SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

uzavřená podle čl. 28 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2016/679 (obecné nařízení o ochraně osobních údajů, dále jen „GDPR“)

Verze 1.2 ze dne 30. září 2026

Smluvní strany

[OBCHODNÍ FIRMA KLIENTA]
IČO: [●], se sídlem [●],
zapsaná v obchodním rejstříku vedeném [●] soudem v [●], oddíl [●], vložka [●],
jednající [jméno a příjmení, funkce]
(dále jen „Správce“)

a

Hospitality CEE, s.r.o.
IČO: 19489617, se sídlem Kaprova 42/14, Staré Město, 110 00 Praha 1,
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 387413,
jednající Annou Dempsey, jednatelkou
(dále jen „Zpracovatel“)

(Správce a Zpracovatel společně dále jen „Smluvní strany“, jednotlivě „Smluvní strana“.)

Úvodní ustanovení

A. Zpracovatel provozuje webovou platformu pro manažerský reporting dostupnou pod doménou reporting.finance a pod obchodním označením „CZ Financial Reporting Paradise“ (dále jen „Služba“).

B. Správce Službu využívá nebo hodlá využívat na základě Hlavní smlouvy. Při poskytování Služby Zpracovatel pro Správce zpracovává osobní údaje obsažené zejména v účetních datech Správce a v uživatelských účtech.

C. Účelem této smlouvy je upravit práva a povinnosti Smluvních stran při tomto zpracování v souladu s čl. 28 GDPR.

Článek 1 – Definice a výklad

1.1 Pojmy „osobní údaje“, „zpracování“, „správce“, „zpracovatel“, „subjekt údajů“, „porušení zabezpečení osobních údajů“, „zvláštní kategorie osobních údajů“ a „dozorový úřad“ mají význam, který jim přiřazuje GDPR (zejména čl. 4 a 9).

1.2 „Hlavní smlouva“ je smlouva, na jejímž základě Zpracovatel poskytuje Správci Službu, tj. smlouva uzavřená podle Všeobecných obchodních podmínek služby reporting.finance (dále jen „VOP“) spolu s objednávkou a ceníkem, nebo jiná smlouva o poskytování Služby, včetně Podmínek beta testování služby reporting.finance, vždy ve znění pozdějších změn.

1.3 „Osobní údaje Správce“ jsou osobní údaje, které Zpracovatel zpracovává pro Správce při poskytování Služby a které jsou popsány v Příloze A.

1.4 „Uživatel“ je fyzická osoba, které Správce prostřednictvím svého administrátora zřídil přístup ke Službě.

1.5 „Další zpracovatel“ je subdodavatel, kterého Zpracovatel zapojí do zpracování Osobních údajů Správce (čl. 28 odst. 2 a 4 GDPR).

1.6 „Pracovní den“ je den, který není sobotou, nedělí ani svátkem v České republice.

1.7 Přílohy A (Popis zpracování), B (Technická a organizační opatření), C (Další zpracovatelé) a, použije-li se, D (Doplňková opatření pro zdravotní a obdobné údaje) jsou nedílnou součástí této smlouvy. Nadpisy slouží pouze pro orientaci.

Článek 2 – Předmět smlouvy a role Smluvních stran

2.1 Zpracovatel se zavazuje zpracovávat Osobní údaje Správce jménem Správce v rozsahu, za účelem a po dobu stanovené v této smlouvě a v Příloze A. Správce se zavazuje poskytovat Zpracovateli součinnost podle této smlouvy.

2.2 Správce je ve vztahu k Osobním údajům Správce správcem. Nahrává-li Správce do Služby účetní data jiných společností ze své skupiny, uvede tyto společnosti v Příloze A, části 2, a ve Službě potvrdí, že je každou z nich k nahrání oprávněn. Vůči Zpracovateli je Správce jediným kontaktním místem pro pokyny a oznámení. Zpracovatel může po každé další společnosti požadovat přistoupení k této smlouvě ve Službě nebo doložení oprávnění. Do přistoupení nebo doložení je Zpracovatel oprávněn nahrávání dat dané společnosti omezit nebo pozastavit. Je-li Správce ve vztahu k takovým údajům sám zpracovatelem, je Zpracovatel jeho dalším zpracovatelem a Správce zajistí, aby jeho smlouva s příslušným správcem takové zapojení umožňovala. Prohlášení o oprávnění nenahrazuje chybějící pokyn skutečného správce.

2.3 Zpracovatel je samostatným správcem (nikoli zpracovatelem) osobních údajů, které zpracovává pro vlastní účely, a to zejména: (a) kontaktních a fakturačních údajů Správce a jeho zástupců pro uzavření a plnění Hlavní smlouvy; (b) záznamů o uzavření této smlouvy (článek 16) a Hlavní smlouvy; a (c) bezpečnostních záznamů o přihlašování a přístupech v rozsahu nezbytném k ochraně Služby před zneužitím. Zpracování podle tohoto odstavce se řídí zásadami ochrany osobních údajů Zpracovatele pro uživatele zveřejněnými na https://reporting.finance/legal/user-privacy-notice. Jiné údaje Uživatelů (jméno, e-mail, role a nastavení účtu potřebné k poskytování Služby Správci) Zpracovatel zpracovává jako zpracovatel. Zaměstnanci a další osoby jednající z pověření Zpracovatele, včetně osob provozujících Službu, zpracovávají Osobní údaje Správce výhradně na pokyn Zpracovatele (čl. 29 a čl. 32 odst. 4 GDPR) a nejsou Dalšími zpracovateli.

2.4 Pokud by Zpracovatel v rozporu s touto smlouvou sám určil účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce (čl. 28 odst. 10 GDPR).

Článek 3 – Pokyny Správce

3.1 Zpracovatel zpracovává Osobní údaje Správce pouze na základě doložených pokynů Správce, a to i pokud jde o předání do třetí země nebo mezinárodní organizaci, ledaže mu zpracování ukládá právo Evropské unie nebo členského státu, které se na Zpracovatele vztahuje. V takovém případě Zpracovatel Správce informuje o tomto právním požadavku před zahájením zpracování, ledaže toto právo takové informování zakazuje z důležitých důvodů veřejného zájmu (čl. 28 odst. 3 písm. a) GDPR).

3.2 Doloženými pokyny Správce jsou: (a) tato smlouva a Hlavní smlouva; (b) nastavení a úkony, které ve Službě provedou Uživatelé Správce v rámci svých oprávnění (např. nahrání dat, mapování, pozvání Uživatele, export, výmaz); a (c) další pokyny udělené Správcem v písemné, včetně elektronické, formě prostřednictvím kontaktů uvedených v Příloze A, části 2.

3.3 Zpracovatel Správce neprodleně informuje, pokud má za to, že určitý pokyn porušuje GDPR nebo jiné předpisy Evropské unie či členského státu o ochraně osobních údajů. Do potvrzení nebo změny pokynu Správcem je Zpracovatel oprávněn provedení pokynu odložit.

3.4 Pokyny, které přesahují funkčnost Služby popsanou v Hlavní smlouvě, je Zpracovatel oprávněn odmítnout nebo provést za úplatu sjednanou předem. Tím nejsou dotčeny povinnosti Zpracovatele podle GDPR a této smlouvy.

3.5 Zpracovatel nepoužije Osobní údaje Správce ani jiná data Správce k vlastním účelům; zejména z nich nevytváří souhrnné ani anonymizované statistiky či srovnávací přehledy (benchmarky) a nepoužívá je k trénování modelů umělé inteligence. Tím není dotčen článek 2.3.

Článek 4 – Povinnosti Správce

4.1 Správce odpovídá za to, že má ke zpracování Osobních údajů Správce právní titul, že subjekty údajů byly o zpracování řádně informovány a že jeho pokyny jsou v souladu s právními předpisy.

4.2 Správce nahrává do Služby pouze údaje potřebné pro účely manažerského reportingu. Správce nebude do Služby záměrně nahrávat zvláštní kategorie osobních údajů (čl. 9 GDPR), osobní údaje týkající se rozsudků v trestních věcech a trestných činů (čl. 10 GDPR) ani rodná čísla, ledaže to výslovně uvede v Příloze A, části 2; v takovém případě se použije Příloha D. Správce bere na vědomí, že podrobně zaúčtované mzdy (např. srážky odborových příspěvků nebo náhrady mzdy při nemoci), texty účetních dokladů a fakturace zdravotním pojišťovnám či jmenovitě uvedeným pacientům mohou takové údaje obsahovat, a nahrává je přednostně v souhrnné podobě. Zákaz v tomto odstavci nezbavuje Zpracovatele povinnosti zavést přiměřená technická opatření (varování při importu, absence polí pro rodné číslo a diagnózu).

4.3 Správce spravuje Uživatele a jejich role, zajistí, aby přístup ke Službě měly jen osoby, které jej potřebují, a bez zbytečného odkladu zruší přístup osobám, které jej již nepotřebují. Správce odpovídá za jednání svých Uživatelů a zajistí, aby nesdíleli své přihlašovací údaje ani prostředky dvoufázového ověření.

4.4 Správce oznámí Zpracovateli bez zbytečného odkladu každé zjištěné nebo podezřelé porušení zabezpečení týkající se Služby nebo přístupových údajů svých Uživatelů.

Článek 5 – Mlčenlivost

5.1 Zpracovatel zajistí, aby se osoby oprávněné zpracovávat Osobní údaje Správce (zaměstnanci, členové orgánů a externí spolupracovníci) zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti (čl. 28 odst. 3 písm. b) GDPR), a aby tyto osoby zpracovávaly Osobní údaje Správce pouze na pokyn Zpracovatele v souladu s touto smlouvou (čl. 29 a čl. 32 odst. 4 GDPR).

5.2 Přístup k Osobním údajům Správce mají jen osoby, které jej potřebují k plnění povinností podle Hlavní smlouvy nebo této smlouvy. Pracovníci Zpracovatele, včetně zaměstnanců provozujících Službu, přistupují k datům Správce ve Službě pouze za účelem podpory na žádost Správce, řešení bezpečnostního incidentu nebo odstranění závady Služby; takový přístup se zaznamenává. Tito pracovníci jsou vázáni mlčenlivostí a zpracovávají údaje jen na pokyn Zpracovatele.

5.3 Povinnost mlčenlivosti trvá i po skončení této smlouvy a po skončení pracovního či jiného vztahu dotčených osob se Zpracovatelem.

Článek 6 – Zabezpečení zpracování

6.1 Zpracovatel přijme a udržuje technická a organizační opatření podle čl. 32 GDPR popsaná v Příloze B, s ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování i na různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob.

6.2 Zpracovatel je oprávněn opatření podle Přílohy B měnit v souvislosti s technickým vývojem, pokud tím nesníží celkovou úroveň zabezpečení. Podstatné změny oznámí Správci zveřejněním aktualizované Přílohy B ve Službě.

6.3 Správce potvrzuje, že se s opatřeními podle Přílohy B seznámil a že je s ohledem na povahu Osobních údajů Správce považuje za přiměřená.

Článek 7 – Další zpracovatelé

7.1 Správce uděluje Zpracovateli obecné písemné povolení k zapojení Dalších zpracovatelů (čl. 28 odst. 2 GDPR). Další zpracovatelé ke dni uzavření této smlouvy jsou uvedeni v Příloze C; Správce jejich zapojení tímto schvaluje.

7.2 Zpracovatel oznámí Správci zamýšlené přidání nebo nahrazení Dalšího zpracovatele nejméně 30 dní předem, a to e-mailem administrátorům Správce ve Službě a zveřejněním aktualizovaného seznamu na https://reporting.finance/legal/sub-processors. Oznámení uvede název a sídlo Dalšího zpracovatele, jeho činnost, zpracovávané kategorie údajů, místo zpracování a záruky pro případné předání do třetí země. Oznamuje-li Další zpracovatel změny svých subdodavatelů v kratší lhůtě, předá Zpracovatel oznámení Správci bez zbytečného odkladu po jeho obdržení, a umožňuje-li to lhůta Dalšího zpracovatele, nejméně 14 dní předem; jinak se použije článek 7.4 obdobně.

7.3 Správce může proti změně z oprávněných důvodů týkajících se ochrany osobních údajů vznést písemnou námitku do 14 dní od oznámení. Smluvní strany v dobré víře projednají řešení (např. nevyužití dotčené funkce pro Správce). Nedojde-li k dohodě do dne účinnosti změny, je Správce oprávněn Hlavní smlouvu v rozsahu dotčené Služby vypovědět s účinností nejpozději ke dni účinnosti změny, bez sankce; Zpracovatel mu vrátí poměrnou část předem uhrazené ceny za nevyčerpané období. Nevznese-li Správce námitku ve lhůtě, platí, že se změnou souhlasí.

7.4 Je-li nahrazení Dalšího zpracovatele nezbytné neodkladně z bezpečnostních důvodů nebo proto, že Další zpracovatel přestal službu poskytovat, může Zpracovatel změnu provést i v kratší lhůtě. Zpracovatel o tom Správce informuje bez zbytečného odkladu; práva Správce podle článku 7.3 se použijí obdobně.

7.5 Funkce Služby, které vyžadují zapojení nového Dalšího zpracovatele nebo novou činnost zpracování u Dalšího zpracovatele uvedeného v Příloze C (zejména budoucí funkce založené na umělé inteligenci), budou pro Správce zpřístupněny až po provedení postupu podle článků 7.2 a 7.3, a jde-li o volitelné funkce, až po jejich zapnutí administrátorem Správce. Funkce umělé inteligence budou využívat pouze služby, na které se vztahují smluvní podmínky Dalšího zpracovatele pro zpracování osobních údajů a u nichž zpracování probíhá v Evropské unii; Osobní údaje Správce nebudou použity k trénování modelů umělé inteligence.

7.6 Zpracovatel uloží každému Dalšímu zpracovateli smlouvou stejné povinnosti týkající se ochrany údajů, jaké má Zpracovatel podle této smlouvy, zejména povinnost poskytnout dostatečné záruky zavedení vhodných technických a organizačních opatření (čl. 28 odst. 4 GDPR). U Dalších zpracovatelů poskytujících standardizované cloudové služby může Zpracovatel využít jejich standardní smluvní podmínky o zpracování osobních údajů, pokud splňují požadavky čl. 28 GDPR. Podstatné odchylky od lhůt a práv v této smlouvě (zejména pokud jde o ohlašování incidentů, výmaz, audity a změny subdodavatelů) jsou uvedeny v Příloze C. Zpracovatel odpovídá Správci za plnění povinností Dalšího zpracovatele v plném rozsahu.

Článek 8 – Předávání do třetích zemí

8.1 Zpracovatel ukládá Osobní údaje Správce v Evropském hospodářském prostoru, zejména v datovém

centru Google Cloud v regionu europe-west3 (Frankfurt nad Mohanem, Německo); další místa zpracování uvádí Příloha C. Předání do třetí země nebo mezinárodní organizaci je přípustné pouze za podmínek kapitoly V GDPR (čl. 44 až 49).

8.2 Správce bere na vědomí a povoluje předání uvedená v Příloze C, která se opírají o: (a) rozhodnutí Komise o odpovídající ochraně podle čl. 45 GDPR, zejména prováděcí rozhodnutí Komise (EU) 2023/1795 ze dne 10. července 2023 o rámci EU-USA pro ochranu osobních údajů (EU-U.S. Data Privacy Framework), jde-li o příjemce certifikovaného podle tohoto rámce; nebo (b) standardní smluvní doložky podle prováděcího rozhodnutí Komise (EU) 2021/914 ze dne 4. června 2021 (čl. 46 odst. 2 písm. c) GDPR), případně s doplňkovými opatřeními.

8.3 Pozbude-li použitý mechanismus předání účinnosti (např. zrušením rozhodnutí o odpovídající ochraně), Zpracovatel bez zbytečného odkladu zajistí jiný mechanismus podle kapitoly V GDPR, nebo dotčené předávání ukončí, a o přijatém řešení Správce informuje.

8.4 Vyžaduje-li to předání podle Přílohy C, je Zpracovatel oprávněn uzavřít s Dalším zpracovatelem standardní smluvní doložky (modul 3 – předání mezi zpracovateli) vlastním jménem.

Článek 9 – Práva subjektů údajů

9.1 Zpracovatel Správci s ohledem na povahu zpracování pomáhá prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, plnit povinnost Správce reagovat na žádosti o výkon práv subjektů údajů stanovených v kapitole III GDPR (čl. 28 odst. 3 písm. e) GDPR).

9.2 Tuto pomoc Zpracovatel poskytuje především prostřednictvím funkcí Služby (zobrazení a export dat, výmaz importních dávek, správa Uživatelů), a nejsou-li k dispozici, na žádost Správce zaslanou podpoře Zpracovatele. Správce bere na vědomí, že Osobní údaje Správce ve Službě jsou kopiemi účetních záznamů vedených v jeho účetním softwaru; opravu je proto zpravidla třeba provést ve zdrojovém systému a data do Služby nahrát znovu.

9.3 Obdrží-li Zpracovatel žádost subjektu údajů přímo, postoupí ji bez zbytečného odkladu Správci a sám na ni věcně neodpoví, ledaže jej k tomu Správce pověří.

Článek 10 – Další součinnost

10.1 Zpracovatel Správci s ohledem na povahu zpracování a informace, které má k dispozici, poskytne přiměřenou součinnost při zajišťování souladu s povinnostmi podle čl. 32 až 36 GDPR, zejména při posouzení vlivu na ochranu osobních údajů a při předchozí konzultaci s dozorovým úřadem (čl. 28 odst. 3 písm. f) GDPR).

10.2 Součinnost spočívající v poskytnutí existující dokumentace (tato smlouva, její přílohy, dokumentace Dalších zpracovatelů) poskytuje Zpracovatel bezúplatně. Rozsáhlejší součinnost může Zpracovatel účtovat podle předem sdělené sazby; to neplatí, byla-li potřeba součinnosti vyvolána porušením povinností Zpracovatele.

Článek 11 – Porušení zabezpečení osobních údajů

11.1 Zpracovatel ohlásí Správci porušení zabezpečení Osobních údajů Správce bez zbytečného odkladu poté, co se o něm dozví (čl. 33 odst. 2 GDPR), nejpozději však do 48 hodin od okamžiku, kdy se o porušení dozví Zpracovatel. Za okamžik uvědomění se považuje i okamžik, kdy Zpracovatel obdrží oznámení od Dalšího zpracovatele. Ohlášení zašle na e-mailovou adresu pro bezpečnostní oznámení uvedenou v Příloze A, části 2, a administrátorům Správce ve Službě; hrozí-li vysoké riziko pro práva a svobody fyzických osob, pokusí se Zpracovatel Správce kontaktovat i telefonicky. Lhůta 48 hodin zavazuje Zpracovatele, nikoli Dalšího zpracovatele, jehož vlastní lhůta může být delší; Zpracovatel předá dostupné informace a doplní je podle článku 11.2.

11.2 Ohlášení obsahuje, pokud je to možné, informace uvedené v čl. 33 odst. 3 GDPR, zejména popis povahy porušení včetně kategorií a přibližného počtu dotčených subjektů údajů a záznamů, kontaktní osobu, pravděpodobné důsledky a přijatá nebo navrhovaná opatření. Nelze-li informace poskytnout současně, poskytne je Zpracovatel postupně bez dalšího zbytečného odkladu (čl. 33 odst. 4 GDPR).

11.3 Zpracovatel neprodleně přijme přiměřená opatření k zastavení porušení a ke zmírnění jeho možných nepříznivých dopadů, dokumentuje je a poskytne Správci součinnost při ohlášení porušení dozorovému úřadu a jeho oznámení subjektům údajů (čl. 33 a 34 GDPR). O ohlášení a oznámení rozhoduje Správce.

11.4 Bez předchozího souhlasu Správce Zpracovatel o porušení týkajícím se Osobních údajů Správce neinformuje třetí osoby, s výjimkou svých odborných poradců, dotčených Dalších zpracovatelů a orgánů veřejné moci, vyžaduje-li to právní předpis.

11.5 Ohlášení porušení zabezpečení Zpracovatelem není samo o sobě uznáním jeho zavinění ani odpovědnosti.

Článek 12 – Informace a audity

12.1 Zpracovatel zpřístupní Správci všechny informace potřebné k doložení splnění povinností stanovených v čl. 28 GDPR a umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje (čl. 28 odst. 3 písm. h) GDPR), a to za podmínek tohoto článku.

12.2 Správce nejprve využije: (a) tuto smlouvu a její přílohy; (b) písemné odpovědi Zpracovatele na přiměřený bezpečnostní dotazník, nejvýše jednou za 12 měsíců; a (c) certifikace a auditní zprávy Dalších zpracovatelů (např. ISO/IEC 27001 a SOC 2 u Google Cloud), pokud je Zpracovatel smí Správci zpřístupnit.

12.3 Nepostačují-li informace podle článku 12.2 k prokázání souladu, může Správce provést audit nebo kontrolu za těchto podmínek: (a) nejvýše jednou za 12 měsíců, ledaže audit nařídí dozorový úřad nebo navazuje na porušení zabezpečení Osobních údajů Správce; (b) na základě písemného oznámení doručeného nejméně 30 dní předem, které obsahuje navržený rozsah; (c) v Pracovní dny v obvyklé pracovní době, přednostně na dálku a bez narušení Služby; (d) auditor je vázán mlčenlivostí a není konkurentem Zpracovatele; (e) audit se nevztahuje na data jiných zákazníků ani na datová centra Dalších zpracovatelů; u nich se použijí jejich auditní zprávy (článek 12.2 písm. c)). Toto ujednání neomezuje oprávnění dozorového úřadu.

12.4 Náklady auditu nese Správce. Přesáhne-li součinnost Zpracovatele při auditu jeden člověkoden, může Zpracovatel účtovat odměnu podle přiměřené sazby oznámené předem. Odhalí-li audit podstatné porušení této smlouvy Zpracovatelem, nese Zpracovatel své náklady i přiměřené náklady auditu a porušení bez zbytečného odkladu odstraní. Náklady nese Zpracovatel také tehdy, byl-li audit vyvolán porušením zabezpečení, které Zpracovatel způsobil.

12.5 Zpracovatel vede záznamy o kategoriích činností zpracování prováděných pro Správce (čl. 30 odst. 2 GDPR) a na požádání spolupracuje s dozorovým úřadem (čl. 31 GDPR).

Článek 13 – Doba trvání

13.1 Tato smlouva nabývá účinnosti okamžikem jejího uzavření podle článku 16 a uzavírá se na dobu trvání Hlavní smlouvy. Zpracovával-li Zpracovatel Osobní údaje Správce již před uzavřením této smlouvy nebo zpracovává-li je bez Hlavní smlouvy (např. ve zkušebním provozu), vztahuje se tato smlouva i na toto zpracování.

13.2 Poruší-li Zpracovatel tuto smlouvu podstatným způsobem a nezjedná nápravu ani do 30 dní od písemné výzvy Správce, je Správce oprávněn tuto smlouvu i Hlavní smlouvu vypovědět s okamžitou účinností.

13.3 Ustanovení, která mají svou povahou trvat i po skončení této smlouvy (zejména články 5, 6, 8, 11, 14, 15 a 18), trvají do vrácení nebo výmazu všech Osobních údajů Správce, případně po dobu nezbytnou k uplatnění nároků; článek 5.3 tím není dotčen.

Článek 14 – Vrácení a výmaz osobních údajů

14.1 Za trvání této smlouvy může Správce kdykoli ze Služby exportovat reporty (zejména ve formátu Excel) a stáhnout nahrané zdrojové soubory, mapovací tabulky a účtový rozvrh ve strojově čitelném formátu (XLSX nebo CSV).

14.2 Po skončení Hlavní smlouvy má Správce po dobu 30 dní (dále jen „Období pro export“) přístup ke Službě v režimu pouze pro čtení za účelem exportu. Na žádost Správce podanou během Období pro export mu Zpracovatel jednou bezúplatně předá kompletní exportní balíček (původní nahrané soubory, mapovací tabulky a účtový rozvrh ve formátu XLSX nebo CSV a auditní záznam) do 10 Pracovních dnů od žádosti.

14.3 Po uplynutí Období pro export Zpracovatel Osobní údaje Správce ve Službě do 30 dní logicky vymaže nebo anonymizuje. Automatické zálohy databáze (Cloud SQL) se uchovávají 7 dní a poté automaticky zanikají. Zbytkové kopie v infrastruktuře Dalšího zpracovatele (Google Cloud) mohou být fyzicky odstraněny až v jeho standardním cyklu, který poskytovatel uvádí v délce až 180 dní; Zpracovatel k těmto kopiím za účelem poskytování Služby nepřistupuje.

14.4 Správce může písemně požádat o dřívější výmaz; dnem doručení žádosti Období pro export končí; je-li žádost podána za trvání Hlavní smlouvy, běží lhůta podle článku 14.3 ode dne jejího doručení. Na žádost Správce Zpracovatel provedení výmazu písemně (i e-mailem) potvrdí.

14.5 Povinnost výmazu se nevztahuje na údaje, které je Zpracovatel povinen uchovat podle práva, ani na údaje, které Zpracovatel zpracovává jako samostatný správce podle článku 2.3 (zejména záznam o přijetí této smlouvy, fakturační údaje a bezpečnostní záznamy). Záznam o přijetí se uchovává po dobu trvání smlouvy a 10 let po jejím skončení, bezpečnostní záznamy o přihlášení zpravidla 12 měsíců, faktury po dobu stanovenou daňovými předpisy.

Článek 15 – Odpovědnost

15.1 Odpovědnost Smluvních stran za újmu způsobenou porušením této smlouvy se řídí ustanoveními Hlavní smlouvy o odpovědnosti a jejím omezení; pro tyto účely se tato smlouva považuje za součást Hlavní smlouvy.

15.2 Celková odpovědnost Zpracovatele vůči Správci ze všech nároků podle této smlouvy a Hlavní smlouvy je omezena částkou rovnající se vyšší z těchto hodnot: (a) cena, kterou Správce uhradil za Službu za 12 měsíců předcházejících události, jež nárok založila; a (b) 10 000 EUR. Ve Zkušebním období a při bezúplatném užívání Služby, včetně užívání podle Podmínek beta testování, je odpovědnost omezena částkou 25 000 Kč. Totéž omezení stanoví článek 7.2 Podmínek beta testování a článek 14.2 VOP. Správní pokuty uložené Zpracovateli a náhrady, které Zpracovatel zaplatil subjektům údajů podle čl. 82 GDPR z důvodů výlučně na své straně, se do limitu podle tohoto článku nezapočítávají.

15.3 Omezení odpovědnosti se nepoužije na újmu způsobenou úmyslně nebo z hrubé nedbalosti, na újmu na přirozených právech člověka ani v dalších případech, kdy je omezení vyloučeno právními předpisy (§ 2898 zákona č. 89/2012 Sb., občanský zákoník). Toto ujednání se nedotýká odpovědnosti Smluvních stran vůči subjektům údajů podle čl. 82 GDPR.

15.4 Uhradí-li jedna Smluvní strana subjektu údajů plnou náhradu újmy, za kterou odpovídá i druhá Smluvní strana, má vůči ní právo na úhradu části náhrady odpovídající podílu odpovědnosti druhé Smluvní strany (čl. 82 odst. 5 GDPR). Správní pokutu nese Smluvní strana, které byla uložena.

Článek 16 – Uzavření smlouvy elektronicky

16.1 Tuto smlouvu lze uzavřít: (a) elektronickým přijetím ve Službě podle článku 16.2; nebo (b) podpisem obou Smluvních stran, a to vlastnoručním nebo elektronickým podpisem podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS), ve znění pozdějších předpisů.

16.2 Zpřístupněním této smlouvy ve Službě činí Zpracovatel návrh na uzavření smlouvy. Správce návrh přijme, když osoba oprávněná za něj jednat: (a) je přihlášena ke svému uživatelskému účtu ve Službě s rolí administrátora a účet má aktivní dvoufázové ověření (TOTP); (b) uvede nebo potvrdí své jméno a příjmení, funkci a identifikační údaje Správce a zvolí právní základ svého oprávnění (člen statutárního orgánu, prokurista, zmocněnec); (c) potvrdí, že je oprávněna za Správce tuto smlouvu uzavřít; (d) potvrdí, že se se smlouvou včetně příloh seznámila a přijímá ji jménem Správce, a že si je vědoma ujednání, podle nichž se změny považují za přijaté, nejsou-li odmítnuty (články 7.3 a 17.3), a ujednání o skupinových společnostech (článek 2.2); a (e) klikne na tlačítko „Přijímám jménem Správce“. Je-li zvolen základ „zmocněnec“, Zpracovatel může žádat nahrání plné moci. Smlouva je uzavřena okamžikem, kdy Služba přijetí zaznamená.

16.3 Služba o přijetí vytvoří záznam, který obsahuje zejména identifikační údaje Správce, jméno, funkci a e-mailovou adresu přijímající osoby, identifikátor jejího uživatelského účtu, datum a čas přijetí (UTC), IP adresu, identifikaci prohlížeče, označení verze smlouvy a kontrolní součet (hash) jejího textu. Záznam je uchováván systematicky, v časové posloupnosti a chráněn proti změnám.

16.4 Smluvní strany souhlasí s tím, že smlouva uzavřená podle článku 16.2 je uzavřena v písemné formě ve smyslu § 562 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, a čl. 28 odst. 9 GDPR, neboť tento způsob umožňuje zachycení obsahu právního jednání a určení jednající osoby, a že záznam podle článku 16.3 je spolehlivým záznamem ve smyslu § 562 odst. 2 občanského zákoníku.

16.5 Bez zbytečného odkladu, nejpozději do 24 hodin od přijetí, zašle Služba přijímající osobě, administrátorům Správce a Zpracovateli e-mail s potvrzením uzavření smlouvy a s kopií smlouvy ve formátu PDF, jejíž součástí jsou údaje ze záznamu podle článku 16.3. Znění smlouvy platné pro Správce a záznam o přijetí jsou Správci trvale k dispozici ve Službě.

16.6 Přijímající osoba prohlašuje, že je oprávněna za Správce jednat, zejména jako člen statutárního orgánu, prokurista nebo na základě plné moci. Zpracovatel je oprávněn požádat o doložení tohoto oprávnění nebo o uzavření smlouvy podle článku 16.1 písm. b). Zjistí-li Správce, že přijímající osoba k jednání oprávněna nebyla, oznámí to Zpracovateli bez zbytečného odkladu. Statutární orgán Správce může jednání ve Službě dodatečně schválit do 15 Pracovních dnů od výzvy Zpracovatele. Není-li oprávnění doloženo ani jednání schváleno, považuje se smlouva za neuzavřenou a Zpracovatel může zpracování pozastavit, dokud není smlouva uzavřena osobou k tomu oprávněnou. Mlčení Správce samo o sobě není schválením.

Článek 17 – Změny smlouvy

17.1 Zpracovatel uzavírá tuto smlouvu v běžném obchodním styku s větším počtem zákazníků a již při jejím uzavření je zřejmá rozumná potřeba jejích pozdějších změn, zejména v důsledku změn právních předpisů, rozhodnutí orgánů veřejné moci, technického vývoje Služby nebo změn Dalších zpracovatelů. Zpracovatel je proto oprávněn tuto smlouvu v přiměřeném rozsahu měnit (§ 1752 občanského zákoníku).

17.2 Změnu Zpracovatel oznámí nejméně 30 dní před její účinností e-mailem administrátorům Správce a oznámením ve Službě; oznámení obsahuje nové znění smlouvy a přehled změn. Zpracovatel může Správce požádat i o přijetí nového znění postupem podle článku 16.

17.3 Správce má právo změnu odmítnout a z tohoto důvodu Hlavní smlouvu i tuto smlouvu vypovědět ve výpovědní době tří měsíců, během níž se použije dosavadní znění; Zpracovatel vrátí Správci poměrnou část předem uhrazené ceny za období po skončení smlouvy. Podstatnou změnu zpracování (nový účel, nová zvláštní kategorie údajů, nový mechanismus předání mimo EHP) Zpracovatel může podmínit novým přijetím podle článku 16. Neodmítne-li Správce změnu písemně před její účinností a nevyžaduje-li se nové přijetí, platí, že ji přijal.

17.4 Změny vyvolané změnou právních předpisů nebo rozhodnutím dozorového úřadu mohou nabýt účinnosti dříve, vyžaduje-li to právní předpis nebo rozhodnutí. Změny Přílohy C se řídí článkem 7. Údaje v Příloze A, části 2, aktualizuje administrátor Správce ve Službě nebo je Správce oznámí Zpracovateli písemně. Jiné změny této smlouvy vyžadují písemnou dohodu Smluvních stran, a to i v elektronické formě.

Článek 18 – Rozhodné právo a řešení sporů

18.1 Tato smlouva se řídí právem České republiky s vyloučením jeho kolizních norem, zejména zákonem č. 89/2012 Sb., občanský zákoník, GDPR a zákonem č. 110/2019 Sb., o zpracování osobních údajů.

18.2 Spory z této smlouvy rozhodují soudy České republiky. Smluvní strany se v souladu s § 89a zákona č. 99/1963 Sb., občanský soudní řád, dohodly, že místně příslušným soudem prvního stupně je soud příslušný podle sídla Zpracovatele. Má-li Správce sídlo mimo Českou republiku, jde zároveň o dohodu o příslušnosti podle čl. 25 nařízení Evropského parlamentu a Rady (EU) č. 1215/2012, je-li použitelné.

Článek 19 – Závěrečná ustanovení

19.1 V případě rozporu mezi touto smlouvou a Hlavní smlouvou má ve věcech ochrany osobních údajů přednost tato smlouva. Uplatní-li se mezi Smluvními stranami standardní smluvní doložky, mají v případě rozporu přednost před touto smlouvou.

19.2 Tato smlouva je vyhotovena v českém a anglickém jazyce. V případě rozporu mezi jazykovými verzemi má přednost česká verze.

19.3 Je-li nebo stane-li se některé ustanovení této smlouvy neplatným nebo neúčinným, nedotýká se to ostatních ustanovení. Smluvní strany jej nahradí ustanovením, které se jeho účelu nejvíce blíží.

19.4 Oznámení podle této smlouvy se činí písemně, včetně e-mailu, na e-mail kontaktní osoby pro ochranu osobních údajů uvedený v Příloze A, části 2, a na adresu Zpracovatele privacy@reporting.finance.

19.5 Tato smlouva nahrazuje veškerá předchozí ujednání Smluvních stran o zpracování Osobních údajů Správce.

Podpisy (pouze při uzavření podle článku 16.1 písm. b); při elektronickém přijetí se nevyplňuje)

Za Správce / For the Controller
V [●] dne [●] / In [●] on [●]

_____
[jméno, funkce / name, position]

Příloha A – Popis zpracování

Část 1 – Obecný popis (platí pro všechny zákazníky)

Předmět zpracování: Poskytování Služby: webová platforma pro manažerský reporting nad účetními daty Správce (POHODA, Money S3 a další podporované účetní systémy).

Povaha zpracování: Přijetí nahraných souborů (případně načtení z propojeného zdroje dat Správce, pokud je sjednáno), uložení, strukturování, převod do jednotného účtového rozvrhu (mapování), agregace, konsolidace, výpočet ukazatelů, zobrazení Uživatelům, export (Excel), zálohování, zasílání transakčních e-mailů (pozvánky, obnovení hesla), výmaz.

Účel zpracování: Sestavování manažerských reportů Správce (výkaz zisku a ztráty, rozvaha, cash flow, konsolidace, klíčové ukazatele výkonnosti (KPI)); správa přístupů Uživatelů a zabezpečení Služby; podpora na žádost Správce.

Nahrávaná data: Účetní deník, účtový rozvrh, střediska, činnosti, zakázky a další číselníky z účetního systému; volitelně provozní statistiky hotelu z rezervačního systému (PMS); rozpočty.

Kategorie subjektů údajů: (a) dodavatelé a odběratelé Správce, kteří jsou fyzickými osobami, včetně podnikajících fyzických osob, a kontaktní osoby obchodních partnerů uvedené v textech dokladů; (b) zaměstnanci a členové orgánů Správce, jsou-li mzdy či odměny zaúčtovány jednotlivě; (c) hosté a jiní

zákazníci uvedení jménem na dokladech; (d) Uživatelé Služby.

Kategorie osobních údajů: (a)–(c): jméno a příjmení, IČO a DIČ, adresa, čísla dokladů, data, částky, texty účetních zápisů a dokladů, účty a střediska; u (b) též výše mezd a odměn, jsou-li takto zaúčtovány. (d): jméno, e-mail, role, jazyk, časy a výsledky přihlášení, IP adresa a identifikace prohlížeče, nastavení dvoufázového ověření (TOTP), auditní záznamy o importech, změnách mapování a rolí. Bezpečnostní záznamy o přihlášení zpracovává Zpracovatel též jako samostatný správce (článek 2.3 písm. c)).

Zvláštní kategorie údajů: Nejsou zamýšleny (viz článek 4.2). Případné výjimky uvede Správce v části 2; použije se na ně Příloha D.

Četnost a doba zpracování: Průběžně po dobu trvání Hlavní smlouvy a Období pro export; výmaz podle článku 14.

Místo zpracování: EHP – Google Cloud, region europe-west3 (Frankfurt, Německo); předání mimo EHP pouze podle Přílohy C.

Část 2 – Údaje Správce (vyplní Správce ve Službě nebo v této listině)

- Klientská skupina ve Službě: [●]
- Společnosti, jejichž data Správce nahrává (obchodní firma, IČO): [●]
- Potvrzení oprávnění za každou další společnost (článek 2.2) – ve Službě / přistoupením: [●]
- Zdrojové systémy (POHODA / Money S3 / jiný) a případný propojený zdroj dat: [●]
- Data od (období): [●]
- Mzdy zaúčtované jednotlivě? (ano / ne): [●]
- Provozní statistiky z PMS? (ano / ne): [●]
- Mohou data obsahovat zvláštní kategorie údajů nebo rodná čísla? (ne / ano – popis; použije se Příloha D): [●]
- Poskytovatel zdravotních služeb, zdravotní pojišťovna nebo obdobný subjekt? (ne / ano – použije se Příloha D): [●]
- Kontaktní osoba pro ochranu osobních údajů (jméno, e-mail, telefon): [●]
- Pověřenec pro ochranu osobních údajů, je-li jmenován: [●]
- E-mail pro bezpečnostní oznámení (článek 11): [●]
- Kontakt pro pokyny (článek 3.2 písm. c)): [●]

Příloha B – Technická a organizační opatření (čl. 32 GDPR)

1. Oddělení dat klientů

Data každé klientské skupiny jsou v databázi oddělena na úrovni řádků (PostgreSQL row-level security); aplikace i dávkové úlohy pracují vždy v kontextu jedné klientské skupiny a tento požadavek je ověřován automatickými testy.
Vývoj probíhá na fiktivních nebo demonstračních datech. Testovací (staging) prostředí je provozováno ve stejném regionu se stejnými opatřeními; data Správce do něj lze umístit jen s jeho předchozím písemným souhlasem (např. při akceptačním testování) a po skončení testu se vymažou.

2. Řízení přístupu a autentizace

Přístup na základě rolí (administrátor, editor, prohlížející); Uživatele zve a jejich role spravuje administrátor Správce.
Povinné dvoufázové ověření (TOTP, ověřovací aplikace s QR kódem při nastavení) pro administrátory, editory a pracovníky Zpracovatele; pro prohlížející je dvoufázové ověření dostupné, nikoli povinné. Tajné klíče TOTP jsou v databázi uloženy šifrovaně.
Omezení počtu pokusů o přihlášení (rate limiting); hesla se ukládají pouze jako solené hashe standardním algoritmem použitého frameworku.
Administrativní rozhraní je chráněno stejným dvoufázovým ověřením. Přijetí této smlouvy ve Službě vyžaduje aktivní TOTP administrátora.
Při importu Služba upozorní, pokud záhlaví sloupce naznačuje rodné číslo nebo diagnózu; Služba nemá pole pro rodné číslo ani diagnózu.

3. Přístup pracovníků Zpracovatele

Pracovníci Zpracovatele přistupují k datům Správce pouze pro podporu na žádost Správce, při řešení incidentu nebo odstranění závady; jsou vázáni mlčenlivostí.
Přístup ke cloudové infrastruktuře je omezen na nezbytné osoby a servisní účty s minimálními oprávněními; nasazení probíhá bez dlouhodobých klíčů (Workload Identity Federation).
Zařízení pracovníků, na nichž mohou být při podpoře dočasně uložena data Správce, mají šifrovaný disk, zámek obrazovky a aktualizovaný software; taková data se po vyřešení požadavku mažou.
Pracovníci Zpracovatele nevkládají data Správce do nástrojů umělé inteligence ani jiných služeb třetích stran, které nejsou uvedeny v Příloze C; s obecnými nástroji umělé inteligence (např. pro vývoj a testování) pracují pouze s fiktivními nebo demonstračními daty.

4. Šifrování a přenos

Veškerá komunikace se Službou probíhá šifrovaně (HTTPS/TLS); aplikační služby jsou dostupné pouze přes load balancer.
Data jsou v úložištích Google Cloud (databáze, souborové úložiště, zálohy) šifrována i v uloženém stavu (at rest).
Přístupové údaje a klíče jsou uloženy ve službě Secret Manager, s pevně určenými verzemi a řízeným přístupem.

5. Integrita a auditní stopa

Nahrané soubory se ukládají s kontrolním součtem SHA-256.
Auditní záznam importů, změn mapování a změn rolí Uživatelů; záznamy o přihlášení.
Změny kódu procházejí revizí a automatickými testy a jsou nasazovány nejprve do testovacího prostředí.

6. Dostupnost a obnova

Spravovaná infrastruktura Google Cloud v regionu europe-west3; automatické zálohy databáze (Cloud SQL) uchovávané 7 dní, s možností obnovy k určitému okamžiku.
Postup obnovy ze zálohy je dokumentován a alespoň jednou ročně ověřován.
Na žádost Správce lze vymazat jednotlivou importní dávku; výmaz se promítne do záloh v jejich běžném cyklu (článek 14.3).

7. Umístění dat

Databáze, soubory a zálohy jsou uloženy v EHP (europe-west3, Frankfurt). Síťová infrastruktura Google (globální load balancer) může šifrované spojení ukončit v nejbližším bodu sítě Google; data se tam neukládají.

8. Organizační opatření

Postup řešení bezpečnostních incidentů včetně ohlášení Správci do 48 hodin (článek 11).
Závazky mlčenlivosti všech osob s přístupem k datům; poučení o ochraně osobních údajů.
Výběr a kontrola Dalších zpracovatelů (Příloha C), přednostně s úložištěm v EHP a s certifikací ISO/IEC 27001 nebo SOC 2.
Záznamy o činnostech zpracování (čl. 30 odst. 2 GDPR) a postup výmazu po skončení smlouvy (článek 14).
Zdrojový kód je uložen v soukromém repozitáři a neobsahuje data zákazníků.

Příloha C – Další zpracovatelé

Stav ke dni: 30. září 2026. Aktuální seznam: https://reporting.finance/legal/sub-processors.

Další zpracovatel	Činnost	Údaje	Místo zpracování	Záruky pro předání
Google Cloud EMEA Limited, Dublin, Irsko (a její přidružené společnosti včetně Google LLC, USA)	Cloudová infrastruktura: Cloud Run, Cloud SQL (PostgreSQL), Cloud Storage, Secret Manager, load balancing, logování	Veškeré Osobní údaje Správce	EHP – europe-west3 (Frankfurt); přístup podpory Google a síťový okraj mohou být mimo EHP	Cloud Data Processing Addendum; EU-U.S. DPF (Google LLC certifikována); standardní smluvní doložky
Plus Five Five, Inc. (Resend), San Francisco, USA	Odesílání transakčních e-mailů (pozvánky, obnovení hesla, potvrzení o přijetí smlouvy)	Jméno a e-mail příjemce, obsah e-mailu, záznamy o doručení; neobsahuje účetní data	Odesílání z regionu EU (je-li nastaveno); správa účtu a záznamy v USA	EU-U.S. DPF (certifikace); standardní smluvní doložky v DPA společnosti Resend
Microsoft Ireland Operations Limited, Dublin, Irsko	E-mailová schránka podpory (Microsoft 365 / Exchange Online)	Obsah e-mailů, které Správce nebo Uživatelé zašlou podpoře (včetně případných příloh)	EHP (EU Data Boundary); omezené výjimky podle podmínek Microsoft	Microsoft Products and Services DPA; EU-U.S. DPF (Microsoft Corporation certifikována); standardní smluvní doložky

Nejsou Dalšími zpracovateli (nezpracovávají Osobní údaje Správce): GitHub (zdrojový kód), registrátor domén.

Plánované funkce umělé inteligence budou využívat modely (včetně modelů Claude společnosti Anthropic) poskytované společností Google v rámci služby Vertex AI s koncovým bodem v EU; zpracování se řídí podmínkami Google Cloud uvedenými výše. Tato nová činnost zpracování bude zahájena až po oznámení podle článku 7.2 a v souladu s článkem 7.5.

Zpracovatel doporučuje posílat účetní data výhradně nahráním do Služby, nikoli e-mailem.

Odchylky standardních smluvních podmínek Dalších zpracovatelů od této smlouvy, za které Zpracovatel Správci nadále odpovídá (článek 7.6): Google Cloud oznamuje incidenty „promptly and without undue delay“ (nikoli do 48 hodin), audit zajišťuje primárně auditními zprávami, fyzické odstranění dat po výmazu trvá až 180 dní a změny subdodavatelů oznamuje zpravidla 30 dní předem. Resend oznamuje změny subdodavatelů zpravidla 14 dní předem; jeho primární provoz a záznamy jsou v USA, odesílání může probíhat z regionu EU. Microsoft 365: EU Data Boundary s omezenými výjimkami podle podmínek společnosti Microsoft. Zpracovatel ověří zápisy v seznamu DPF (Plus Five Five, Inc.; Google LLC; Microsoft Corporation) před prvním použitím a uchová jejich výpis.

Příloha D – Doplňková opatření pro zdravotní a obdobné údaje

Použije se, pouze pokud je to uvedeno v Příloze A, části 2, nebo pokud ji Smluvní strany výslovně připojí.

D.1 Předmět a použití. Tato příloha se použije, jestliže Správce v Příloze A, části 2, uvede, že nahrávaná data mohou obsahovat zvláštní kategorie osobních údajů nebo rodná čísla, nebo že jde o poskytovatele zdravotních služeb, zdravotní pojišťovnu či osobu zpracovávající údaje o pacientech, nebo jestliže Smluvní strany tuto přílohu výslovně připojí. Není-li v této příloze stanoveno jinak, platí tato smlouva.

D.2 Účel a co Služba není. Účelem zpracování zůstává manažerský reporting (výnosy, náklady, střediska, konsolidace, KPI). Služba není zdravotnickou dokumentací, klinickým informačním systémem ani nástrojem pro poskytování zdravotní péče. Zpracovatel neurčuje, které pacientské nebo pojistné údaje Správce smí nahrát.

D.3 Pokyny Správce. Správce nahrává přednostně agregované údaje (obrat za středisko, počet výkonů bez jména pacienta, mzdové náklady v součtu). Záměrně nenahrává: zdravotnickou dokumentaci, diagnózy, kódy výkonů spojené se jménem pacienta, rodná čísla, výsledky vyšetření, fotografie pacientů. Připouští se, že text faktury zdravotní pojišťovně nebo jmenovitě označenému pacientovi může zdravotní údaj odhalit; takový údaj se zpracovává jen jako součást účetního záznamu pro reporting a jen je-li to uvedeno v Příloze A, části 2.

D.4 Role a právní tituly. Správce odpovídá za právní titul včetně čl. 9 odst. 2 GDPR (typicky péče o zdraví, pracovněprávní povinnosti nebo výslovný souhlas, podle jeho činnosti) a za informační povinnost vůči pacientům, zaměstnancům a jiným subjektům. Zpracovatel tyto tituly nepřezkoumává. Je-li Správce sám zpracovatelem jiného poskytovatele, zajistí, že smlouva s tímto poskytovatelem zapojení Zpracovatele a tuto přílohu dovoluje.

D.5 Doplňková technická a organizační opatření. K Příloze B se přidává: (a) ve Službě nejsou pole pro rodné číslo, diagnózu ani kód MKN; (b) import zobrazí varování, pokud záhlaví sloupce odpovídá rodnému číslu nebo slovu „diagnóza“; (c) přístup pracovníků Zpracovatele jen na tiket podpory nebo incident, se záznamem; (d) data Správce se neukládají trvale na přenosná zařízení – dočasný export na šifrovaném disku se po tiketu maže; (e) staging jen s předchozím písemným souhlasem a následným výmazem; (f) funkce umělé inteligence jsou pro tohoto Správce vypnuté, dokud Správce neudělí samostatný souhlas po posouzení vlivu.

D.6 Posouzení vlivu a součinnost. Zpracovatel doporučuje Správci posoudit vliv na ochranu osobních údajů (čl. 35 GDPR), pokud bude pravidelně nahrávat identifikovatelné zdravotní nebo pojistné údaje. Součinnost podle článku 10 této smlouvy zahrnuje poskytnutí této přílohy, Příloh B a C a popisu toků dat ve Službě. Samotné posouzení provádí Správce.

D.7 Porušení a výmaz. Ohlášení podle článku 11 této smlouvy u tohoto Správce vždy obsahuje informaci, zda se porušení mohlo týkat zdravotních nebo obdobných údajů. Správce může požádat o předčasný výmaz konkrétní importní dávky; Zpracovatel ji vymaže bez zbytečného odkladu, nejpozději do 15 dní, s výhradou záloh podle článku 14.3 této smlouvy.

D.8 Skupinové společnosti. Každá právnická osoba, jejíž data se nahrávají, musí být uvedena v Příloze A, části 2. Správce ve Službě potvrdí oprávnění za každou z nich, nebo daná osoba k této smlouvě a k této příloze přistoupí. Do té doby může Zpracovatel nahrávání dat dané osoby pozastavit. Prohlášení jedné společnosti nenahrazuje pokyn ostatních.

D.9 Oddělitelnost. Je-li některé ustanovení této přílohy neplatné nebo neúčinné, nejsou tím dotčena

ostatní ustanovení této přílohy a této smlouvy. V případě rozporu mezi touto přílohou a smlouvou má u zdravotních a obdobných údajů přednost tato příloha.

DATA PROCESSING AGREEMENT

concluded pursuant to Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, the “GDPR”)

Version 1.2 dated 30 September 2026

Parties

[CLIENT COMPANY NAME]
Company ID (IČO): [●], registered office at [●],
registered in the Commercial Register kept by the [●] Court in [●], section [●], file [●],
acting through [name, position]
(the “Controller”)

and

Hospitality CEE, s.r.o.
Company ID (IČO): 19489617, registered office at Kaprova 42/14, Staré Město, 110 00 Prague 1, Czech Republic,
registered in the Commercial Register kept by the Municipal Court in Prague, section C, file 387413,
acting through Anna Dempsey, executive director (jednatelka)
(the “Processor”)

(the Controller and the Processor together the “Parties”, each a “Party”.)

Recitals

A. The Processor operates a web-based management reporting platform available at the domain reporting.finance under the trade name “CZ Financial Reporting Paradise” (the “Service”).

B. The Controller uses or intends to use the Service under the Main Agreement. In providing the Service, the Processor processes, on behalf of the Controller, personal data contained mainly in the Controller’s accounting data and in user accounts.

C. The purpose of this Agreement is to set out the rights and obligations of the Parties in respect of that processing in accordance with Article 28 GDPR.

Article 1 – Definitions and interpretation

1.1 The terms “personal data”, “processing”, “controller”, “processor”, “data subject”, “personal data breach”, “special categories of personal data” and “supervisory authority” have the meaning given to them in the GDPR (in particular Articles 4 and 9).

1.2 “Main Agreement” means the agreement under which the Processor provides the Service to the Controller, i.e. the agreement concluded under the General Terms and Conditions of the reporting.finance Service (the “Terms”) together with the order and price list, or any other agreement for the provision of the Service, including the Beta Terms for the reporting.finance Service, in each case as amended.

1.3 “Controller Personal Data” means the personal data processed by the Processor on behalf of the Controller in providing the Service, as described in Annex A.

1.4 “User” means a natural person to whom the Controller, through its administrator, has granted access to the Service.

1.5 “Sub-processor” means a subcontractor engaged by the Processor in the processing of Controller Personal Data (Article 28(2) and (4) GDPR).

1.6 “Business Day” means a day other than a Saturday, Sunday or public holiday in the Czech Republic.

1.7 Annexes A (Description of processing), B (Technical and organisational measures), C (Sub-processors) and, where it applies, D (Supplementary measures for health and similar data) form an integral part of this Agreement. Headings are for convenience only.

Article 2 – Subject matter and roles of the Parties

2.1 The Processor undertakes to process Controller Personal Data on behalf of the Controller to the extent, for the purpose and for the duration set out in this Agreement and in Annex A. The Controller

undertakes to cooperate with the Processor as provided in this Agreement.

2.2 The Controller is the controller of the Controller Personal Data. Where the Controller uploads to the Service accounting data of other companies of its group, it shall list those companies in Annex A, Part 2 and confirm in the Service that each of them has authorised the upload. The Controller is the Processor's sole point of contact for instructions and notices. The Processor may require each further company to accede to this Agreement in the Service or to evidence its authority. Until accession or evidence is provided, the Processor may restrict or suspend uploads of that company's data. Where the Controller is itself a processor of such data, the Processor acts as its sub-processor and the Controller shall ensure that its agreement with the relevant controller permits such engagement. A representation of authority does not replace missing instructions from the actual controller.

2.3 The Processor is an independent controller (not a processor) of personal data that it processes for its own purposes, in particular: (a) contact and billing data of the Controller and its representatives for concluding and performing the Main Agreement; (b) records of the conclusion of this Agreement (Article 16) and of the Main Agreement; and (c) security records of sign-ins and access to the extent necessary to protect the Service against misuse. Processing under this paragraph is governed by the Processor's user privacy notice published at https://reporting.finance/legal/user-privacy-notice. Other User data (name, email, role and account settings needed to provide the Service to the Controller) are processed by the Processor as processor. Employees and other persons acting under the Processor's authority, including persons who operate the Service, process Controller Personal Data solely under the Processor's instructions (Articles 29 and 32(4) GDPR) and are not Sub-processors.

2.4 Should the Processor, in breach of this Agreement, determine the purposes and means of processing, it shall be considered a controller in respect of that processing (Article 28(10) GDPR).

Article 3 – Controller's instructions

3.1 The Processor processes Controller Personal Data only on documented instructions from the Controller, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Article 28(3)(a) GDPR).

3.2 The Controller's documented instructions are: (a) this Agreement and the Main Agreement; (b) settings made and actions taken in the Service by the Controller's Users within their permissions (e.g. uploading data, mapping, inviting a User, exporting, deleting); and (c) further instructions given by the Controller in writing, including electronically, through the contacts listed in Annex A, Part 2.

3.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. The Processor may suspend the execution of such instruction until the Controller confirms or amends it.

3.4 The Processor may decline instructions that go beyond the functionality of the Service described in the Main Agreement, or carry them out for a fee agreed in advance. This does not affect the Processor's obligations under the GDPR and this Agreement.

3.5 The Processor shall not use Controller Personal Data or other Controller data for its own purposes; in particular, it does not create aggregated or anonymised statistics or benchmarks from them and does not use them to train artificial-intelligence models. Article 2.3 is not affected.

Article 4 – Obligations of the Controller

4.1 The Controller is responsible for having a legal basis for the processing of Controller Personal Data, for data subjects having been duly informed of the processing, and for its instructions complying with the law.

4.2 The Controller shall upload to the Service only data needed for management reporting purposes. The Controller shall not knowingly upload special categories of personal data (Article 9 GDPR), personal data relating to criminal convictions and offences (Article 10 GDPR) or Czech birth numbers (rodná čísla), unless it expressly states so in Annex A, Part 2, in which case Annex D applies. The Controller acknowledges that payroll booked in detail (e.g. trade-union dues deductions or sick-pay compensation), texts of accounting documents and invoices to health insurers or named patients may contain such data, and shall preferably upload them in aggregated form. The prohibition in this paragraph does not relieve the Processor of the duty to implement reasonable technical measures (import warnings; no fields for birth numbers or diagnoses).

4.3 The Controller manages Users and their roles, ensures that only persons who need access to the Service have it, and revokes without undue delay the access of persons who no longer need it. The Controller is responsible for the conduct of its Users and shall ensure that they do not share their credentials or two-factor authentication devices.

4.4 The Controller shall notify the Processor without undue delay of any detected or suspected security breach affecting the Service or its Users' access credentials.

Article 5 – Confidentiality

5.1 The Processor shall ensure that persons authorised to process Controller Personal Data (employees, members of corporate bodies and external contractors) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Article 28(3)(b) GDPR), and that such persons process Controller Personal Data only on the Processor's instructions in accordance with this Agreement (Articles 29 and 32(4) GDPR).

5.2 Access to Controller Personal Data is limited to persons who need it to perform obligations under the Main Agreement or this Agreement. The Processor's staff, including employees who operate the Service, access the Controller's data in the Service only to provide support at the Controller's request, to handle a security incident or to fix a fault in the Service; such access is logged. Those staff are bound by confidentiality and process the data only on the Processor's instructions.

5.3 The duty of confidentiality survives the termination of this Agreement and the end of the employment or other relationship of the persons concerned with the Processor.

Article 6 – Security of processing

6.1 The Processor shall implement and maintain the technical and organisational measures under Article 32 GDPR described in Annex B, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons.

6.2 The Processor may change the measures in Annex B in line with technical developments, provided that the overall level of security is not reduced. The Processor shall notify the Controller of material changes by publishing an updated Annex B in the Service.

6.3 The Controller confirms that it has reviewed the measures in Annex B and considers them appropriate in view of the nature of the Controller Personal Data.

Article 7 – Sub-processors

7.1 The Controller grants the Processor a general written authorisation to engage Sub-processors (Article 28(2) GDPR). The Sub-processors as at the date of this Agreement are listed in Annex C; the Controller hereby approves their engagement.

7.2 The Processor shall notify the Controller of any intended addition or replacement of a Sub-processor at least 30 days in advance, by email to the Controller's administrators in the Service and by publishing the updated list at https://reporting.finance/legal/sub-processors. The notice shall state the Sub-processor's name and seat, its activity, the categories of data processed, the location of processing and the safeguards for any transfer to a third country. Where a Sub-processor notifies changes to its own subcontractors at shorter notice, the Processor shall pass the notice on to the Controller without undue delay after receipt and, where the Sub-processor's notice period allows, at least 14 days in advance; otherwise Article 7.4 applies mutatis mutandis.

7.3 The Controller may object to the change in writing on reasonable data-protection grounds within 14 days of the notice. The Parties shall discuss a solution in good faith (e.g. not using the affected feature for the Controller). If no agreement is reached by the date the change takes effect, the Controller may terminate the Main Agreement in respect of the affected Service with effect no later than that date, without penalty; the Processor shall refund the pro-rata portion of any prepaid fees for the unused period. If the Controller does not object within that period, it is deemed to have consented to the change.

7.4 Where a Sub-processor must be replaced urgently for security reasons or because it has ceased to provide its service, the Processor may make the change at shorter notice. It shall inform the Controller without undue delay; the Controller's rights under Article 7.3 apply mutatis mutandis.

7.5 Features of the Service that require engaging a new Sub-processor or a new processing activity by a Sub-processor listed in Annex C (in particular future artificial-intelligence features) will be made available to the Controller only after the procedure under Articles 7.2 and 7.3 has been completed and, where such features are optional, only after the Controller's administrator has switched them on. Artificial-intelligence features will use only services that are covered by the Sub-processor's data processing terms and in which processing takes place in the European Union; Controller Personal Data will not be used to train artificial-intelligence models.

7.6 The Processor shall impose on each Sub-processor, by contract, the same data protection obligations as those binding the Processor under this Agreement, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organisational measures (Article 28(4) GDPR). For Sub-processors providing standardised cloud services, the Processor may rely on their standard data processing terms, provided they meet the requirements of Article 28 GDPR. Material differences from the time limits and rights in this Agreement (in particular on incidents, deletion, audits and sub-processor changes) are set out in Annex C. The Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations.

Article 8 – Transfers to third countries

8.1 The Processor stores Controller Personal Data within the European Economic Area, primarily in the Google Cloud data centre region europe-west3 (Frankfurt am Main, Germany); other processing locations are set out in Annex C. Transfers to a third country or an international organisation are permitted only under the conditions of Chapter V GDPR (Articles 44 to 49).

8.2 The Controller acknowledges and authorises the transfers listed in Annex C, which rely on: (a) a Commission adequacy decision under Article 45 GDPR, in particular Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the EU-U.S. Data Privacy Framework, where the recipient is certified under that framework; or (b) the standard contractual clauses under Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Article 46(2)(c) GDPR), with supplementary measures where required.

8.3 If a transfer mechanism relied upon ceases to be effective (e.g. because an adequacy decision is invalidated), the Processor shall without undue delay put in place another mechanism under Chapter V GDPR or stop the transfer concerned, and inform the Controller of the solution adopted.

8.4 Where required for a transfer under Annex C, the Processor may conclude the standard contractual clauses (Module Three – processor to processor) with the Sub-processor in its own name.

Article 9 – Data subject rights

9.1 Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III GDPR (Article 28(3)(e) GDPR).

9.2 The Processor provides this assistance primarily through features of the Service (viewing and exporting data, deleting import batches, managing Users) and, where such features are not available, upon the Controller’s request sent to the Processor’s support. The Controller acknowledges that Controller Personal Data in the Service are copies of accounting records kept in its accounting software; rectification therefore normally has to be made in the source system and the data re-uploaded to the Service.

9.3 If the Processor receives a request directly from a data subject, it shall forward it to the Controller without undue delay and shall not respond to it on the merits unless authorised by the Controller to do so.

Article 10 – Further assistance

10.1 Taking into account the nature of the processing and the information available to it, the Processor shall provide the Controller with reasonable assistance in ensuring compliance with the obligations under Articles 32 to 36 GDPR, in particular with data protection impact assessments and prior consultation with the supervisory authority (Article 28(3)(f) GDPR).

10.2 Assistance consisting in providing existing documentation (this Agreement, its annexes, documentation of Sub-processors) is provided free of charge. The Processor may charge for more extensive assistance at a rate communicated in advance; this does not apply where the need for assistance results from the Processor’s breach of its obligations.

Article 11 – Personal data breaches

11.1 The Processor shall notify the Controller of a personal data breach affecting Controller Personal Data without undue delay after becoming aware of it (Article 33(2) GDPR) and in any event within 48 hours of the Processor becoming aware. The Processor is also deemed aware when it receives notice from a Sub-processor. The notice shall be sent to the security notification email address stated in Annex A, Part 2, and to the Controller’s administrators in the Service; where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the Processor shall also try to reach the Controller by telephone. The 48-hour period binds the Processor, not a Sub-processor whose own period may be longer; the Processor shall pass on the information available and supplement it under Article 11.2.

11.2 The notice shall contain, where possible, the information referred to in Article 33(3) GDPR, in particular a description of the nature of the breach including the categories and approximate number of data subjects and records concerned, a contact point, the likely consequences and the measures taken or proposed. Where it is not possible to provide the information at the same time, the Processor shall provide it in phases without undue further delay (Article 33(4) GDPR).

11.3 The Processor shall promptly take reasonable measures to contain the breach and mitigate its possible adverse effects, document them and assist the Controller in notifying the breach to the supervisory authority and communicating it to data subjects (Articles 33 and 34 GDPR). The decision on notification and communication rests with the Controller.

11.4 Without the Controller’s prior consent, the Processor shall not inform third parties of a breach

affecting Controller Personal Data, except its professional advisers, the Sub-processors concerned and public authorities where required by law.

11.5 The Processor’s notification of a breach does not in itself constitute an acknowledgement of fault or liability.

Article 12 – Information and audits

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller (Article 28(3)(h) GDPR), on the terms of this Article.

12.2 The Controller shall first rely on: (a) this Agreement and its annexes; (b) the Processor’s written answers to a reasonable security questionnaire, no more than once every 12 months; and (c) certifications and audit reports of Sub-processors (e.g. ISO/IEC 27001 and SOC 2 for Google Cloud), to the extent the Processor may share them with the Controller.

12.3 If the information under Article 12.2 is not sufficient to demonstrate compliance, the Controller may conduct an audit or inspection on the following terms: (a) no more than once every 12 months, unless ordered by a supervisory authority or following a personal data breach affecting Controller Personal Data; (b) with written notice of at least 30 days, including a proposed scope; (c) on Business Days during normal business hours, preferably remotely and without disrupting the Service; (d) the auditor is bound by confidentiality and is not a competitor of the Processor; (e) the audit does not extend to other customers' data or to Sub-processors' data centres, for which their audit reports are used. This clause does not limit the powers of a supervisory authority.

12.4 The Controller bears the costs of the audit. If the Processor’s assistance with the audit exceeds one person-day, the Processor may charge a reasonable fee at a rate communicated in advance. If the audit reveals a material breach of this Agreement by the Processor, the Processor bears its own costs and the reasonable costs of the audit and shall remedy the breach without undue delay. The Processor also bears the costs where the audit was triggered by a personal data breach it caused.

12.5 The Processor maintains a record of the categories of processing activities carried out on behalf of the Controller (Article 30(2) GDPR) and cooperates with the supervisory authority on request (Article 31 GDPR).

Article 13 – Term

13.1 This Agreement takes effect upon its conclusion under Article 16 and is concluded for the term of the Main Agreement. Where the Processor processed Controller Personal Data before this Agreement was concluded, or processes it without a Main Agreement (e.g. during a trial), this Agreement also applies to such processing.

13.2 If the Processor materially breaches this Agreement and fails to remedy the breach within 30 days of the Controller’s written notice, the Controller may terminate this Agreement and the Main Agreement with immediate effect.

13.3 Provisions which by their nature are intended to survive termination (in particular Articles 5, 6, 8, 11, 14, 15 and 18) survive until all Controller Personal Data have been returned or deleted or, where relevant, for as long as needed to assert claims; Article 5.3 is not affected.

Article 14 – Return and deletion of personal data

14.1 During the term of this Agreement, the Controller may at any time export reports from the Service (in particular in Excel format) and download uploaded source files, mapping tables and the chart of accounts in a machine-readable format (XLSX or CSV).

14.2 After the Main Agreement ends, the Controller has read-only access to the Service for 30 days for export purposes (the “Export Period”). At the Controller’s request made during the Export Period, the Processor shall provide once, free of charge, a complete export package (original uploaded files, mapping tables and the chart of accounts in XLSX or CSV format, and the audit log) within 10 Business Days of the request.

14.3 After the Export Period the Processor shall logically delete or anonymise Controller Personal Data in the Service within 30 days. Automated database backups (Cloud SQL) are retained for 7 days and then expire in that cycle. Residual copies in a Sub-processor’s infrastructure (Google Cloud) may be physically erased only in that provider’s standard cycle, which the provider states may take up to 180 days; the Processor does not access those copies to provide the Service.

14.4 The Controller may request earlier deletion in writing; the Export Period ends on the day the request is received; if the request is made during the term of the Main Agreement, the period under Article 14.3 runs from its receipt. At the Controller’s request, the Processor shall confirm the deletion in writing (email

sufficing).

14.5 The deletion duty does not apply to data the Processor must keep by law, or to data the Processor processes as an independent controller under Article 2.3 (in particular the record of acceptance of this Agreement, billing data and security logs). The acceptance record is kept for the term of the Agreement and 10 years after it ends, sign-in security logs as a rule for 12 months, and invoices for the period required by tax law.

Article 15 – Liability

15.1 The Parties' liability for harm caused by a breach of this Agreement is governed by the provisions of the Main Agreement on liability and its limitation; for this purpose, this Agreement is deemed to form part of the Main Agreement.

15.2 The Processor’s aggregate liability to the Controller for all claims under this Agreement and the Main Agreement is limited to the higher of: (a) the fees paid by the Controller for the Service in the 12 months preceding the event giving rise to the claim; and (b) EUR 10,000. During the Beta Period and for free use of the Service, including use under the Beta Terms, liability is limited to CZK 25,000. Article 7.2 of the Beta Terms and Article 14.2 of the Terms set the same limit. Administrative fines imposed on the Processor and compensation the Processor has paid to data subjects under Article 82 GDPR solely by reason of its own conduct do not count towards the limit under this Article.

15.3 The limitation of liability does not apply to harm caused intentionally or by gross negligence, to harm to a person’s natural rights or in other cases where limitation is excluded by law (Section 2898 of Act No. 89/2012 Coll., the Civil Code). This provision does not affect the Parties' liability towards data subjects under Article 82 GDPR.

15.4 Where one Party has paid full compensation to a data subject for harm for which the other Party is also liable, it may claim back from the other Party the part of the compensation corresponding to the other Party’s share of responsibility (Article 82(5) GDPR). An administrative fine is borne by the Party on which it was imposed.

Article 16 – Electronic conclusion

16.1 This Agreement may be concluded: (a) by electronic acceptance in the Service under Article 16.2; or (b) by signature of both Parties, either handwritten or by an electronic signature under Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS), as amended.

16.2 By making this Agreement available in the Service the Processor offers to conclude it. The Controller accepts the offer when a person authorised to act on its behalf: (a) is signed in to his or her user account in the Service with the administrator role and that account has active two-factor authentication (TOTP); (b) enters or confirms his or her name, position and the Controller’s identification details and selects the basis of authority (member of the statutory body, registered proxy (prokurista), attorney-in-fact); (c) confirms that he or she is authorised to conclude this Agreement on behalf of the Controller; (d) confirms that he or she has read this Agreement including its annexes and accepts it on behalf of the Controller, and that he or she is aware of the provisions under which changes are deemed accepted unless rejected (Articles 7.3 and 17.3) and of the provisions on group companies (Article 2.2); and (e) clicks the button “Accept on behalf of the Controller”. Where “attorney-in-fact” is selected, the Processor may require a power of attorney to be uploaded. The Agreement is concluded when the Service records the acceptance.

16.3 The Service creates a record of the acceptance containing in particular the Controller’s identification details, the name, position and email address of the accepting person, the identifier of his or her user account, the date and time of acceptance (UTC), the IP address, browser identification, the version identifier of this Agreement and a checksum (hash) of its text. The record is kept systematically, in chronological order and protected against alteration.

16.4 The Parties agree that an Agreement concluded under Article 16.2 is concluded in written form within the meaning of Section 562(1) of Act No. 89/2012 Coll., the Civil Code, and Article 28(9) GDPR, since this method allows the content of the legal act to be captured and the acting person to be identified, and that the record under Article 16.3 is a reliable record within the meaning of Section 562(2) of the Civil Code.

16.5 Without undue delay, and no later than 24 hours after acceptance, the Service shall send to the accepting person, the Controller’s administrators and the Processor an email confirming the conclusion of the Agreement with a PDF copy of the Agreement, including the data from the record under Article 16.3. The version of the Agreement applicable to the Controller and the acceptance record remain permanently available to the Controller in the Service.

16.6 The accepting person represents that he or she is authorised to act on behalf of the Controller, in particular as a member of its statutory body, as a registered proxy (prokurista) or under a power of attorney. The Processor may request evidence of such authority or ask for the Agreement to be concluded under Article 16.1(b). If the Controller becomes aware that the accepting person was not authorised, it shall notify the Processor without undue delay. The Controller’s statutory body may ratify the act in the Service within 15 Business Days of the Processor’s request. If authority is neither evidenced

nor the act ratified, the Agreement is treated as not concluded and the Processor may suspend processing until it is concluded by a person with authority. The Controller's silence alone is not ratification.

Article 17 – Amendments

17.1 The Processor concludes this Agreement in the ordinary course of business with a larger number of customers, and a reasonable need for later amendments is apparent at the time of conclusion, in particular due to changes in legislation, decisions of public authorities, technical development of the Service or changes of Sub-processors. The Processor may therefore amend this Agreement to a reasonable extent (Section 1752 of the Civil Code).

17.2 The Processor shall notify an amendment at least 30 days before it takes effect, by email to the Controller's administrators and by a notice in the Service; the notice shall include the new version and a summary of the changes. The Processor may also ask the Controller to accept the new version using the procedure in Article 16.

17.3 The Controller may reject the amendment and, for that reason, terminate the Main Agreement and this Agreement with a notice period of three months, during which the existing version applies; the Processor shall refund the pro-rata portion of prepaid fees for the period after the Agreement ends. The Processor may require a material change to the processing (a new purpose, a new special category of data, a new transfer mechanism outside the EEA) to be accepted again under Article 16. If the Controller does not reject the amendment in writing before it takes effect and a fresh acceptance is not required, the Controller is deemed to have accepted it.

17.4 Amendments required by changes in law or by a decision of a supervisory authority may take effect earlier where the law or decision so requires. Changes to Annex C are governed by Article 7. The details in Annex A, Part 2, are updated by the Controller's administrator in the Service or notified by the Controller to the Processor in writing. Other amendments to this Agreement require a written agreement of the Parties, which may be in electronic form.

Article 18 – Governing law and disputes

18.1 This Agreement is governed by the laws of the Czech Republic, excluding its conflict-of-laws rules, in particular Act No. 89/2012 Coll., the Civil Code, the GDPR and Act No. 110/2019 Coll., on the Processing of Personal Data.

18.2 Disputes arising from this Agreement shall be decided by the courts of the Czech Republic. In accordance with Section 89a of Act No. 99/1963 Coll., the Code of Civil Procedure, the Parties agree that the court of first instance having local jurisdiction shall be the court competent for the Processor's registered office. Where the Controller has its seat outside the Czech Republic, this also constitutes a choice-of-court agreement under Article 25 of Regulation (EU) No 1215/2012 of the European Parliament and of the Council, where applicable.

Article 19 – Final provisions

19.1 In the event of conflict between this Agreement and the Main Agreement, this Agreement prevails in matters of personal data protection. Where standard contractual clauses apply between the Parties, they prevail over this Agreement in the event of conflict.

19.2 This Agreement is made in the Czech and English languages. In the event of any discrepancy between the language versions, the Czech version prevails.

19.3 If any provision of this Agreement is or becomes invalid or ineffective, the remaining provisions are not affected. The Parties shall replace it with a provision that comes closest to its purpose.

19.4 Notices under this Agreement shall be given in writing, including by email, to the email of the data protection contact stated in Annex A, Part 2, and to the Processor at privacy@reporting.finance.

19.5 This Agreement supersedes all prior arrangements between the Parties on the processing of Controller Personal Data.

Signatures (only where concluded under Article 16.1(b); not used for electronic acceptance)

Za Zpracovatele / For the Processor
V Praze dne [●] / In Prague on [●]

_____
Anna Dempsey, jednatelka / executive director

Annex A – Description of processing

Part 1 – General description (applies to all customers)

Subject matter: Provision of the Service: a web-based management reporting platform operating on the Controller's accounting data (POHODA, Money S3 and other supported accounting systems).

Nature of processing: Receipt of uploaded files (or retrieval from a connected data source of the Controller, where agreed), storage, structuring, mapping to a common chart of accounts, aggregation, consolidation, calculation of indicators, display to Users, export (Excel), backup, sending of transactional emails (invitations, password resets), deletion.

Purpose of processing: Preparation of the Controller's management reports (profit and loss, balance sheet, cash flow, consolidation, KPIs); administration of User access and security of the Service; support at the Controller's request.

Data uploaded: Accounting journal, chart of accounts, cost centres (střediska), activities, contracts and other code lists from the accounting system; optionally hotel operating statistics from the property management system (PMS); budgets.

Categories of data subjects: (a) the Controller's suppliers and customers who are natural persons, including sole traders, and contact persons of business partners named in document texts; (b) the Controller's employees and members of its corporate bodies, where salaries or remuneration are booked individually; (c) guests and other customers named on documents; (d) Users of the Service.

Categories of personal data: (a)–(c): name, company and VAT IDs, address, document numbers, dates, amounts, texts of accounting entries and documents, accounts and cost centres; for (b) also salary and remuneration amounts where so booked. (d): name, email, role, language, sign-in times and results, IP address and browser identification, two-factor (TOTP) settings, audit records of imports, mapping changes and role changes. The Processor also processes sign-in security records as an independent controller (Article 2.3(c)).

Special categories of data: Not intended (see Article 4.2). Any exceptions are stated by the Controller in Part 2 and are governed by Annex D.

Frequency and duration: Continuously during the term of the Main Agreement and the Export Period; deletion under Article 14.

Location of processing: EEA – Google Cloud, region europe-west3 (Frankfurt, Germany); transfers outside the EEA only as set out in Annex C.

Part 2 – Controller details (completed by the Controller in the Service or in this document)

- Client group in the Service: [●]
- Companies whose data the Controller uploads (name, company ID): [●]
- Confirmation of authority for each further company (Article 2.2) – in the Service / by accession: [●]
- Source systems (POHODA / Money S3 / other) and any connected data source: [●]
- Data from (period): [●]
- Payroll booked per person? (yes / no): [●]
- PMS operating statistics? (yes / no): [●]
- May the data contain special categories or birth numbers? (no / yes – description; Annex D applies): [●]
- Healthcare provider, health insurer or similar? (no / yes – Annex D applies): [●]
- Data protection contact (name, email, phone): [●]
- Data protection officer, if appointed: [●]
- Email for security notices (Article 11): [●]
- Contact for instructions (Article 3.2(c)): [●]

Annex B – Technical and organisational measures (Article 32 GDPR)

1. Separation of client data

Each client group's data are separated at row level in the database (PostgreSQL row-level security); the application and batch jobs always operate in the context of a single client group, and this requirement is verified by automated tests.
Development uses fictitious or demo data. The staging environment runs in the same region with the same measures; Controller data may be placed there only with the Controller's prior written consent (e.g. for acceptance testing) and are deleted when testing ends.

2. Access control and authentication

Role-based access (admin, editor, viewer); Users are invited and their roles managed by the Controller's administrator.
Mandatory two-factor authentication (TOTP, authenticator app with a QR code at set-up) for admins, editors and the Processor's staff; two-factor authentication is available to viewers but not mandatory. TOTP secrets are stored encrypted in the database.
Rate-limited sign-in; passwords are stored only as salted hashes using the framework's standard algorithm.
The administration interface is protected by the same two-factor authentication. Acceptance of this Agreement in the Service requires the administrator's active TOTP.
On import, the Service warns if a column header suggests a birth number or diagnosis; the Service has no fields for birth numbers or diagnoses.

3. Processor staff access

The Processor's staff access Controller data only for support at the Controller's request, incident handling or fault resolution; they are bound by confidentiality.
Access to the cloud infrastructure is limited to the persons and service accounts that need it, with least privilege; deployments run without long-lived keys (Workload Identity Federation).
Staff devices on which Controller data may be temporarily stored during support have disk encryption, screen lock and up-to-date software; such data are deleted once the request is resolved.
The Processor's staff do not enter Controller data into artificial-intelligence tools or other third-party services not listed in Annex C; general-purpose AI tools (e.g. for development and testing) are used only with fictitious or demo data.

4. Encryption and transmission

All communication with the Service is encrypted (HTTPS/TLS); application services are reachable only through the load balancer.
Data are encrypted at rest in Google Cloud storage (database, file storage, backups).
Credentials and keys are stored in Secret Manager, with pinned versions and controlled access.

5. Integrity and audit trail

Uploaded files are stored with a SHA-256 checksum.
Audit log of imports, mapping changes and User role changes; sign-in records.
Code changes go through review and automated tests and are deployed to the staging environment first.

6. Availability and recovery

Managed Google Cloud infrastructure in region europe-west3; automated database backups (Cloud SQL) retained for 7 days, with point-in-time recovery.
The restore-from-backup procedure is documented and tested at least annually.
At the Controller's request an individual import batch can be deleted; the deletion reaches backups in their normal cycle (Article 14.3).

7. Data location

The database, files and backups are stored in the EEA (europe-west3, Frankfurt). Google's network infrastructure (global load balancer) may terminate the encrypted connection at the nearest Google network edge; data are not stored there.

8. Organisational measures

Incident response procedure including notification to the Controller within 48 hours (Article 11).
Confidentiality undertakings from all persons with access to data; data protection instructions.
Selection and review of Sub-processors (Annex C), preferring EEA storage and ISO/IEC 27001 or SOC 2 certification.
Records of processing activities (Article 30(2) GDPR) and the post-termination deletion procedure (Article 14).
Source code is kept in a private repository and contains no customer data.

Annex C – Sub-processors

Status as at: 30 September 2026. Current list: https://reporting.finance/legal/sub-processors.

Sub-processor	Activity	Data	Location	Transfer safeguards
Google Cloud EMEA Limited, Dublin, Ireland (and its affiliates incl. Google LLC, USA)	Cloud infrastructure: Cloud Run, Cloud SQL (PostgreSQL), Cloud Storage, Secret Manager, load balancing, logging	All Controller Personal Data	EEA – europe-west3 (Frankfurt); Google support access and network edge may be outside the EEA	Cloud Data Processing Addendum; EU-U.S. DPF (Google LLC certified); standard contractual clauses
Plus Five Five, Inc. (Resend), San Francisco, USA	Sending transactional emails (invitations, password resets, acceptance confirmations)	Recipient name and email, email content, delivery logs; no accounting data	Sending from the EU region (where configured); account management and logs in the USA	EU-U.S. DPF (certified); standard contractual clauses in Resend's DPA
Microsoft Ireland Operations Limited, Dublin, Ireland	Support mailbox (Microsoft 365 / Exchange Online)	Content of emails the Controller or Users send to support (including any attachments)	EEA (EU Data Boundary); limited exceptions under Microsoft's terms	Microsoft Products and Services DPA; EU-U.S. DPF (Microsoft Corporation certified); standard contractual clauses

Not Sub-processors (no Controller Personal Data): GitHub (source code), domain registrar.

Planned artificial-intelligence features will use models (including Anthropic's Claude models) provided by Google through Vertex AI with an EU endpoint; processing is governed by the Google Cloud terms above. This new processing activity will start only after notice under Article 7.2 and in accordance with Article 7.5.

The Processor recommends sending accounting data only by uploading it to the Service, not by email.

Differences between the Sub-processors' standard terms and this Agreement, for which the Processor remains liable to the Controller (Article 7.6): Google Cloud notifies incidents "promptly and without undue delay" (not within 48 hours), provides audits primarily through audit reports, physically erases data up to 180 days after deletion and typically gives 30 days' notice of sub-processor changes. Resend typically gives 14 days' notice of sub-processor changes; its primary operations and logs are in the USA, while sending may use an EU region. Microsoft 365: EU Data Boundary with limited exceptions under Microsoft's terms. The Processor shall verify the DPF list entries (Plus Five Five, Inc.; Google LLC; Microsoft Corporation) before first use and keep a copy.

Annex D – Supplementary measures for health and similar data

Applies only where so stated in Annex A, Part 2, or where the Parties expressly attach it.

D.1 Subject and application. This annex applies where the Controller states in Annex A, Part 2 that uploaded data may contain special categories of personal data or birth numbers, or that it is a healthcare provider, health insurer or a person processing patient data, or where the Parties expressly attach this annex. This Agreement applies except as this annex provides otherwise.

D.2 Purpose and what the Service is not. The purpose of processing remains management reporting (revenue, cost, cost centres, consolidation, KPIs). The Service is not a medical record, a clinical information system or a tool for providing healthcare. The Processor does not decide which patient or insurance data the Controller may upload.

D.3 Controller instructions. The Controller shall preferably upload aggregated data (turnover by cost centre, procedure counts without patient names, payroll in total). It shall not knowingly upload: health records, diagnoses, procedure codes linked to a patient name, birth numbers, test results, patient photographs. It is accepted that the text of an invoice to a health insurer or a named patient may reveal health data; such data are processed only as part of the accounting record for reporting and only where so stated in Annex A, Part 2.

D.4 Roles and legal bases. The Controller is responsible for the legal basis including Article 9(2) GDPR (typically healthcare, employment law or explicit consent, depending on its activity) and for informing

patients, employees and other data subjects. The Processor does not review those bases. If the Controller is itself a processor for another provider, it shall ensure that its contract with that provider permits engaging the Processor and this annex.

D.5 Supplementary technical and organisational measures. In addition to Annex B: (a) the Service has no fields for birth number, diagnosis or ICD code; (b) import shows a warning if a column header matches a birth number or the word “diagnosis”; (c) Processor staff access only on a support ticket or incident, and is logged; (d) Controller data are not stored permanently on portable devices – a temporary export on an encrypted disk is deleted after the ticket; (e) staging only with prior written consent and subsequent deletion; (f) artificial-intelligence features stay off for this Controller until the Controller gives separate consent after an impact assessment.

D.6 Impact assessment and assistance. The Processor recommends that the Controller carry out a data-protection impact assessment (Article 35 GDPR) if it will regularly upload identifiable health or insurance data. Assistance under Article 10 of this Agreement includes providing this annex, Annexes B and C and a description of data flows in the Service. The assessment itself is the Controller’s.

D.7 Breach and deletion. A notice under Article 11 of this Agreement for this Controller always states whether the breach may have affected health or similar data. The Controller may request early deletion of a specific import batch; the Processor shall delete it without undue delay and within 15 days, subject to backups under Article 14.3 of this Agreement.

D.8 Group companies. Each legal entity whose data are uploaded must be listed in Annex A, Part 2. The Controller shall confirm authority for each of them in the Service, or that entity shall accede to this Agreement and this annex. Until then the Processor may suspend uploads of that entity’s data. One company’s representation does not replace instructions from the others.

D.9 Severability. If any provision of this annex is invalid or ineffective, the other provisions of this annex and of this Agreement are not affected. In the event of conflict between this annex and this Agreement, this annex prevails for health and similar data.