popsaná v Příloze 1. Bereme v úvahu stav techniky, náklady a rizika pro dotčené osoby.

8.2 Opatření můžeme měnit, pokud tím úroveň ochrany nesnížíme.

8.3 I vy máte svou část práce: pouštět do Organizace jen ty, kdo tam patří, rušit přístupy odcházejícím lidem, hlídat sdílecí odkazy a klientské stránky a nevkládat do zadání víc osobních údajů, než je potřeba.

9. Sub-zpracovatelé

9.1 Dáváte nám **obecné povolení** zapojit sub-zpracovatele. Aktuální seznam je v Příloze 2.

9.2 Každému sub-zpracovateli ukládáme smluvně stejné povinnosti, jaké máme my vůči vám. Za jejich práci odpovídáme, jako bychom ji dělali sami.

9.3 Změnu nebo přidání sub-zpracovatele oznámíme e-mailem správcům účtu **nejméně 30 dní předem**.

9.4 Do 30 dnů od oznámení můžete vznést odůvodněnou námitku. Odůvodněnou znamená, že popíšete konkrétní riziko pro ochranu údajů. Pokusíme se najít řešení. Pokud ho do 30 dnů nenajdeme, můžete smlouvu o Službě vypovědět ke dni změny, bez sankce.

10. Pomoc s právy subjektů údajů

10.1 Ve Službě máte nástroje, kterými většinu žádostí vyřídíte sami: export modelů a dat, mazání projektů, konverzací a souborů, správu uživatelů.

10.2 Kde nástroje nestačí, pomůžeme vám. Odpovíme a poskytneme součinnost **do 10 pracovních dnů** od vaší žádosti na kluch@buildify.cz. Přiměřenou součinnost děláme zdarma.

10.3 Pokud se subjekt údajů obrátí přímo na nás, sami mu jeho žádost nevyřídíme. **Smíme mu ale sdělit, že správcem jeho údajů jste vy**, včetně vašeho obchodního jména a kontaktu, a žádost vám předat.

10.4 Stejně postupujeme u dotazů dozorového úřadu, které se týkají vašich dat.

11. Porušení zabezpečení

11.1 Porušení zabezpečení osobních údajů ve vašich datech vám oznámíme **do 48 hodin od zjištění**, e-mailem správcům účtu.

11.2 **Zjištěním** se rozumí okamžik, kdy jsme s přiměřenou jistotou ověřili, že k porušení skutečně došlo. Prověřování děláme bez zbytečného odkladu a vedeme si o něm záznam.

11.3 Oznámení obsahuje popis toho, co se stalo, kdy k tomu došlo a kdy jsme to zjistili, jaké kategorie a přibližný rozsah údajů to zasáhlo, pravděpodobné následky, co jsme už udělali a co doporučujeme udělat vám, a kontakt pro další dotazy. Co v tu chvíli nevíme, doplníme následně.

11.4 Ohlášení dozorovému úřadu a informování dotčených osob je vaše věc - správcem jste vy. My vám k tomu dodáme podklady.

12. Kontrola

12.1 Na požádání vám poskytneme informace a dokumentaci potřebnou k doložení toho, že plníme článek 28 GDPR - popis opatření, přehled sub-zpracovatelů a nastavení AI dodavatelů, záznamy o incidentech, které se vás týkaly.

12.2 Nad rámec toho máte právo na audit **jednou za rok**, po oznámení **30 dní předem**, v pracovní době, na vlastní náklady a v rozsahu, na kterém se předem dohodneme. Audit můžete provést sami nebo přes auditora, který není naším konkurentem a podepíše mlčenlivost.

12.3 Audit nesmí zasáhnout do provozu Služby, do našeho obchodního tajemství ani do dat jiných zákazníků. Infrastrukturu cloudu a AI dodavatelů nelze auditovat fyzicky - místo toho poskytneme jejich dokumentaci.

12.4 Řekneme to na rovinu: nemáme žádnou nezávislou auditní zprávu ani bezpečnostní certifikaci. Vše, co dokládáme, je naše vlastní dokumentace a dokumentace našich dodavatelů.

13. Co bude s daty po skončení

13.1 Po skončení smlouvy máte **30 dní** přístup jen pro export.

13.2 Dalších **60 dní** po nich držíme jen zálohu, ze které vám data na požádání obnovíme. Pak je nevratně smažeme, včetně kopií u sub-zpracovatelů, ledaže musíme něco uchovat podle zákona.

13.3 **Záznamy AI běhů** - zadání, odpovědi a kroky AI - mažeme nejpozději **30 dní** od jejich vzniku, i za trvání smlouvy. Modely a soubory ve vašich projektech tím dotčené nejsou.

13.4 Na písemnou žádost vám po dokončení výmazu vystavíme potvrzení.

13.5 Kopie souborů, které si vaši lidé stáhli do svých zařízení, smazat nedokážeme.

14. Kde se data zpracovávají

14.1 **Soubory, modely a databáze** jsou uložené v Evropské unii, v Google Cloud v regionu **europe-west3 (Frankfurt)**. Tamtéž jsou zálohy a logy.

14.2 **Výjimky mimo EU:**

- **AI dodavatelé** uvedení v Příloze 2. Ke zpracování jim posíláme zadání, konverzaci, přílohy a snímky modelu potřebné pro danou operaci. Jejich modely běží **mimo Evropskou unii, zejména v USA**. Předání se opírá o standardní smluvní doložky podle prováděcího rozhodnutí Komise (EU) 2021/914,

které jsou součástí zpracovatelských dodatků Anthropic a Google Cloud. Google LLC je navíc certifikovaný v rámci EU-US Data Privacy Framework.

- **Stripe** může platební údaje předat uvnitř své skupiny mimo EHP na základě standardních smluvních doložek podle prováděcího rozhodnutí Komise (EU) 2021/914. Do dat vašich projektů Stripe nevidí.

14.3 **AI dodavatelé na datech netrénují.** Anthropic data z API podle svých obchodních podmínek k tréninku nepoužívá a Google podle podmínek Vertex AI také ne. Trénink na našich datech jsme nikde nepovolili. Dodavatelé data uchovávají jen dočasně: kvůli zrychlení opakovaných dotazů (cache) nejvýše 24 hodin a v záznamech pro kontrolu zneužití nejvýše 30 dní. Obsah, který dodavatel vyhodnotí jako porušení svých pravidel užívání, může uchovat déle. Smlouvu o nulovém uchovávání dat (zero data retention) s dodavateli nemáme.

14.4 **Mapové služby.** Když v editoru hledáte místo stavby, prohlížeč posílá zadanou adresu nebo souřadnice přímo veřejným mapovým službám - Českému úřadu zeměměřickému a katastrálnímu (RÚIAN, katastrální mapa, výškopis) a geokodérům nad OpenStreetMap. Tyto služby nejsou našimi sub-zpracovateli; adresu do nich odesíláte vy hledáním v editoru. Když AI asistent hledá informace na webu, náš server pošle vyhledávací dotaz, který AI sestaví ze zadání, vyhledávači DuckDuckGo a načte nalezené veřejné stránky. Vaše jméno, kontakty ani soubory se tam neposílají. Vyhledávač není naším sub-zpracovatelem.

15. Odpovědnost, trvání a podpisy

15.1 Odpovědnost se řídí obchodními podmínkami BIM Harness, včetně limitu odpovědnosti. To neplatí pro nároky, u kterých takové omezení GDPR nebo jiný zákon nedovoluje.

15.2 Každá strana nese sankci uloženou dozorovým úřadem za své vlastní porušení. Pokud jedna strana uhradí náhradu škody i za tu druhou, má vůči ní právo na vypořádání podle míry zavinění.

15.3 Smlouva platí po dobu trvání smlouvy o Službě. Ustanovení o mlčenlivosti, výmazu dat a odpovědnosti platí i po jejím skončení.

15.4 V otázkách ochrany osobních údajů má tahle smlouva **přednost před obchodními podmínkami**. Ve všem ostatním platí obchodní podmínky.

15.5 **Začlenění do obchodních podmínek.** Pokud tenhle dokument používáte jako přílohu obchodních podmínek, není potřeba ho podepisovat zvlášť. Do smlouvy nebo objednávky stačí vložit větu:

```
Smluvní strany se dohodly, že zpracování osobních údajů podle článku 28
Nařízení (EU) 2016/679 se řídí Smlouvou o zpracování osobních údajů
BIM Harness, která tvoří přílohu obchodních podmínek BIM Harness a je
dostupná na buildify.cz. Zákazník potvrzuje, že se s ní seznámil.
```

15.6 **Podpisy** (jen u samostatného dokumentu):

Za Poskytovatele - Buildify Digital s.r.o., Lukáš Kluch, jednatel

V ..... dne .....

Podpis: .....

Za Zákazníka

Jméno a funkce: .....

V ..... dne .....

Podpis: .....

Příloha 1 - Technická a organizační opatření

Přístupy a přihlašování

- přihlášení e-mailem a heslem, heslo ukládáme jen jako otisk, nikdy v čitelné podobě
- povinné ověření e-mailu před prvním použitím účtu
- volitelné přihlášení účtem Microsoft nebo Google
- druhý faktor povinně u super-administrátorů Poskytovatele
- krátkodobý přístupový token a obnovovací token s platností 30 dnů
- omezení počtu pokusů a četnosti požadavků na rozhraní

Oddělení zákazníků a oprávnění

- oddělení dat jednotlivých Organizací na úrovni databáze identifikátorem organizace; filtry pracují fail-closed
- přístup do Organizace jen pro pozvané Uživatele; tarif Start jen pro jednoho Uživatele
- sdílecí odkazy a klientské stránky lze kdykoli zrušit

Šifrování a integrita dat

- šifrovaný přenos mezi prohlížečem, našimi servery a AI dodavateli
- šifrování dat v klidu zajišťuje Google Cloud na úrovni úložiště a databáze
- verzování modelů v projektu

Opatření u umělé inteligence

- AI dodavatelům posíláme jen data potřebná pro danou operaci: zadání, konverzaci, přílohy a snímky modelu; nikdy přihlašovací údaje ani platební údaje
- volání AI jde přes náš server s naším klíčem; AI dodavatel nevidí, kdo jste, ani data jiných Organizací
- AI dodavatelé na našich datech netrénují; dočasně je uchovávají nejvýše 30 dní (cache nejvýše 24 hodin, záznamy pro kontrolu zneužití)
- vlastní modely nedotrénováváme a na datech zákazníků AI netrénujeme
- záznamy AI běhů (zadání, odpovědi, kroky) uchováváme **30 dní**, pak je mažeme
- k ladění výpočetního jádra používáme data jen po anonymizaci podle článku 6.3
- odpovědi a změny modelu navržené AI jsou ve Službě označené jako AI výstup
- jedna instrukce AI má pevný strop spotřeby, aby se běh nemohl vymknout kontrole

Logy a dohledatelnost

- provozní logy a telemetrie 90 dnů
- záznamy o porušení zabezpečení a o žádostech subjektů údajů vedeme písemně

Zálohy a dostupnost

- denní zálohy databáze a úložiště, retence 30 dnů
- cílová dostupnost 99 % měsíčně, bez garance

Vývoj, lidé a sub-zpracovatelé

- oddělené vývojové a produkční prostředí; do vývoje nepoužíváme kopie ostrých zákaznických dat, jen anonymizovaná data podle článku 6.3
- tajné klíče k produkci a k AI dodavatelům držíme ve správci tajemství, ne ve zdrojovém kódu
- správa verzí kódu a revize změn před nasazením
- přístup k produkci má jen jednatel a spolupracovníci vázaní písemnou mlčenlivostí

- se sub-zpracovateli máme uzavřené zpracovatelské smlouvy

Co nemáme - otevřeně

- žádnou bezpečnostní certifikaci ani nezávislou auditní zprávu
- žádné externí bezpečnostní testování
- žádnou geografickou redundanci; vše běží v jednom regionu
- žádné závazné doby obnovení provozu ani maximální ztráty dat
- žádný nepřetržitý bezpečnostní dohled

Fyzickou bezpečnost datových center zajišťují Google Cloud a AI dodavatelé jako provozovatelé infrastruktury.

Příloha 2 - Sub-zpracovatelé

Subjekt	Entita	Účel	Kde
Google Cloud	Google Cloud EMEA Limited, Irsko	provoz aplikace, databáze, úložiště souborů, hosting, logy	europe-west3, Frankfurt
Google Cloud - Vertex AI	Google Cloud EMEA Limited, Irsko	AI modely Gemini, případně Claude přes Vertex AI: AI asistent, generování modelu, čtení zadání, AI render	kdekoli ve světě, i mimo EU (lokace „global“)
Anthropic	Anthropic Ireland, Limited, Irsko; modely provozuje Anthropic, PBC	AI modely Claude: AI asistent, generování modelu, čtení zadání	mimo EU, zejména USA
Stripe	Stripe Payments Europe, Limited, Irsko	platby a předplatné	Evropská unie; uvnitř skupiny standardní smluvní doložky
Brevo	Sendinblue SAS, Francie	transakční e-maily	Evropská unie
MailerSend	MailerSend, skupina MailerLite	transakční e-maily	Evropská unie
Microsoft	Microsoft Ireland Operations Limited	volitelné přihlášení účtem Microsoft	Evropská unie
Google	Google Ireland Limited	volitelné přihlášení účtem Google	Evropská unie

Jak oznamujeme změny. Přidání nebo výměnu sub-zpracovatele oznámíme e-mailem správcům účtu nejméně 30 dní předem a zároveň aktualizujeme tuhle přílohu na buildify.cz. Postup pro námitku je v článku 9.