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 1.5 ze dne 27. října 2026 (nahrazuje verzi 1.2 ze dne 30. září 2026, verzi 1.3 ze dne 22. října 2026 a verzi 1.4 ze dne 26. října 2026). Datum účinnosti je uvedeno při zveřejnění na https://cfopanorama.com/legal/ a v oznámení podle článku 17.2.

Smluvní strany

— doplní se při přijetí —
IČO: — doplní se při přijetí —, se sídlem — doplní se při přijetí —,
— doplní se při přijetí —,
za niž jedná — doplní se při přijetí —
(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 cfopanorama.com a pod obchodním označením „CFO Panorama“ (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. Během bezúplatné beta fáze jde o smlouvu podle Podmínek beta testování služby CFO Panorama („Podmínky beta testování“). Jiná, zejména placená smlouva se použije jen tehdy, pokud ji Smluvní strany řádně uzavřely; tyto podmínky samy nezavádějí placenou službu.

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, jejíž přístup ke Službě pro Správce byl řádně schválen, ať již na základě pozvánky nebo schválené samostatné registrace. Registrace ani role administrátora samy nezakládají oprávnění uzavřít smlouvu za Správce.

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 Každá přímo smluvní společnost a její role jsou určeny v záznamu o přijetí nebo podepsané dohodě a v Příloze A, části 2. Nahrává-li Správce údaje dalších společností, zajistí buď jejich platné přistoupení prostřednictvím oprávněných zástupců, nebo doloží, že je zpracovává jako zpracovatel a že příslušný správce povolil zapojení Zpracovatele jako dalšího zpracovatele podle čl. 28 GDPR. Před umožněním nahrávání údajů dané společnosti musí být příslušné oprávnění a smluvní zapojení doloženo. Jedna osoba může přijmout smlouvu za více společností pouze v rozsahu oprávnění za každou z nich. Společné kontaktní místo uděluje pokyny a přijímá oznámení jen v rozsahu příslušného pověření; samotná příslušnost ke skupině toto pověření nenahrazuje.

2.3 Zpracovatel jedná jako samostatný správce pouze pro vlastní, samostatně určené účely: správu smluvního vztahu a kontaktů, plnění vlastních účetních a daňových povinností, nezbytné zabezpečení Služby a prokazování právních nároků. Pro tyto účely zpracovává jen nezbytné údaje podle zásad ochrany osobních údajů na https://cfopanorama.com/legal/user-privacy-notice. Účetní obsah a uživatelské a provozní záznamy vedené pro reporting Správce zpracovává jako zpracovatel; toto postavení se posuzuje podle účelu, nikoli pouze podle názvu databázové tabulky. Stejný údaj může sloužit různým účelům, ale samostatné správcovství neopravňuje k plošnému ponechání klientských dat po výmazu. Osoby přímo podřízené Zpracovateli jednají podle jeho pokynů v souladu s pokyny Správce; u samostatných dodavatelů se podle skutečné činnosti posoudí režim Dalšího zpracovatele.

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 jsou tato smlouva a Hlavní smlouva, úkony a nastavení oprávněných Uživatelů a další písemné, včetně elektronických, pokyny oprávněných kontaktů podle Přílohy A. Uzavřením smlouvy Správce dává trvalý pokyn k nezbytnému přístupu a zpracování pro onboarding, nastavení a provoz reportingu, import, kontrolu a mapování dat, diagnostiku a řešení problémů, podporu, údržbu, obnovu a zabezpečení Služby. Tento pokyn zahrnuje technické opravy a úpravy dat potřebné k provedení sjednaného reportingu; obchodní rozhodnutí, věcné účetní volby a přidělení nových uživatelských oprávnění musí odpovídat pověření Správce. V tomto rozsahu není nutný samostatný souhlas ani tiket pro každý přístup pracovníka. Činnosti nad tento rozsah vyžadují další doložený pokyn.

3.3 Zpracovatel Správce neprodleně informuje, pokud má za to, že pokyn porušuje GDPR nebo jiné použitelné předpisy o ochraně osobních údajů, a může jeho provedení pozastavit do vyjasnění. Pokyn, o němž zjistí, že je protiprávní, neprovede ani po jeho potvrzení Správcem.

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 jen údaje potřebné pro manažerský reporting. Bez předchozí písemné dohody se Zpracovatelem o konkrétním rozsahu a opatřeních nebude záměrně nahrávat zvláštní kategorie osobních údajů podle čl. 9 GDPR, údaje podle čl. 10 GDPR ani rodná čísla. Výjimka se zaznamená v Příloze A, části 2; použije se Příloha D a případná další sjednaná opatření. Samotné jednostranné vyplnění Přílohy A nepostačuje. Správce zajistí příslušný právní základ a další podmínky podle práva; DPA je nenahrazuje. Podrobné mzdy, texty dokladů a fakturace pacientům či zdravotním pojišťovnám mohou citlivé údaje obsahovat; Správce přednostně používá souhrnné nebo očištěné exporty. Zpracovatel přijme přiměřená opatření k omezení nechtěného importu; automatické upozornění nenahrazuje kontrolu Správce ani nezaručuje odhalení všech takových údajů.

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 Pověření pracovníci Zpracovatele mohou mít plný administrátorský přístup ke kterékoli klientské skupině v rozsahu nezbytném k provádění pokynů podle článku 3.2. Mohou zejména nahrávat, kontrolovat a mapovat data, provádět technické opravy, pořizovat nebo měnit zápisy ve Službě podle sjednaného reportingu, připravovat výstupy a spravovat uživatele v rozsahu pověření Správce. Přístup není omezen na čtení a nemusí být podmíněn samostatným požadavkem podpory. Oprávnění samo neopravňuje k nesouvisejícímu použití údajů. Přístup je omezen na pracovníky, kteří jej potřebují, podléhá mlčenlivosti, dvoufázovému ověření a přiměřenému záznamu bezpečnostně významných činností podle Přílohy B.

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. Toto potvrzení nezbavuje Zpracovatele jeho zákonných povinností.

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://cfopanorama.com/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 změna nezbytná naléhavě z bezpečnostních důvodů nebo pro ukončení služby Dalšího zpracovatele, oznámí Zpracovatel důvod a ochranná opatření co nejdříve, pokud možno předem. Zachová podmínky povolení podle čl. 28 odst. 2 GDPR a skutečnou možnost vznést námitku; lhůta k námitce je 14 dní od oznámení. Nelze-li zapojení zákonně provést v rámci stávajícího povolení, získá před předáním konkrétní povolení nebo dotčené zpracování pozastaví. Článek 7.3 se použije obdobně.

7.5 Funkce vyžadující nového Dalšího zpracovatele nebo novou činnost u stávajícího Dalšího zpracovatele se zavádějí postupem podle článků 7.2 až 7.4. Funkce umělé inteligence nejsou aktuálně aktivní; pro Správce budou spuštěny pouze po oznámení konkrétního rozsahu, dodavatelů, umístění, uchování a předání údajů a po výslovné aktivaci oprávněným administrátorem. Aktivace je doloženým pokynem klienta, nikoli náhradou právního základu subjektů údajů. Zpracovatel předem ověří podmínky konkrétního modelu; zpracování pro tyto funkce bude probíhat v EU a údaje Správce nebudou použity k trénování modelů.

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. Uvedení odchylek v Příloze C nezhojuje nesoulad s GDPR. Zpracovatel zajistí odpovídající smluvní krytí a zpřístupní informace potřebné k identifikaci relevantních Dalších zpracovatelů a ověření jejich záruk.

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 Zpracovatel ověří použitelný mechanismus a rozsah předání včetně relevantních navazujících předání. Pozbude-li mechanismus účinnosti, zajistí před pokračováním dotčeného předávání jiný platný mechanismus, jinak je pozastaví nebo ukončí, a Správce informuje. Samotné umístění úložiště nebo koncového bodu v EU nepotvrzuje všechny lokality zpracování. Informace o použitých zárukách jsou Správci dostupné na žádost.

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. Součinnost poskytne bez zbytečného odkladu tak, aby Správce mohl splnit příslušné zákonné lhůty; její rozsah zohlední povahu údajů a žádosti.

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. Spor o odměnu nesmí zdržet součinnost nezbytnou k dodržení zákonné lhůty.

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 je nejzazší lhůtou, nikoli oprávněním oznámení odkládat. Zpracovatel předá dostupné informace bez zbytečného odkladu a doplní je podle článku 11.2; nečeká na úplné vyšetření. Odlišné podmínky Dalšího zpracovatele neomezují zákonné povinnosti Zpracovatele ani článek 7.6.

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. Uvedená omezení se nepoužijí v rozsahu, v němž by bránila nezbytnému ověření podle čl. 28 GDPR, zejména při důvodném podezření na porušení nebo ověřování nápravy. Strany zachovají přiměřenou ochranu důvěrnosti, bezpečnosti a provozu; audity Dalších zpracovatelů se přednostně řeší dostupnými nezávislými zprávami a navazující součinností.

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. Účtované náklady nesmějí nepřiměřeně bránit výkonu zákonného práva na audit.

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 řádným uzavřením podle článku 16 a trvá po dobu Hlavní smlouvy a následného zpracování nezbytného podle článku 14. Nahrávání údajů Správce se umožní až po platném smluvním zapojení; zpětné ujednání samo nezhojuje dřívější nesoulad s GDPR.

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 přístup pouze pro čtení za účelem exportu („Období pro export“), pokud prostřednictvím oprávněné osoby nepožádá o dřívější výmaz. Správce rozhodne, zda budou údaje vráceny a následně vymazány, nebo přímo vymazány. Na žádost během Období pro export Zpracovatel jednou bezúplatně předá do 10 Pracovních dnů export Osobních údajů

Správce v běžně používaném strojově čitelném formátu, včetně dostupných zdrojových souborů, mapování, účtového rozvrhu, zápisů a dalších klientských údajů; není povinen vytvářet záznamy, které již byly oprávněně vymazány.

14.3 Po skončení Období pro export Zpracovatel bez zbytečného odkladu vymaže Osobní údaje Správce z aktivních systémů a zajistí výmaz příslušných kopií, včetně exportů a kopií u Dalších zpracovatelů. Výmaz není pouhým skrytím dat v rozhraní. Automatické zálohy Cloud SQL zanikají v sedmidenním cyklu; zbytkové kopie v infrastruktuře Google mohou být fyzicky odstraněny až v jeho standardním cyklu, podle použitelných podmínek až do 180 dní od zahájení příslušného výmazu u Google. Tyto kopie se nevyužívají k běžnému poskytování Služby a zůstávají chráněny. Při nezbytné obnově zálohy se již provedené výmazy znovu uplatní před běžným použitím. Anonymizace namísto výmazu se provede jen na doložený pokyn Správce; pseudonymizace není výmaz.

14.4 Správce může kdykoli prostřednictvím oprávněné osoby požádat ve Službě nebo písemně o trvalý výmaz vymezených nebo všech svých údajů. Zpracovatel přiměřeně ověří oprávnění a rozsah; požadavek na výmaz uživatelského účtu sám neopravňuje k výmazu dat celé společnosti. Platný pokyn k dřívějšímu výmazu ukončuje v příslušném rozsahu Období pro export a Zpracovatel provede výmaz bez zbytečného odkladu podle článku 14.3, bez povinné další čekací doby. Správce předem zajistí potřebné kopie. Zpracovatel potvrdí dokončení výmazu z aktivních systémů a uvede případné zbývající kategorie záložních kopií a dobu jejich zániku.

14.5 Výmaz se nevztahuje na údaje, jejichž uchování vyžaduje právo EU nebo členského státu, ani na minimální údaje zákonně zpracovávané Zpracovatelem jako samostatným správcem podle článku 2.3. Běžné bezpečnostní a diagnostické záznamy se uchovávají nejdéle 90 dní od události. Provozní historie reportingu Správce (importy, změny mapování, zápisy, změny uživatelů a oprávnění, včetně úkonů pracovníků Zpracovatele podle článku 3.2) je součástí dat Správce, uchovává se s nimi a při výmazu klientských dat se odstraní, není-li doložen samostatný zákonný důvod. Minimální důkazy o smlouvě, oprávnění, pokynech a provedení výmazu lze uchovat po dobu nezbytnou k ochraně právních nároků, zpravidla nejdéle 3 roky po skončení smlouvy; konkrétní spor, zákonná povinnost nebo doložená delší použitelná lhůta může odůvodnit pouze nezbytné delší uchování. Záznamy o konkrétním incidentu se oddělí a uchovají jen po dobu potřebnou k jeho vyřešení a souvisejícím povinnostem či nárokům. Tato výjimka neopravňuje k plošnému uchování účetních dat. Přístup a další použití zbylých údajů se omezí na příslušný účel.

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. Při bezúplatném užívání Služby, včetně užívání podle Podmínek beta testování, je odpovědnost omezena částkou 25 000 Kč. Při beta testování se použije shodný limit podle článku 7.2 Podmínek beta testování; nejde o dva oddělené limity. 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. To zahrnuje ochranu slabší strany podle § 2898 občanského zákoníku a kogentní právo na vypořádání podle čl. 82 odst. 5 GDPR; částky plněné z těchto neomezitelných titulů nesnižují limit pro ostatní nároky.

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. Přijímající osoby výslovně potvrdí také

ujednání o odpovědnosti v článku 15 a v Hlavní smlouvě. Pro každou společnost je přijetí dokončeno zaznamenáním všech projevů vůle potřebných k jejímu zastoupení; při společném jednání zůstává první přijetí neúplné, dokud další potřebné osoby nepřijmou totožné znění a seznam společností.

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 dostupné ve Službě po dobu jeho přístupu; následně lze kopii vyžádat po dobu oprávněného uchování podle článku 14.5.

16.6 Přijímající osoba uvede a na žádost doloží oprávnění za každou společnost; Zpracovatel může požadovat plnou moc nebo podpis podle článku 16.1 písm. b). Plná moc musí být udělena příslušnou společností zastoupenou předepsaným způsobem a pokrývat dotčené jednání. Při zjištění nedostatku oprávnění Zpracovatel omezí zpracování na nezbytné zabezpečení a vyřešení situace. Dodatečné schválení podle § 440 občanského zákoníku musí být učiněno bez zbytečného odkladu osobou nebo osobami oprávněnými společnost zastoupit a určit schvalované jednání a znění. Mlčení není schválením. Ratifikace se odlišuje od dokončení společného přijetí podle článku 16.2. Není-li oprávnění doloženo ani jednání řádně schváleno, Zpracovatel neumožní další provozní zpracování a zajistí zákonné vrácení nebo výmaz již předaných údajů.

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. Nový účel nebo podstatné rozšíření pokynů vyžaduje předchozí výslovný doložený pokyn Správce; samotné mlčení nepostačuje. Změny Dalších zpracovatelů a předání se řídí také články 7 a 8. Neodmítne-li Správce změnu písemně před její účinností a nevyžaduje-li se nové přijetí, platí, že ji přijal. Přechodné období nelze zkrátit výpovědí Hlavní smlouvy pouze z důvodu odmítnutí změny; právo Správce ukončit bezúplatnou beta službu dříve zůstává zachováno.

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@cfopanorama.com>.

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 — doplní se při přijetí — dne — doplní se při přijetí — / In — doplní se při přijetí — on — doplní se při přijetí —

_____
— doplní se při přijetí —, — doplní se při přijetí —

Za Zpracovatele: Hospitality CEE, s.r.o.
V Praze dne _____

_____
Anna Dempsey, jednatelka

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. Zahrnuje také nastavení klientského reportingu, kontrolu a opravu importů a mapování, zadávání reportovacích zápisů a správu uživatelů v rozsahu pokynů podle článku 3.2.

Účel zpracování: Sestavování manažerských reportů Správce (výkaz zisku a ztráty, rozvaha, cash flow, konsolidace, KPI); nezbytné zavedení, provoz, údržba a zabezpečení Služby, diagnostika importů a technických obtíží, podpora a správa přístupů v rozsahu článku 3.2.

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. Nezbytné bezpečnostní a diagnostické záznamy se zpracovávají a uchovávají podle článků 2.3 a 14.5 a Přílohy B; tyto kategorie nezakládají povinnost vést dlouhodobou historii každé aktivity.

Zvláštní kategorie údajů: Nejsou zamýšleny. Případné výjimky, údaje podle čl. 10 GDPR a rodná čísla vyžadují předchozí písemnou dohodu podle článku 4.2, popis v části 2 a použitelná doplňková opatření; pouhé vyplnění formuláře výjimku nepovoluje.

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: — doplní se při přijetí —
- Společnosti, jejichž data se nahrávají (pro každou: obchodní firma, IČO, sídlo, role správce /

zpracovatele, přímá smluvní strana / zastoupení podle článku 2.2):

— doplní se při přijetí —

- Oprávnění pro každou společnost: přijímající osoba či osoby, funkce, způsob jednání, případná plná moc; při řetězci zpracovatelů potvrzení pověření od příslušného správce (článek 2.2):

— doplní se při přijetí —

- Zdrojové systémy (POHODA / Money S3 / jiný) a případný propojený zdroj dat: — doplní se při přijetí —
- Data od (období): — doplní se při přijetí —
- Mzdy zaúčtované jednotlivě? (ano / ne): — doplní se při přijetí —
- Provozní statistiky z PMS? (ano / ne): — doplní se při přijetí —
- Mohou data obsahovat zvláštní kategorie, údaje podle čl. 10 GDPR nebo rodná čísla? (ne / ano – přesný rozsah, právní titul, dohodnutá opatření a předchozí písemné schválení podle článku 4.2): — doplní se při přijetí —
- Poskytovatel zdravotních služeb, zdravotní pojišťovna nebo obdobný subjekt? (ne / ano – použije se Příloha D): — doplní se při přijetí —
- Kontaktní osoba pro ochranu osobních údajů (jméno, e-mail, telefon): — doplní se při přijetí —
- Pověřenec pro ochranu osobních údajů, je-li jmenován: — doplní se při přijetí —
- E-mail pro bezpečnostní oznámení (článek 11): — doplní se při přijetí —
- Osoba oprávněná udílet provozní pokyny a jejich rozsah podle článku 3.2: — doplní se při přijetí —

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 nebo pracovník Zpracovatele v mezích pokynů podle článku 3.2.
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

Pověření pracovníci Zpracovatele, vázaní mlčenlivostí, mohou v nezbytném rozsahu přistupovat k datům a provádět úkony podle stálých a dalších doložených pokynů v článku 3.2, včetně zavedení, diagnostiky importů, podpory a provozu reportingu. Zvláštní požadavek podpory ani samostatný souhlas ke každému vstupu se nevyžaduje.
Superuživatel Zpracovatele může vstoupit do každé klientské skupiny s plnými právy administrátora, včetně nahrávání, mapování, reportovacích zápisů a pozvání uživatelů. Tato technická možnost nerozšiřuje účel ani rozsah pokynů; obchodní a účetní rozhodnutí zůstávají Správci. Tento režim vyžaduje opětovné ověření druhým faktorem nejméně každých 12 hodin. Nezbytné záznamy přístupů a úkonů jsou dostupné Správci v Nastavení → Protokol přístupu platformy po dobu jejich uchování podle oddílu 5 a článku 14.5.
Přístup k infrastruktuře je omezen na nezbytné osoby a servisní účty s přiměřenými oprávněními; nasazení využívá Workload Identity Federation bez dlouhodobých klíčů. Dočasné pracovní kopie se vytvářejí jen v nezbytném rozsahu na zařízeních se šifrovaným diskem, zámkem obrazovky a aktualizovaným softwarem a mažou se po odpadnutí potřeby.
Data Správce se nevkládají do obecných nástrojů umělé inteligence ani do neschválených služeb. Obecné nástroje AI pracovníci používají pouze s fiktivními nebo demonstračními daty. Budoucí klientská funkce AI podléhá článku 7.5.

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. Přiměřené bezpečnostní a diagnostické záznamy zachycují přihlášení, vstupy pracovníků Zpracovatele do klientských skupin, omezení pokusů a chyby potřebné k zabezpečení a diagnostice. Nevedeme samostatnou dlouhodobou historii běžných zobrazení stránek. Tyto záznamy obsahují jen nezbytné identifikátory, čas, druh úkonu a výsledek, nikoli běžně celý obsah dokladů; uchovávají se nejdéle 90 dní od události, s úzce vymezenými výjimkami podle článku 14.5. Provozní historie reportingu (importy, změny mapování, zápisy, změny rolí a oprávnění, včetně úkonů pracovníků Zpracovatele) není bezpečnostním záznamem: je součástí dat Správce, je mu dostupná ve Službě a uchovává se a maže s jeho daty podle článku 14.
Uživatelský účet lze vymazat i při předchozí aktivitě. Případné zbývající záznamy používají omezený interní identifikátor, například „smazaný uživatel #id“; jde o pseudonymizaci, nikoli automaticky anonymizaci. Záznamy se dále mažou podle příslušné lhůty nebo platného pokynu, není-li doložen samostatný důvod uchování. Důkazy o přijetí smlouvy se řídí článkem 14.5 a netvoří obecnou historii užívání.
Změny kódu procházejí revizí, automatickými testy a testovacím prostředím.

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.
Výmaz na pokyn Správce se řídí článkem 14; při obnově se již provedené výmazy znovu uplatní před běžným použitím. Zbytkové kopie v infrastruktuře dodavatele podléhají cyklu uvedenému v článku 14.3.

7. Umístění dat

Databáze, soubory a zálohy Služby jsou uloženy v EHP (europe-west3, Frankfurt). Globální síť, diagnostika a podpora dodavatelů mohou zahrnovat zpracování nebo vzdálený přístup mimo EHP; použijí se článek 8 a Příloha C. Uložení v EU samo nevylučuje předání.

8. Organizační opatření

Postup řešení bezpečnostních incidentů včetně ohlášení Správci bez zbytečného odkladu, nejpozději do 48 hodin od zjištění (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

Verze seznamu 1.2 ze dne 27. října 2026; účinnost ode dne uvedeného při zveřejnění na https://cfopanorama.com/legal/sub-processors a v oznámení podle článku 7.2. Tento seznam tvoří Přílohu C použitelného DPA. Aktuální seznam: https://cfopanorama.com/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	Google Cloud Data Processing Addendum; DPF pouze při platné certifikaci příslušného příjemce pokrývající předání; jinak použitelné sjednané SCC a potřebná doplňková opatření podle článku 8.

Další zpracovatel	Činnost	Údaje	Místo zpracování	Záruky pro předání
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	Resend DPA; DPF pouze při platné certifikaci příslušného příjemce pokrývající předání; jinak použitelné sjednané SCC a potřebná doplňková opatření podle článku 8.
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; DPF pouze při platné certifikaci příslušného příjemce pokrývající předání; jinak použitelné sjednané SCC a potřebná doplňková opatření podle článku 8.

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

Žádná klientská funkce umělé inteligence nyní není aktivní. Případná budoucí funkce může využívat modely včetně Anthropic Claude prostřednictvím Google Vertex AI s koncovým bodem v EU. Před jejím zapnutím Zpracovatel oznámí konkrétní poskytovatele, tok a rozsah dat, místo zpracování, dobu uchování a záruky předání a získá výslovný doložený pokyn Správce podle článku 7.5. Samotný koncový bod v EU nezaručuje zpracování výhradně v EU. Data Správce nebudou použita k trénování modelů. Obecné AI nástroje pracovníci používají jen s fiktivními nebo demonstračními daty.

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

Použitelné podmínky a omezení dodavatelů: Google Cloud oznamuje incidenty bez zbytečného odkladu a audit dokládá přednostně zprávami; Zpracovatel tím není zbaven povinností podle článků 11 a 12. Automatické zálohy databáze Služby se uchovávají 7 dní. Zbytkové kopie Google mohou být fyzicky odstraněny ve standardním cyklu až do 180 dní od zahájení příslušného výmazu u Google. Resend zpracovává údaje také v USA; region odesílání EU musí být skutečně nastaven. Microsoft EU Data Boundary obsahuje výjimky včetně určitých přístupů podpory a bezpečnostního zpracování. Resend oznamuje porušení zabezpečení bez zbytečného odkladu (čl. 8.6 DPA Resend); jeho čl. 8.8 vylučuje oznámení u porušení způsobených jednáním nebo opomenutím zákazníka, standardní smluvní doložky však mají podle čl. 10.1 DPA Resend přednost a Zpracovatel tím není zbaven povinností podle článku 11. Resend oznamuje změny svých subdodavatelů 14 dní předem; vůči Správci platí lhůty článku 7. Konkrétní doby uchování: Resend – obsah zpráv a záznamy o doručení po dobu nastavenou v účtu Zpracovatele u Resend (omezený počet dní), nejpozději však výmaz do 90 dnů od ukončení účtu (DPA Resend, příloha A); Microsoft 365 – odstraněné zprávy lze obnovit 14 dní, poté je Microsoft odstraní ve svém cyklu (nejdéle 30 dní); schránky podpory nejsou v režimu zadržení (hold) ani archivace. Aktivní pracovní kopie podpory se mažou, jakmile nejsou potřebné; minimální korespondence k uzavřenému požadavku nejdéle do 90 dní, s výjimkami článku 14.5.
DPF lze použít jen při platné certifikaci příslušného příjemce pokrývající předání; jinak musí být před předáním sjednány použitelné standardní smluvní doložky a provedeno potřebné posouzení a doplňková opatření podle článku 8. Zpracovatel ověřuje použitelný mechanismus. Uvedení odlišností nezhojuje nesoulad dodavatelské smlouvy s článkem 28 GDPR a neomezuje odpovědnost podle článku 7.6. Změny se řídí článkem 7, nikoli automaticky kratší lhůtou dodavatele.

Příloha D – Doplňková opatření pro zdravotní a obdobné údaje

Použije se jen na zpracování předem písemně dohodnuté podle článku 4.2 a popsané v Příloze A, části 2; sama nepovoluje další kategorie nebo účely.

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. Použití vždy podléhá předchozí písemné dohodě podle článku 4.2.

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 použitelný právní základ podle článku 6 GDPR a výjimku podle článku 9 odst. 2 GDPR, za případné podmínky článku 10 GDPR a českého práva a za informační povinnost. Příslušný titul musí pokrývat zamýšlený reporting; samotné poskytování zdravotní péče jej pro každé další použití nezakládá. Zpracovatel neposkytuje právní posouzení titulů Správce, ale splní povinnost upozornit na protiprávní pokyn podle článku 3.3. Je-li Správce sám zpracovatelem, zajistí odpovídající pověření a řetězec smluv podle článku 2.2.

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“; varování není kontrolou veškerého obsahu; (c) nezbytný přístup pověřených pracovníků, včetně administrátorských úkonů při zavedení, diagnostice a provozu, se řídí stálými pokyny podle článku 3.2 a Přílohou B oddílem 3; samostatný tiket pro každý vstup není nutný, přístupy a významné úkony se zaznamenávají v rozsahu a po dobu podle Přílohy B oddílu 5; (d) data se neukládají trvale na přenosná zařízení a nezbytné dočasné kopie na šifrovaném disku se mažou po odpadnutí potřeby; (e) staging jen s předchozím písemným souhlasem a následným výmazem; (f) AI funkce zůstávají vypnuté do samostatného doloženého pokynu podle článku 7.5 a dokončení posouzení vlivu, je-li podle článku 35 GDPR povinné.

D.6 Posouzení vlivu a součinnost. Správce provede posouzení vlivu, pokud je podle čl. 35 GDPR vyžadováno, zejména při pravděpodobném vysokém riziku; pouhá existence této přílohy je nenahrazuje. Zpracovatel poskytne součinnost podle článku 10, včetně popisu toků dat a použitelných opatření. Samotné posouzení a případnou předchozí konzultaci zajišťuje 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. Oprávnění a případný řetězec zpracovatelů musí být doloženy podle článku 2.2 před zahájením nahrávání a zpracování. Prohlášení jedné společnosti samo nenahrazuje oprávnění nebo 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 1.5 dated 27 October 2026 (supersedes version 1.2 dated 30 September 2026, version 1.3 dated 22 October 2026 and version 1.4 dated 26 October 2026). The effective date is stated on publication at https://cfopanorama.com/legal/ and in the notice under Article 17.2.

Parties

— completed at acceptance —
Company ID (IČO): — completed at acceptance —, registered office at — completed at acceptance —, — completed at acceptance —,
acting through — completed at acceptance —
(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 cfopanorama.com under the trade name “CFO Panorama” (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” is the agreement under which the Processor provides the Service to the Controller. During the free beta phase it is the agreement under the CFO Panorama Beta Terms (“Beta Terms”). Another agreement, in particular for paid service, applies only if validly concluded by the Parties; these terms do not themselves introduce a paid service.

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 whose access to the Service for the Controller has been duly approved, whether through an invitation or approved self-registration. Registration or an administrator role does not itself confer authority to conclude a contract for the Controller.

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 Each direct contracting company and its role are identified in the acceptance record or signed agreement and Annex A, Part 2. Where the Controller uploads other companies' data, it arranges either their valid accession through authorised representatives or evidence that it acts as their processor and that the relevant controller has authorised the Processor's engagement as sub-processor under Article 28 GDPR. The relevant authority and contractual participation must be evidenced before that company's data uploads are enabled. One person may accept for several companies only within their authority for each. A common contact point gives instructions and receives notices only within its mandate; group membership alone does not establish that mandate.

2.3 The Processor acts as an independent controller only for its own separately identified purposes: managing contractual relationships and contacts, complying with its own accounting and tax duties, necessary Service security and establishing, exercising or defending legal claims. It processes only necessary data for those purposes under the privacy notice at https://cfopanorama.com/legal/user-privacy-notice. Accounting content and user and operational records maintained for the Controller's reporting are processed as processor; status is determined by purpose, not merely a database-table label. The same data may serve different purposes, but independent controllership does not authorise blanket retention of client data after deletion. Persons directly under the Processor's authority follow its instructions consistently with the Controller's instructions; independent contractors are assessed for Sub-processor status according to their actual activities.

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 Documented instructions comprise this Agreement and the Main Agreement, actions and settings of authorised Users, and further written instructions, including electronic instructions, from authorised contacts under Annex A. By concluding this Agreement, the Controller gives a standing instruction for necessary access and processing for onboarding, reporting setup and operation, data import, validation and mapping, diagnosis and resolution of problems, support, maintenance, recovery and Service security. This includes technical corrections and data adjustments needed to deliver the agreed reporting; business decisions, substantive accounting choices and grants of new user permissions must remain within the Controller's authorisation. Within that scope, no separate consent or ticket is required for each staff access. Activities outside that scope require further documented instructions.

3.3 The Processor immediately informs the Controller if it considers that an instruction infringes the GDPR or other applicable data-protection law and may suspend execution pending clarification. It does not execute an instruction established to be unlawful merely because the Controller confirms 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 uploads only data needed for management reporting. Without prior written agreement with the Processor on the specific scope and safeguards, it does not intentionally upload special-category personal data under Article 9 GDPR, Article 10 data or Czech birth numbers. Any exception is recorded in Annex A, Part 2; Annex D and any further agreed safeguards apply. Unilateral completion of Annex A alone is insufficient. The Controller ensures the applicable legal basis and other legal conditions; the DPA does not replace them. Detailed payroll, document text and invoices to patients or health insurers may contain sensitive data; the Controller preferably uses aggregated or cleansed exports. The Processor takes appropriate measures to limit unintended imports; an automated warning does not replace the Controller's review or guarantee detection of all such data.

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 Authorised Processor staff may have full administrator access to any client group to the extent necessary to execute Article 3.2 instructions. They may, in particular, upload, validate and map data, make technical corrections, create or amend entries within the Service for the agreed reporting, prepare outputs and administer users within the Controller’s authorisation. Access is not read-only and need not depend on a separate support request. The permission itself does not authorise unrelated use of data. Access is limited to staff who need it and is subject to confidentiality, two-factor authentication and proportionate recording of security-significant activities under Annex B.

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. This acknowledgement does not discharge the Processor’s statutory duties.

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://cfopanorama.com/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 change is urgently necessary for security reasons or because a Sub-processor ceases service, the Processor notifies the reason and safeguards as early as possible, preferably in advance. It preserves the authorisation conditions under Article 28(2) GDPR and a genuine opportunity to object; the objection period is 14 days from notice. If engagement cannot lawfully proceed under the existing authorisation, it obtains specific authorisation before transfer or suspends the affected processing. Article 7.3 applies accordingly.

7.5 Features requiring a new Sub-processor or a new activity by an existing Sub-processor are introduced under Articles 7.2–7.4. AI features are not currently active; they will be enabled for the Controller only

after notice of the specific scope, suppliers, locations, retention and transfers and express activation by an authorised administrator. Activation is a documented client instruction, not a substitute for a legal basis concerning data subjects. The Processor verifies the specific model's terms beforehand; processing for these features will take place in the EU and Controller data will not be used to train 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. Disclosing differences in Annex C does not cure non-compliance with the GDPR. The Processor ensures appropriate contractual coverage and makes available information necessary to identify relevant Sub-processors and verify their safeguards.

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 The Processor verifies the applicable mechanism and scope of transfers, including relevant onward transfers. If a mechanism ceases to be effective, it ensures another valid mechanism before continuing the affected transfers; otherwise it suspends or ends them and informs the Controller. EU storage or endpoint location alone does not establish all processing locations. Information about the safeguards used is available to the Controller on request.

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. Assistance is provided without undue delay so that the Controller can meet applicable statutory deadlines, with scope proportionate to the data and request.

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. A dispute about charges must not delay assistance necessary to meet a statutory deadline.

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 is an outer limit, not permission to delay. The Processor passes on available information without undue delay and supplements it under Article 11.2; it does not await a complete investigation. Different Sub-processor terms do not restrict the Processor's statutory duties or Article 7.6.

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. These restrictions do not apply to the extent they would prevent necessary verification under Article 28 GDPR, in particular on substantiated suspicion of non-compliance or verification of remediation. The parties maintain proportionate protection of confidentiality, security and operations; Sub-processor audits are addressed primarily through available independent reports and follow-up assistance.

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. Charges must not disproportionately obstruct exercise of the statutory audit right.

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 on valid conclusion under Article 16 and lasts for the Main Agreement and subsequent processing necessary under Article 14. Controller data uploads are enabled only after valid contractual participation; a retrospective agreement does not itself cure earlier GDPR non-compliance.

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 for export for 30 days (the “Export Period”), unless it requests earlier deletion through an authorised person. The Controller chooses return followed by deletion, or direct deletion. On a request during the Export Period, the Processor supplies once, free of charge within 10 Business Days, an export of Controller Personal Data in a commonly used machine-readable format, including available source files, mappings, chart of accounts, entries and other client data; it need not recreate records already lawfully deleted.

14.3 After the Export Period ends, the Processor deletes Controller Personal Data from active systems without undue delay and arranges deletion of relevant copies, including exports and Sub-processor copies. Deletion is not merely hiding data in the interface. Automatic Cloud SQL backups expire in their seven-day cycle; residual copies in Google infrastructure may be physically erased only in its standard cycle, under applicable terms up to 180 days from initiation of the relevant deletion at Google. These copies are not used for ordinary Service delivery and remain protected. If a backup must be restored, completed deletions are reapplied before ordinary use. Anonymisation instead of deletion is performed only on the Controller’s documented instruction; pseudonymisation is not deletion.

14.4 The Controller may at any time, through an authorised person, request permanent deletion of specified or all its data in the Service or in writing. The Processor proportionately verifies authority and scope; a request to delete a user account does not itself authorise deletion of the whole company’s data. A valid early-deletion instruction ends the Export Period to the relevant extent and the Processor deletes without undue delay under Article 14.3, without a mandatory additional waiting period. The Controller first obtains any copies it needs. The Processor confirms deletion from active systems and identifies any remaining categories of backup copies and their expiry period.

14.5 Deletion does not extend to data whose retention is required by EU or Member State law or minimal data lawfully processed by the Processor as an independent controller under Article 2.3. Routine security and diagnostic records are retained for no longer than 90 days from the event. The Controller's reporting operational history (imports, mapping changes, entries, user and permission changes, including operations by Processor staff under Article 3.2) forms part of the Controller's data, is retained with it and is removed when client data are deleted unless a separate lawful basis is documented. Minimal evidence of the contract, authority, instructions and completed deletion may be retained as necessary to protect legal claims, normally for no longer than 3 years after the contract ends; a specific dispute, statutory duty or documented longer applicable period may justify only necessary longer retention. Records of a specific incident are segregated and kept only as needed to resolve it and address related duties or claims. This exception does not authorise blanket retention of accounting data. Access and further use of remaining data are restricted to the relevant purpose.

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 free use of the Service, including use under the Beta Terms, liability is limited to CZK 25,000. During beta testing, the same limit applies under Article 7.2 of the Beta Terms; these are not two separate limits. 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. This includes protection of a weaker party under Section 2898 of the Civil Code and the mandatory contribution right under Article 82(5) GDPR; amounts paid under these non-limitable heads do not reduce the limit for other claims.

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. Accepting persons also expressly acknowledge the liability provisions in Article 15 and the Main Agreement. For each company, acceptance is completed when all declarations required for its representation are recorded; where joint action is required, the first acceptance remains incomplete until the other necessary persons accept the identical text and company schedule.

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 applicable Agreement and acceptance record are available in the Service while the Controller has access; subsequently, a copy may be requested during lawful retention under Article 14.5.

16.6 The accepting person identifies and, on request, evidences authority for each company; the Processor may require a power of attorney or signature under Article 16.1(b). A power of attorney must be granted by the relevant company represented in the required manner and cover the act concerned. If insufficient authority is identified, the Processor restricts processing to necessary protection and resolution of the situation. Ratification under Section 440 of the Civil Code must be made without undue delay by the person or persons authorised to represent the company and identify the act and text being approved. Silence is not ratification. Ratification is distinct from completion of joint acceptance under Article 16.2. If authority is neither evidenced nor the act validly ratified, the Processor does not enable further operational processing and arranges lawful return or deletion of data already supplied.

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. A new purpose or material expansion of instructions requires the Controller's prior express documented instruction; silence alone is insufficient. Sub-processor and transfer changes are also governed by Articles 7 and 8. 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. The transition period may not be shortened by terminating the Main Agreement solely because the amendment was rejected; the Controller retains its right to end the free beta service earlier.

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@cfopanorama.com>.

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)

For the Processor: Hospitality CEE, s.r.o.
In Prague on _____

_____
Anna Dempsey, executive director (jednatelka)

For the Controller
In — completed at acceptance — on — completed at acceptance —

_____
— completed at acceptance —, — completed at acceptance —

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. This also includes setting up client reporting, checking and correcting imports and mappings, entering reporting journals and administering users within the instructions under Article 3.2.

Purpose of processing: Preparing the Controller's management reports (profit and loss, balance sheet, cash flow, consolidation, KPIs); necessary onboarding, operation, maintenance and security of the Service, diagnosis of import and technical difficulties, support and access administration within Article 3.2.

Data uploaded: Accounting journal, chart of accounts, cost centres (střediska), activities, jobs/projects/orders 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. Necessary security and diagnostic records are processed and retained under Articles 2.3 and 14.5 and Annex B; these categories do not require a long-term history of every activity.

Special categories of data: Not intended. Any exceptions, Article 10 GDPR data and birth numbers require prior written agreement under Article 4.2, description in Part 2 and applicable supplementary measures; merely completing a form does not authorise an exception.

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: — completed at acceptance —
- Companies whose data are uploaded (for each: legal name, company ID, registered office, controller / processor role, direct contracting party / representation under Article 2.2):

— completed at acceptance —

- Authority for each company: accepting person(s), position, representation rules, any power of attorney; in a processor chain, confirmation of the relevant controller’s authorisation (Article 2.2):

— completed at acceptance —

- Source systems (POHODA / Money S3 / other) and any connected data source: — completed at acceptance —
- Data from (period): — completed at acceptance —
- Payroll booked per person? (yes / no): — completed at acceptance —
- PMS operating statistics? (yes / no): — completed at acceptance —
- May the data contain special categories, Article 10 GDPR data or birth numbers? (no / yes – exact scope, legal basis, agreed measures and prior written approval under Article 4.2): — completed at acceptance —
- Healthcare provider, health insurer or similar? (no / yes – Annex D applies): — completed at acceptance —
- Data protection contact (name, email, phone): — completed at acceptance —
- Data protection officer, if appointed: — completed at acceptance —
- Email for security notices (Article 11): — completed at acceptance —
- Person authorised to give operational instructions and their scope under Article 3.2: — completed at acceptance —

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 or Processor staff within the instructions under Article 3.2.
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

Authorised Processor staff, bound by confidentiality, may access data and perform operations as necessary under the standing and further documented instructions in Article 3.2, including onboarding, import diagnostics, support and reporting operations. No separate support request or consent for every access is required.
The Processor’s superuser can enter every client group with full administrator rights, including uploads, mapping, reporting journals and user invitations. This technical capability does not expand the purpose or scope of instructions; business and accounting decisions remain with the Controller. This mode requires renewed second-factor verification at least every 12 hours. Necessary access and operation records are available to the Controller under Settings → Platform access log for the retention period in section 5 and Article 14.5.
Infrastructure access is limited to necessary persons and service accounts with appropriate permissions; deployment uses Workload Identity Federation without long-lived keys. Temporary working copies are made only as necessary on devices with disk encryption, screen lock and current software and are deleted when no longer needed.
Controller data are not entered into general-purpose AI tools or unapproved services. Staff use general-purpose AI tools only with fictitious or demo data. Any future client AI feature is subject to Article 7.5.

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. Proportionate security and diagnostic records capture sign-ins, Processor staff entries into client groups, rate limiting and errors needed for security and diagnostics. We do not maintain a separate long-term history of routine page views. These records contain only necessary identifiers, time, operation type and result, not routinely full document contents; they are retained for no more than 90 days from the event, subject to the narrow exceptions in Article 14.5. The reporting operational history (imports, mapping changes, entries, role and permission changes, including operations by Processor staff) is not a security record: it forms part of the Controller's data, is available to the Controller in the Service and is retained and deleted with its data under Article 14.
A user account can be deleted despite prior activity. Any remaining records use a restricted internal identifier, such as “deleted user #id”; this is pseudonymisation, not automatically anonymisation. Records are subsequently deleted under the applicable period or valid instruction unless a separate retention basis is documented. Contract-acceptance evidence is governed by Article 14.5 and is not a general usage history.
Code changes undergo review, automated tests and a test environment.

6. Availability and recovery

Managed Google Cloud infrastructure in region europe-west3; automatic 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.
Deletion on the Controller’s instruction is governed by Article 14; on restoration, completed deletions are reapplied before ordinary use. Residual supplier infrastructure copies follow the cycle in Article 14.3.

7. Data location

Service databases, files and backups are stored in the EEA (europe-west3, Frankfurt). Suppliers’ global networks, diagnostics and support may involve processing or remote access outside the EEA; Article 8 and Annex C apply. EU storage alone does not exclude a transfer.

8. Organisational measures

Incident response procedure including notification to the Controller without undue delay and within 48 hours of awareness (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

List version 1.2 dated 27 October 2026; effective from the date stated on publication at https://cfopanorama.com/legal/sub-processors and in the notice under Article 7.2. This list forms Annex C to the applicable DPA. Current list: https://cfopanorama.com/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	Google Cloud Data Processing Addendum; DPF only with valid recipient certification covering the transfer; otherwise applicable agreed SCCs and necessary supplementary measures under Article 8.
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	Resend DPA; DPF only with valid recipient certification covering the transfer; otherwise applicable agreed SCCs and necessary supplementary measures under Article 8.
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; DPF only with valid recipient certification covering the transfer; otherwise applicable agreed SCCs and necessary supplementary measures under Article 8.

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

No client AI feature is currently active. A future feature may use models including Anthropic Claude through Google Vertex AI with an EU endpoint. Before activation, the Processor will notify the specific providers, data flow and scope, processing location, retention and transfer safeguards and obtain the Controller's express documented instruction under Article 7.5. An EU endpoint alone does not guarantee EU-only processing. Controller data will not be used to train models. Staff use general-purpose AI tools only with fictitious or demo data.

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

Applicable supplier terms and limitations: Google Cloud notifies incidents without undue delay and primarily supports audits through reports; this does not release the Processor from Articles 11 and 12. Automatic Service database backups are retained for 7 days. Residual Google copies may be physically erased in the standard cycle up to 180 days from initiation of the relevant deletion at Google. Resend also processes data in the USA; EU sending must actually be configured. Microsoft's EU Data Boundary has exceptions, including certain support access and security processing. Resend notifies personal data

breaches without undue delay (Resend DPA clause 8.6); its clause 8.8 excludes notification for breaches resulting from the customer's acts or omissions, but the standard contractual clauses prevail under Resend DPA clause 10.1 and the Processor is not released from Article 11. Resend gives 14 days' notice of changes to its own sub-processors; towards the Controller the periods of Article 7 apply.
Specific retention periods: Resend – message content and delivery records for the period configured in the Processor's Resend account (a limited number of days) and in any event deleted no later than 90 days after termination of the account (Resend DPA, Exhibit A); Microsoft 365 – deleted messages are recoverable for 14 days and are then removed by Microsoft within its cycle (at most 30 days); the support mailboxes are not under hold or archiving. Active support working copies are deleted when no longer needed; minimal correspondence about a closed request within 90 days at the latest, subject to Article 14.5 exceptions.
DPF may be used only where the relevant recipient has valid certification covering the transfer; otherwise applicable standard contractual clauses must be in place before transfer, with necessary assessment and supplementary measures under Article 8. The Processor verifies the applicable mechanism. Disclosing differences does not cure a supplier contract’s failure to comply with Article 28 GDPR or restrict liability under Article 7.6. Changes follow Article 7, not automatically a supplier’s shorter period.

Annex D – Supplementary measures for health and similar data

Applies only to processing agreed in writing in advance under Article 4.2 and described in Annex A, Part 2; it does not itself authorise further categories or purposes.

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. Application always requires prior written agreement under Article 4.2.

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 an applicable Article 6 GDPR basis and Article 9(2) exception, any Article 10 GDPR and Czech-law conditions, and transparency duties. The basis must cover the intended reporting; providing healthcare does not itself establish a basis for every further use. The Processor does not provide a legal assessment of the Controller’s bases but complies with its duty to flag unlawful instructions under Article 3.3. Where the Controller is itself a processor, it ensures appropriate authorisation and a contractual chain under Article 2.2.

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 warns if a column header matches a birth number or the word “diagnosis”; the warning is not a check of all content; (c) necessary access by authorised staff, including administrator operations for onboarding, diagnostics and operation, follows the standing instructions under Article 3.2 and Annex B section 3; a separate ticket for every access is unnecessary, and access and material operations are logged to the extent and for the period in Annex B section 5; (d) data are not permanently stored on portable devices and necessary temporary copies on encrypted disks are deleted when no longer needed; (e) staging only with prior written consent and subsequent deletion; (f) AI features stay off until a separate documented instruction under Article 7.5 and completion of an impact assessment where Article 35 GDPR requires one.

D.6 Impact assessment and assistance. The Controller carries out an impact assessment where Article 35 GDPR requires it, in particular where high risk is likely; this annex does not replace that assessment. The Processor assists under Article 10, including a description of data flows and applicable measures. The Controller carries out the assessment and any required prior consultation.

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. Authority and any processor chain must be established under Article 2.2 before uploads and processing begin. One company’s declaration does not itself replace the others’ authority or instructions.

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.