

Smlouva o zpracování osobních údajů (DPA)

⚠ DRAFT — PŘED POUŽITÍM REVIDOVAT ADVOKÁTEM Vychází z čl. 28 nařízení (EU) 2016/679 (GDPR) a doporučení Evropského sboru pro ochranu osobních údajů (EDPB).

Verze: 1.1 (draft pro právní revizi — pre-review) **Účinnost od:** [DD.MM.RRRR]

Verze 1.1 (2026-05-12) doplňuje oproti 1.0: kontaktní osobu pro GDPR (po Smluvních stranách), granulórní tabulku „Doba uchování dle kategorie údajů“ (čl. 2.2), rozšířený výčet 14 sub-processorů včetně AWS, Resend a Google (čl. 7.1), explicitní AI opt-in v sub-processor tabulce, detailní EU/EHP garanci s konkrétními regiony (čl. 8), prodloužený 90denní export při insolvenci + WORM Object Lock + OpenTimestamps garanci dostupnosti archivu (čl. 9.2 a 9.3).

Smluvní strany

Správce osobních údajů (Zákazník):

Obchodní firma: [Doplní Zákazník] IČO: [Doplní Zákazník] Sídlo: [Doplní Zákazník] Zastoupený: [Doplní Zákazník] (dále jen „**Správce**“)

Zpracovatel:

TaskGrip s.r.o. IČO: 21511306 Sídlo: nábřeží Závodu míru 1885, 530 02 Pardubice Zapsaná v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, oddíl C, vložka 52788 Zastoupený: Petr Slavík a Ing. Martin Malý, jednatelé (společnost zastupují vždy oba jednatelé společně) Kontakt pro GDPR: info@taskgrip.com (dále jen „**Zpracovatel**“)

Kontaktní osoba pro ochranu osobních údajů na straně Zpracovatele:

Ing. Martin Malý — jednatel Zpracovatele E-mail: info@taskgrip.com Telefon: +420 777 038 092

Poznámka: Zpracovatel s ohledem na rozsah a povahu zpracování nepodléhá povinnosti jmenovat pověřence pro ochranu osobních údajů (DPO) dle čl. 37 GDPR. Zpracovatel se k roli kontaktní osoby pro GDPR dobrovolně přihlašuje pro zjednodušení komunikace se Správcem.

uzavírají v souladu s **čl. 28 odst. 3 GDPR** tuto Smlouvu o zpracování osobních údajů (dále jen „**DPA**“).

1. Předmět DPA

1.1 Zpracovatel zpracovává pro Správce osobní údaje v rámci poskytování služby **TaskGrip Construction** (digitální stavební deník) na základě hlavní smlouvy uzavřené dle VOP Zpracovatele.

1.2 Tato DPA upravuje práva a povinnosti stran v souvislosti se zpracováním osobních údajů.

2. Předmět, doba a povaha zpracování

2.1 **Předmět zpracování:** vedení digitálního stavebního deníku, elektronické podepisování dokumentů, archivace.

2.2 **Doba zpracování** se liší podle kategorie údajů. Po uplynutí dané doby jsou údaje vymazány nebo anonymizovány, není-li dále uvedeno jinak:

Kategorie údajů	Doba uchování	Důvod
Podepsané stavební deníky (PDF + audit data)	10 let od dokončení stavby	§ 166 odst. 3 zák. č. 283/2021 Sb.
WORM archivní záznamy (Object Lock)	11 let od uložení	Zákonná archivace + technická rezerva
Hash chain a audit log	Po dobu trvání archivu (10–11 let)	Důkazní hodnota integrity dat
Provozní logy (přihlášení, IP, prohlížeč)	6 měsíců	Bezpečnost a detekce zneužití
Účetní a daňové doklady	10 let	§ 35 zák. č. 235/2004 Sb. o DPH
Customer support tickety	3 roky od uzavření	Smluvní obhajoba
Marketing kontakty / newsletter	Do odvolání souhlasu	Souhlas dle čl. 6 odst. 1 písm. a) GDPR
Neúspěšné registrace / opuštěné checkouty	30 dní	Bezpečnostní účely + technická rezerva
Údaje BankID Identify	Po dobu trvání smlouvy + 10 let archivu	§ 166 NSZ + plnění právní povinnosti
Přílohy (fotografie, dokumenty)	Po dobu trvání smlouvy + 10 let pro podepsané	Plnění smlouvy + archivace

2.3 **Povaha zpracování:** ukládání, organizace, strukturování, vyhledávání, sdělování přenosem, archivace.

2.4 **Účel zpracování:** plnění zákonných povinností Správce v oblasti stavebního práva, zajištění průkazné evidence stavebních činností.

3. Kategorie subjektů údajů a osobních údajů

3.1 Subjekty údajů

Kategorie	Příklad
Zaměstnanci Správce	stavbyvedoucí, mistři, dělníci
Externí pracovníci	TDI, autorský dozor, koordinátor BOZP
Zástupci investora / objednatele	jednatelé, projektoví manažeři
Subdodavatelé	jednatelé subdodavatelských firem
Návštěvy stavby	kontrolní orgány, hosté zaznamenaní v deníku

3.2 Kategorie zpracovávaných údajů

Identifikační a kontaktní:

- jméno a příjmení
- titul
- e-mail, telefonní číslo
- pracovní pozice / role na stavbě
- IČO / DIČ (u OSVČ)
- adresa pracoviště

Údaje pro elektronický podpis (KEP):

- kvalifikovaný certifikát (vydaný ICA / Signi)
- údaje o podpisu (čas, IP adresa, zařízení)
- BankID identifikace (jméno, bydliště, datum narození — dle úrovně BankID)

Provozní údaje:

- pracovní docházka na stavbě (čas příchodu/odchodu)
- GPS souřadnice (pokud Správce povolí GPS funkci)
- fotografie z místa stavby (mohou obsahovat osoby)
- IP adresy, log údaje o přihlášení

Zpracovatel NEzpracovává:

- ✗ údaje o zdravotním stavu (mimo BOZP záznamy)
- ✗ údaje o náboženském vyznání
- ✗ rodné číslo (s výjimkou BankID Identify, kde je předáno bankou)
- ✗ údaje o platebních kartách (zpracovává přímo Stripe)

4. Pokyny Správce

4.1 Zpracovatel zpracovává osobní údaje **výhradně na základě doložených pokynů Správce**, s výjimkou případů, kdy mu zpracování ukládá právo EU nebo členského státu.

4.2 Pokyny Správce jsou obsaženy:

a) v této DPA a hlavní smlouvě, b) v konfiguraci uživatelského účtu Správce, c) v dodatečných písemných instrukcích zaslaných na info@taskgrip.com.

4.3 Pokud se Zpracovatel domnívá, že pokyn Správce porušuje GDPR nebo jiný předpis o ochraně údajů, **neprodleně Správce informuje**.

5. Povinnosti Zpracovatele

Zpracovatel se zavazuje:

5.1 **Mlčenlivost:** Zajistit, aby osoby oprávněné zpracovávat osobní údaje byly zavázány k mlčenlivosti.

5.2 **Bezpečnostní opatření** (čl. 32 GDPR), zejména:

- šifrování dat v klidu (AES-256) i při přenosu (TLS 1.3+),
- pseudonymizaci kde je to možné,
- ochranu přístupu vícefaktorovou autentizací (MFA pro administrátorské účty),
- pravidelné penetrační testy (min. 1× ročně),
- zálohy s šifrováním a geografickou redundancí,
- detekci anomálií a monitoring přístupů,
- WORM (write-once-read-many) ukládání podepsaných dokumentů,
- denní kotvení integrity archivu do veřejného blockchainu.

5.3 **Sub-processoři:** Zapojit další zpracovatele pouze v souladu s čl. 7 této DPA.

5.4 **Asistence Správci** při:

a) plnění žádostí subjektů údajů (čl. 12–22 GDPR), b) plnění povinností dle čl. 32–36 GDPR (bezpečnost, hlášení incidentů, DPIA), c) komunikaci s dozorovým úřadem (ÚOOÚ).

5.5 **Hlášení bezpečnostních incidentů:** Zpracovatel oznámí Správci bezpečnostní incident **bez zbytečného odkladu, nejpozději do 48 hodin** od zjištění. Hlášení obsahuje:

- popis povahy incidentu,
- kategorie a přibližný počet dotčených subjektů údajů,
- pravděpodobné důsledky,
- přijatá nebo navrhovaná opatření.

5.6 **Podpora při auditu:** Umožnit Správci provedení auditu max. 1× ročně s předchozím oznámením 30 dní. Náklady auditu nese Správce. Audit lze nahradit certifikací ISO 27001 nebo SOC 2 Zpracovatele.

5.7 **Záznamy o činnostech:** Vést záznamy o zpracování dle čl. 30 odst. 2 GDPR.

6. Práva subjektů údajů

6.1 Zpracovatel poskytne Správci nezbytnou součinnost při plnění žádostí subjektů údajů, zejména:

- právo na přístup (čl. 15)
- právo na opravu (čl. 16)
- právo na výmaz (čl. 17)

- právo na omezení zpracování (čl. 18)
- právo na přenositelnost (čl. 20)
- právo vznést námitku (čl. 21)

6.2 **Výjimka z práva na výmaz:** Podepsané dokumenty uložené v důvěryhodném archivu **nelze vymazat před uplynutím zákonné archivační lhůty 10 let** (čl. 17 odst. 3 písm. b) GDPR — plnění právní povinnosti).

6.3 Žádosti subjektů údajů přijímá Správce; Zpracovatel poskytuje technickou součinnost do **15 dnů** od předání žádosti.

7. Sub-processoři

7.1 Správce uděluje Zpracovateli **obecný souhlas** se zapojením následujících sub-processorů:

Sub-processor	Účel	Lokalita	DPA
Vercel Inc.	Hosting webové aplikace, edge funkce, CDN	EU (Frankfurt, region fra1)	vercel.com/legal/dpa
Supabase Inc.	Databáze PostgreSQL, souborové úložiště, autentizace	EU (Frankfurt, region eu-central-1)	supabase.com/dpa
Amazon Web Services, Inc.	WORM archiv podepsaných dokumentů (S3 Object Lock Compliance Mode) + šifrovaný off-platform backup audit logu	EU (Frankfurt, region eu-central-1)	aws.amazon.com/agreement
Signi a.s.	Kvalifikovaný elektronický podpis, BankID integrace, důvěryhodný archiv PAdES-LTA	ČR	signi.com/dpa
První certifikační autorita, a.s. (ICA)	Vydání kvalifikovaného certifikátu (zapojena prostřednictvím Signi a.s.)	ČR	DPA mezi Signi a ICA
Bankovní identita, a.s.	BankID Sign / BankID Identify (zapojena prostřednictvím Signi a.s.)	ČR	DPA mezi Signi a Bankovní identitou
Stripe Payments Europe, Ltd. / Stripe Inc.	Platební brána (zpracování plateb, NE osobních údajů uživatelů Služby)	EU (Irsko) + USA (SCC + EU-US Data Privacy Framework)	stripe.com/legal/dpa
Ecomail.cz s.r.o.	Transakční e-maily (potvrzení účtu, notifikace, pozvánky) + případné marketingové newslettery	ČR / EU	ecomail.cz/podminky
Bird (MessageBird B.V.)	SMS OTP (dvoufaktorová autentizace)	EU (Nizozemsko)	messagebird.com/legal/dpa
Visual Crossing Corporation	Historická data počasí (pouze GPS souřadnice stavby, žádné osobní údaje)	USA	N/A — služba nezpracovává osobní údaje
OpenTimestamps + Bitcoin calendars	Veřejné kotvení hashe archivu (žádné osobní údaje , pouze SHA-256 hash)	distribuovaně	N/A — pouze hash
OpenAI, L.L.C. (přes Vercel AI Gateway nebo přímo)	AI funkce — pouze pokud Správce explicitně aktivuje AI funkce v nastavení účtu (defaultně vypnuté)	USA (SCC + EU-US DPF)	openai.com/policies/data-processing-addendum

Sub-processor	Účel	Lokalita	DPA
Anthropic PBC (přes Vercel AI Gateway nebo přímo)	AI funkce — pouze pokud Správce explicitně aktivuje AI funkce v nastavení účtu (defaultně vypnuté)	USA (SCC + EU-US DPF)	anthropic.com/legal/dpa
Google LLC (Google OAuth, volitelná Gmail integrace)	Sign-in s Google + volitelná Gmail synchronizace	EU/USA (SCC + EU-US DPF)	cloud.google.com/terms/data-processing-addendum

7.2 Zpracovatel je povinen **uložit sub-processorům smluvně stejné povinnosti** jako jsou uvedeny v této DPA.

7.3 O **změně sub-processorů** (přidání/výměna) Zpracovatel informuje Správce **e-mailem minimálně 30 dní předem**. Správce má právo proti změně **vznést písemnou námitku**; v takovém případě:

a) Zpracovatel může pro daného Správce sub-processora nezapojit, nebo b) Správce má právo smlouvu vypovědět bez sankce.

7.4 Aktuální seznam sub-processorů je publikován na www.taskgrip.cz/sub-processors.

8. Předávání osobních údajů do třetích zemí

8.1 **Hlavní zákaznická data** (databáze stavebních deníků, fotografie, audit log, podepsané dokumenty, údaje uživatelů) **jsou zpracovávána výhradně v rámci EU/EHP**, konkrétně:

- Databáze PostgreSQL a souborové úložiště: **Supabase, region eu-central-1 (Frankfurt)**
- Hosting aplikace, cron a edge funkce: **Vercel, region fra1 (Frankfurt)**
- WORM archiv podepsaných dokumentů: **AWS S3, region eu-central-1 (Frankfurt)**
- Šifrovaný off-platform backup audit logu: **AWS S3, region eu-central-1 (Frankfurt)**
- Kvalifikované elektronické podpisy a důvěryhodný archiv: **Signi a.s. (ČR)**

EU lokalita hlavních dat je garantována smluvně i technicky (region je hard-coded v konfiguraci nasazení Služby).

8.2 **Předání mimo EU/EHP** probíhá pouze v omezeném rozsahu pro:

a) **Stripe** — platební metadata (nezbytné minimum pro zúčtování plateb), b) **OpenAI / Anthropic** — texty a obrazové údaje, **pouze pokud Správce explicitně aktivuje AI funkce v nastavení účtu** (defaultně vypnuté), c) **Google** — pouze pokud Správce použije sign-in s Google nebo Gmail integraci, d) **Visual Crossing Weather API** — pouze GPS souřadnice stavby (žádné osobní údaje subjektů).

8.3 Veškerá předání mimo EU/EHP jsou zajištěna na základě:

a) **standardních smluvních doložek (SCC)** Komise EU dle čl. 46 odst. 2 GDPR, b) **certifikace EU-US Data Privacy Framework** (pro USA poskytovatele, kde je certifikace dostupná), c) výslovného souhlasu subjektu údajů (kde je to nezbytné dle čl. 49 GDPR).

9. Doba trvání a ukončení

9.1 Tato DPA je účinná po dobu trvání hlavní smlouvy.

9.2 Po ukončení hlavní smlouvy Zpracovatel:

a) umožní Správci **export osobních údajů po dobu 30 dnů** (export je bezplatný a probíhá ve strojově čitelném formátu — PDF/A pro dokumenty, JSON/CSV pro metadata, v souladu s čl. 20 GDPR), b) následně osobní údaje **smaže** ze všech systémů, c) **s výjimkou podepsaných dokumentů a auditních záznamů**, které jsou uchovávány v souladu se zákonnou archivační povinností (10 let dle stavebního zákona, eIDAS, čl. 17 odst. 3 písm. b) GDPR — plnění právní povinnosti), d) na žádost Správce vystaví **písemné potvrzení o smazání** s uvedením kategorií a období smazaných údajů, e) v případě **ukončení provozu Služby Zpracovatelem** (např. insolvence, likvidace) Zpracovatel poskytne **prodlouženou lhůtu 90 dnů pro export** a archiv podepsaných dokumentů předá nezávislé akreditované archivační službě dle čl. 8 odst. 4 VOP.

9.3 Pro zajištění **trvalé dostupnosti archivu** podepsaných dokumentů po dobu zákonné archivační lhůty využívá Zpracovatel:

a) **technický režim Object Lock Compliance Mode** (AWS S3, retence 11 let), který fyzicky znemožňuje smazání objektů kýmkoliv, včetně Zpracovatele a administrátora cloudového účtu, b) **nezávislé denní kotvení integrity** archivu do veřejného Bitcoin blockchainu (OpenTimestamps), umožňující prokázat existenci a integritu archivu k danému datu bez závislosti na infrastruktuře Zpracovatele.

10. Odpovědnost

10.1 Strany odpovídají za škodu způsobenou porušením této DPA dle obecných pravidel GDPR a občanského zákoníku.

10.2 Limitace odpovědnosti dle hlavní smlouvy se přiměřeně použije i na DPA, **s výjimkou pokuty uložené dozorovým úřadem** za prokazatelné porušení povinností Zpracovatele.

11. Závěrečná ustanovení

11.1 V případě rozporu mezi DPA a hlavní smlouvou má **přednost DPA** v otázkách zpracování osobních údajů.

11.2 Změny DPA vyžadují písemnou formu (postačuje e-mail s elektronickým podpisem).

11.3 DPA se řídí právem České republiky a GDPR.

Za Zpracovatele: TaskGrip s.r.o. Petr Slavík, jednatel Ing. Martin Malý, jednatel (společnost zastupují vždy oba jednatele společně) Datum: [DD.MM.RRRR]

Za Správce: [Doplní Zákazník] [Jméno + funkce] Datum: [DD.MM.RRRR]