SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

uzavřená podle čl. 28 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2016/679 (dále jen „GDPR“)

Smluvní strany

firma (právnická osoba nebo podnikající fyzická osoba), pro kterou je v Systému zřízeno prostředí, identifikovaná obchodní firmou, sídlem a IČO uvedenými v Systému (Nastavení → Firma) podle veřejného rejstříku,
za kterou jedná osoba, jež smlouvu v Systému potvrdila a prohlásila, že je k tomu oprávněna
kontaktní e-mail: e-mail uvedený při registraci nebo v nastavení firmy

(dále jen „Správce“)

a

Petr Kozák
místo podnikání Topolová 910, Mladá, 289 24 Milovice
IČO: 01530127, DIČ: CZ9004141069
fyzická osoba podnikající, zapsaná v živnostenském rejstříku
kontaktní e-mail: logos@logos-system.cz

(dále jen „Zpracovatel“)

Smluvní strany uzavírají tuto smlouvu ke smlouvě o poskytování služby LOGOS, případně k obchodním podmínkám zkušební verze (dále jen „Hlavní smlouva“), na jejímž základě Zpracovatel provozuje pro Správce informační systém LOGOS (dále jen „Systém“).

1. Předmět, povaha a účel zpracování

1.1 Zpracovatel zpracovává osobní údaje pro Správce výhradně za účelem provozu Systému: uložení, zobrazení, úpravy, vyhodnocení a výmazu údajů, které do Systému vkládá Správce nebo jeho uživatelé, zálohování, podpory a údržby.

1.2 Systém slouží k řízení obchodu, výroby, skladu, docházky, mezd a dokladů Správce.

1.3 Zpracování trvá po dobu trvání Hlavní smlouvy a dále po dobu potřebnou k vrácení a výmazu údajů podle čl. 9.

2. Kategorie subjektů a osobních údajů

Subjekty údajů	Osobní údaje
Uživatelé Systému (zaměstnanci a spolupracovníci)	jméno, přihlašovací jméno, e-mail, role a oprávnění, otisk hesla, identifikátor schváleného zařízení, záznamy o činnosti v Systému (historie změn), IP adresa v provozních záznamech
Pracovníci (evidence zaměstnanců)	jméno, osobní číslo, pozice, datum narození, adresa, telefon, e-mail, číslo osobního dokladu, typ smlouvy, datum nástupu a výstupu, otisk PIN a identifikátor čipu, docházka, výkazy práce a výkon, žádosti o volno, termíny pracovnělékařských prohlídek a školení, tarif, mzdové údaje a výplatnice, hodnocení
Uchazeči o zaměstnání	jméno, kontakt, termín a poznámky z pohovoru
Kontaktní osoby obchodních partnerů	jméno, funkce, e-mail, telefon, obsah obchodní komunikace (e-maily, zprávy datové schránky, chat)
Zákazníci s přístupem do portálu	e-mail, otisk hesla, jazyk, přehled objednávek
Fyzické osoby podnikající	údaje z dokladů a plateb (jméno, adresa, IČO, číslo účtu)

2.1 Zvláštní kategorie údajů (čl. 9 GDPR) Systém cíleně nezpracovává. Výjimkou je informace o pracovní neschopnosti a o termínu a platnosti pracovnělékařské prohlídky v rozsahu, který vyžaduje pracovněprávní evidence. Výsledky vyšetření ani diagnózy Správce do Systému nevkládá.

2.2 Rozsah údajů určuje Správce. Kategorie, které Správce nepoužívá (např. modul výplat), se nezpracovávají.

3. Povinnosti Zpracovatele

Zpracovatel se zavazuje:

- zpracovávat osobní údaje pouze na základě doložených pokynů Správce, včetně předání do třetích zemí. Pokynem je tato smlouva a obsluha Systému Správcem a jeho uživateli. Pokud by pokyn podle Zpracovatele porušoval právní předpisy, upozorní na to;
- zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- přijmout opatření podle čl. 32 GDPR popsaná v čl. 5 a v dokumentu Bezpečnostní opatření — LOGOS;
- dodržovat podmínky pro zapojení dalšího zpracovatele podle čl. 4;
- být Správci nápomocen prostřednictvím vhodných opatření při vyřizování žádostí subjektů údajů (přístup, oprava, výmaz, omezení, přenositelnost, námitka). Systém k tomu umožňuje údaje vyhledat, upravit, vyexportovat a smazat; co Správce nezvládne sám, provede Zpracovatel na jeho žádost;
- být Správci nápomocen při plnění povinností podle čl. 32 až 36 GDPR (zabezpečení, ohlašování porušení, posouzení vlivu,

předchozí konzultace), a to s ohledem na povahu zpracování a informace, které má Zpracovatel k dispozici;
- po skončení poskytování služeb osobní údaje podle rozhodnutí Správce vrátit nebo vymazat podle čl. 9;
- poskytnout Správci informace potřebné k doložení splnění povinností podle čl. 28 GDPR a umožnit audit podle čl. 7.

4. Další zpracovatelé

4.1 Správce uděluje obecné povolení k zapojení dalších zpracovatelů. Ke dni podpisu jde o tyto zpracovatele:

Zpracovatel	Činnost	Místo / záruky předání	Kdy
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Německo	pronájem serveru (datové centrum Norimberk), na kterém Systém běží a jsou uložena všechna data	EU (Německo)	vždy
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irsko (Google Disk)	uložení záložních kopií databáze a souborů mimo produkční server	EU; možný přístup ze USA — EU-US Data Privacy Framework (Google LLC)	vždy
Microsoft Ireland Operations Limited, One Microsoft Place, Leopardstown, Dublin 18, Irsko (OneDrive)	druhá záložní kopie mimo produkční server	EU; možný přístup ze USA — EU-US Data Privacy Framework (Microsoft Corporation)	vždy
Anthropic PBC, 548 Market Street, San Francisco, USA (příp. Anthropic Ireland, Limited, Dublin, Irsko — podle smluvních podmínek Anthropic)	funkce umělé inteligence (čtení výkresů, dokladů a výplatnic, návrhy technologie a kalkulace); zasílá se jen obsah zpracovávaného dokumentu, data se podle obchodních podmínek Anthropic nepoužívají k tréninku modelů	USA — standardní smluvní doložky (součást podmínek Anthropic pro zpracování dat)	jen je-li AI zapnuta

4.2 Za další zpracovatele se nepovažují služby, které si Správce sám zvolí a připojí vlastním účtem: jeho poštovní server (SMTP/IMAP), jeho banka (napojení Česká spořitelna), jeho datová schránka, jeho vlastní cloudové úložiště dokumentů (Google Disk / OneDrive Správce). Data tam Systém předává na pokyn Správce a ve vztahu k těmto službám je Správce smluvní stranou sám. Veřejné rejstříky (ARES, registr plátců DPH) se dotazují pouze podle IČO / DIČ firem.

4.3 O zamýšleném přidání nebo nahrazení dalšího zpracovatele informuje Zpracovatel Správce e-mailem nejméně 30 dnů předem. Správce může do 15 dnů vznést odůvodněnou námitku. Nedohodnou-li se strany, může Správce Hlavní smlouvu vypovědět bez sankce ke dni účinnosti změny.

4.4 Zpracovatel uloží dalšímu zpracovateli stejné povinnosti na ochranu osobních údajů, jaké má sám podle této smlouvy, a za jeho plnění odpovídá.

4.5 Správce může funkce umělé inteligence vypnout. Pak se jeho údaje zpracovateli podle řádku Anthropic nepředávají.

5. Zabezpečení

5.1 Zpracovatel zajišťuje zejména:

- oddělení dat: každý zákazník má vlastní databázi, firmu určuje adresa, ke které se uživatel přihlašuje, a přístup do databáze jiného zákazníka aplikace neumožňuje;
- šifrovaný přenos (HTTPS, TLS 1.2 a vyšší, HSTS), šifrované relace s cookie pouze přes HTTPS;
- přihlášení jen ze zařízení schváleného správcem firmy, omezení počtu pokusů o přihlášení, hesla a PIN pouze jako kryptografický otisk;
- oprávnění podle rolí a modulů vynucovaná na serveru, historie změn záznamů s autorem změny;
- tajná nastavení (hesla k poště, klíče k bance a službám) jsou jen pro zápis a do prohlížeče se nevracejí;
- každodenní zálohu databází a souborů, dvě kopie mimo produkční server, lokální retenci nejméně 7 dní, vzdálenou 60 dní, měsíční archiv 12 měsíců;
- automatizované testy před každým nasazením změny, nepřetržitou automatickou kontrolu provozu s upozorněním správci;
- firewall, ochranu proti opakovaným pokusům o přihlášení k serveru a pravidelnou aktualizaci serveru a knihoven.

5.2 Zpracovatel může opatření měnit, pokud tím nesníží úroveň zabezpečení.

6. Porušení zabezpečení osobních údajů

6.1 Zpracovatel ohlásí Správci porušení zabezpečení osobních údajů bez zbytečného odkladu, nejpozději do 24 hodin od okamžiku, kdy se o něm dozvěděl, e-mailem na kontaktní adresu Správce a telefonicky.

6.2 Ohlášení obsahuje informace podle čl. 33 odst. 3 GDPR: povahu porušení, kategorie a přibližný počet subjektů a záznamů, pravděpodobné důsledky a přijatá či navržená opatření. Informace, které ještě nejsou známé, doplní postupně.

6.3 Ohlášení dozorovému úřadu a subjektům údajů provádí Správce. Zpracovatel mu k tomu poskytne potřebnou součinnost a podklady.

6.4 Zpracovatel vede evidenci všech porušení zabezpečení týkajících se údajů Správce.

7. Kontrola a audit

7.1 Zpracovatel na žádost, nejvýše jednou ročně, poskytne aktuální dokument Bezpečnostní opatření, seznam dalších zpracovatelů a shrnutí výsledku posledního bezpečnostního testu, pokud byl proveden.

7.2 Audit na místě nebo vlastní bezpečnostní test Správce je možný po písemné dohodě o termínu a rozsahu, s oznámením nejméně 30 dnů předem, bez zásahu do dat jiných zákazníků a na náklady Správce. Při podezření na porušení zabezpečení lhůta neplatí.

8. Předání do třetích zemí

8.1 Data jsou uložena na serverech v Německu (EU). Do třetí země se předávají jen v rozsahu čl. 4 (záložní kopie u poskytovatelů s možným přístupem ze USA, funkce umělé inteligence), a to na základě rozhodnutí Evropské komise o odpovídající ochraně (EU-US Data Privacy Framework) nebo standardních smluvních doložek.

9. Vrácení a výmaz

9.1 Na žádost podanou do 30 dnů po skončení služby Zpracovatel předá data Správce ve strojově čitelném formátu (export databáze firmy ve formátu SQL, na žádost i CSV po tabulkách; soubory v původním formátu).

9.2 Po 60 dnech od skončení služby, nejdříve však po předání podle odst. 9.1, Zpracovatel databázi a soubory Správce smaže. Záložní kopie zaniknou uplynutím retence podle čl. 5, nejpozději do 12 měsíců (měsíční archiv). Do té doby se z nich data neobnovují jinak než na žádost Správce.

9.3 Na žádost vydá Zpracovatel potvrzení o výmazu.

10. Odpovědnost a závěrečná ustanovení

10.1 Odpovědnost stran se řídí čl. 82 GDPR a ustanoveními Hlavní smlouvy o odpovědnosti.

10.2 V otázkách ochrany osobních údajů má tato smlouva přednost před ostatními ujednáními stran.

10.3 Smlouva nabývá účinnosti dnem uzavření a trvá po dobu zpracování podle čl. 1.3. Vztahuje se i na zpracování před jejím uzavřením. Řídí se právem České republiky.

Uzavření

Smlouva se uzavírá elektronicky: osoba jednající za Nabyvatele (Zákazníka, Správce) ji v systému LOGOS otevře, zaškrtne prohlášení, že je oprávněna za firmu jednat, a potvrdí tlačítkem „Souhlasím“. Tím projevuje vůli být touto Smlouvou vázána; Poskytovatel ji uzavírá jejím zpřístupněním v Systému. Poskytovatel uchovává záznam o uzavření (datum a čas, jméno a přihlašovací jméno osoby, IP adresa, verze dokumentu) a zašle jej spolu s textem dokumentu na kontaktní e-mail firmy. Strany se mohou dohodnout i na listinném podpisu.