

BUILDIFY CDE

Smlouva o zpracování osobních údajů

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

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 Buildify CDE (dále „Služba“). Řídí se českým právem.

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

2. Kdo je tady kým

2.1 U obsahu, který nahrajete do projektů — dokumenty, modely, fotografie, formuláře, úkoly, komentáře — jste **správce** **vy**. My jsme **zpracovatel** a řídíme se vašimi pokyny.

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

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

Prostou řečí: Data máte pořád svoje. My je jen hostujeme. O tom, kdo je uvidí, rozhodujete vy. Naopak za to, že vedeme seznam uživatelů a záznam o tom, kdo se kdy přihlásil, 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, verzování podle ISO 19650, zálohování, zobrazení a editace v prohlížeči, extrakce textu z dokumentů, zpřístupnění přes sdílecí odkazy a plugíny, notifikace, exporty, mazání.

3.3 Účel: výhradně poskytování Služby vám podle smlouvy a dokumentace. Vaše data nepoužíváme pro vlastní účely, neprodáváme je, nepůjčujeme a neanalyzujeme pro nikoho jiného.

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
- zaměstnanci a zástupci subdodavatelů Zákazníka
- osoby zachycené na fotografiích ze stavby
- kontaktní osoby investora, objednatele a dalších účastníků projektu
- projektanti, autoři dokumentace a osoby uvedené v razítkách a revizních záznamech
- osoby uvedené ve vyplněných formulářích a v projektové dokumentaci

4.2 Kategorie osobních údajů:

- identifikační a kontaktní údaje: jméno, příjmení, e-mail, telefon, firma
- pracovní zařazení, role v projektu, příslušnost k organizaci
- podpisy a jména v razítkách, revizních kódech a schvalovacích záznamech
- obrazové záznamy včetně obličejů osob a registračních značek vozidel na fotografiích vad a fotografiích z terénního režimu
- údaje, které kdokoli z vašich uživatelů napíše do volných polí formulářů, komentářů, úkolů nebo markupů

4.3 Nad rozsahem údajů v posledním bodě nemáme kontrolu. Volná pole si definujete vy a vyplňují je vaši lidé.

5. Zvláštní kategorie údajů

5.1 Služba není určena 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.

5.3 Buďme konkrétní: k tomu snadno dojde u záznamů o pracovních úrazech a bezpečnostních kontrolách, které si mnoho firem vede ve formulářích. Popis zranění je údajem o zdravotním stavu. Pokud takové formuláře ve Službě vedete, je na vás posoudit právní důvod, omezit okruh lidí s přístupem a zvážit, jestli nepotřebujete posouzení vlivu na ochranu osobních údajů podle článku 35 GDPR. My vám k tomu poskytneme informace o technických opatřeních, ale posouzení za vás udělat nemůžeme.

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 — nastavení oprávnění ke složkám, uživatelské skupiny, sdílecí odkazy, zapnuté pluginy, doby uchování. Další pokyny nám pošlete e-mailem.

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

6.4 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 použijeme 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 jednočlenná firma. Přístup k produkčním datům má fakticky jen jednatel a případní 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: udržovat správně nastavená oprávnění, rušit přístupy odcházejícím lidem, hlídat sdílecí odkazy a nesdílet přihlašovací údaje.

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, a my vám vrátíme poměrnou část předplatného za nevyčerpané období.

10. Pomoc s právy subjektů údajů

10.1 Ve Službě máte nástroje, kterými většinu žádostí vyřídíte sami: vyhledávání, export dat projektu, správu uživatelů, mazání dokumentů a formulářů, úpravu a odstranění fotografií.

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; opakované rozsáhlé exporty nad rámec běžné funkčnosti můžeme vyúčtovat po předchozí dohodě.

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. Souhlasíte s tím a berete na vědomí, že to bez uvedení vaší totožnosti nejde.

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. Není jím pouhé podezření, automatický poplach z monitoringu ani hlášení, které se teprve prověřuje. Prověřování ale nesmíme protahovat — děláme ho bez zbytečného odkladu a po celou dobu si vedeme záznam o tom, co jsme kdy zjistili.

11.3 Oznámení obsahuje popis toho, co se stalo, kdy k tomu došlo a kdy jsme to zjistili, jaké kategorie a přibližný rozsah údajů a projektů 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, konfigurace, přehled sub-zpracovatelů, 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. Mimořádný audit je možný po prokazatelném porušení zabezpečení, které se vás týkalo.

12.3 Audit nesmí zasáhnout do provozu Služby, do našeho obchodního tajemství ani do dat jiných zákazníků. Sdílenou infrastrukturu, do které nemáme přístup my sami, nelze auditovat fyzicky — místo toho poskytneme dokumentaci našeho poskytovatele cloudu.

12.4 Řekneme to na rovinu: nemáme žádnou nezávislou auditní zprávu ani bezpečnostní certifikaci. Vše, co dokládáme, je naše vlastní dokumentace a naše vlastní tvrzení. Až takové doklady mít budeme, dáme vám vědět.

13. Co bude s daty po skončení

13.1 Po skončení smlouvy máte **30 dní** přístup jen pro čtení a export. Během té doby si data stáhnete.

13.2 Dalšíh **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 (typicky účetní doklady).

13.3 ZIP export je ke stažení **3 dny**, pak odkaz expiruje. Vygenerovat si ho můžete znovu.

13.4 Na písemnou žádost vám po dokončení výmazu vystavíme potvrzení.

13.5 **Důležité:** kopie souborů, které si vaši lidé stáhli do svých počítačů, smazat nedokážeme — na ta zařízení nevidíme a nemáme k nim přístup. Jejich odstranění je na vás.

14. Kde se data zpracovávají

14.1 Veškeré zpracování probíhá **v Evropské unii**. Produkční prostředí, databáze, úložiště souborů i logy běží v Google Cloud v regionu **europe-west3 (Frankfurt)**.

14.2 Extrakce textu z dokumentů běží na našich serverech v témže regionu. Data z nich za tímhle účelem neodcházejí nikam ven.

14.3 Jediná výjimka je **Stripe**. Ten může platební údaje předat uvnitř své skupiny mimo Evropský hospodářský prostor na základě standardních smluvních doložek podle prováděcího rozhodnutí Komise (EU) 2021/914. Do dat vašich projektů Stripe nevidí.

15. Odpovědnost, trvání a podpisy

15.1 Odpovědnost se řídí obchodními podmínkami, 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, která tvoří přílohu obchodních podmínek Poskytovatele 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 (jednorázový kód) povinně u super-administrátorů Poskytovatele
- krátkodobý přístupový token a obnovovací token s platností 30 dnů; odhlášení token okamžitě zneplatní přes seznam zakázaných identifikátorů
- pozvánka do Organizace platí 14 dnů, pak propadá
- omezení počtu pokusů a četnosti požadavků na rozhraní

Oprávnění a oddělení zákazníků

- oddělení dat jednotlivých zákazníků na úrovni databáze pomocí identifikátoru organizace a globálních filtrů, které se uplatní na každý dotaz
- filtry pracují **fail-closed**: když identifikátor chybí, dotaz nevrátí nic, místo aby vrátil všechno
- granulární oprávnění na jednotlivé složky, uživatelské skupiny a role
- kontrola členství v projektu na úrovni rozhraní, ne jen v uživatelském prostředí
- tokeny pro pluginy platí 5 minut a mají rozsah omezený na to, k čemu je plugin oprávněn
- sdílecí odkazy lze kdykoli zneplatnit; veřejná ověřovací stránka výtisku ukazuje jen platnost výtisku, ne jeho obsah

Šifrování a integrita dat

- šifrovaný přenos mezi prohlížečem a našimi servery
- šifrování dat v klidu zajišťuje Google Cloud na úrovni úložiště a databáze
- verzování dokumentů, soft delete se záznamem kdo a kdy, koš po dobu 30 dnů
- optimistické zamykání proti přepsání souběžnou úpravou; three-way merge při konfliktu synchronizace
- extrakce textu z dokumentů probíhá lokálně na našich serverech, nic se neposílá ven

Logy a dohledatelnost

- audit log zaznamenává uživatele, akci, entitu, starou a novou hodnotu, adresu, prohlížeč a projekt; uchováváme ho 24 měsíců
- 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
- obnovu ze zálohy zkusíme namátkově
- cílová dostupnost 99 % měsíčně podle SLA

Vývoj, lidé a sub-zpracovatelé

- oddělené vývojové a produkční prostředí; do vývoje nepoužíváme kopie ostrých zákaznických dat
- správa verzí kódu a revize změn před nasazením
- přístup k produkci má jen jednatel a případní spolupracovníci vázaní písemnou mlčenlivostí
- se sub-zpracovateli máme uzavřené zpracovatelské smlouvy

Co nemáme — otevřeně

- žádnou bezpečnostní certifikaci ani nezávislou auditní zprávu
- žádný nezávislý audit či externí bezpečnostní testování
- žádnou geografickou redundanci; vše běží v jednom regionu
- žádné závazné doby obnovení provozu ani maximální ztráty dat
- žádný nepřetržitý bezpečnostní dohled; monitoring je automatický, reakce člověka podle SLA

Fyzickou bezpečnost datových center — vstupy, kamery, napájení, hašení, likvidaci disků — zajišťuje Google Cloud jako provozovatel infrastruktury. My do datových center nemáme fyzický přístup a spoléháme se na jeho opatření.

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
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	volitelné přihlášení účtem	Evropská unie

Subjekt	Entita	Účel	Kde
	Limited	Microsoft	
Google	Google Ireland Limited	volitelné přihlášení účtem Google	Evropská unie

Poznámka ke Collabora Online. Editaci dokumentů přímo v prohlížeči zajišťuje Collabora Online, kterou provozujeme sami na vlastní virtuální infrastruktuře v Google Cloud. Dokumenty tedy při editaci neopouštějí naše prostředí a Collabora Online **není sub-zpracovatelem**.

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.