Ochrana osobních údajů v CFO Panorama – stručně

Kdo je kdo: Vaše společnost je zpravidla správcem; Hospitality CEE, s.r.o. je zpracovatelem klientských dat podle DPA. Případný řetězec zpracovatelů musí odpovídat článku 2.2. Přijaté DPA obsahuje stálý pokyn k nezbytnému zavedení, importům, mapování, diagnostice, podpoře a provozu reportingu. Pro každý takový vstup pracovníka není potřeba samostatný tiket nebo souhlas. Pro omezené vlastní účely, například bezpečnost platformy a důkaz o smlouvě, jsme samostatným správcem podle zásad pro uživatele.

Jaké údaje: Účetní exporty, účtový rozvrh, střediska, činnosti, zakázky, rozpočty a případně statistiky PMS. Mohou obsahovat osobní údaje dodavatelů, zaměstnanců a hostů; jejich rozsah není automaticky zanedbatelný. Minimalizujte údaje a přednostně používejte souhrny. Zvláštní kategorie, údaje podle článku 10 GDPR a rodná čísla nenahrávejte bez předchozí písemné dohody podle článku 4.2 a odpovídajících opatření.

Kde jsou data: Databáze, soubory a zálohy Služby jsou v Google Cloud ve Frankfurtu. Resend zpracovává transakční e-maily také v USA; Microsoft 365 slouží pro podporu. Zahraniční podpora a globální infrastruktura mohou znamenat předání mimo EHP. Použitelné mechanismy a poskytovatele uvádí článek 8 a Příloha C; samotný region EU nestačí. Seznam: https://reporting.finance/legal/sub-processors.

Zabezpečení a přístup: Oddělení klientů, role, povinné 2FA pro administrátory, editory a pracovníky, šifrování a sedmidenní databázové zálohy. Superuživatel poskytovatele má plná administrátorská oprávnění ve všech skupinách pro činnosti podle pokynů, včetně importů a nastavení reportingu; nejméně každých 12 hodin obnovuje druhý faktor. Nezbytné záznamy přístupů a významných úkonů jsou viditelné v Nastavení → Protokol přístupu platformy. Běžné bezpečnostní a diagnostické záznamy se uchovávají nejdéle 90 dní; provozní historie vašeho reportingu (importy, mapování, zápisy, změny uživatelů) je součástí vašich dat a maže se s nimi; samostatná dlouhodobá historie běžných zobrazení stránek se nevede. Výjimky pro konkrétní incidenty, povinnosti a právní nároky jsou úzké a doložené.

Incident: Porušení zabezpečení vám oznámíme bez zbytečného odkladu, nejpozději do 48 hodin od chvíle, kdy se o něm dozvíme (včetně zprávy od subdodavatele).

Subdodavatelé a AI: Změny oznamujeme podle článku 7 DPA, zpravidla 30 dní předem; pro změny subdodavatelů dodavatele a naléhavé situace platí zvláštní postup článků 7.2 a 7.4; právo na námitku a řešení zůstává zachováno. Žádná klientská AI funkce není aktivní. Budoucí funkce přes Vertex AI s koncovým bodem v EU vyžaduje předchozí oznámení konkrétního zpracování a váš výslovný doložený pokyn; data se nepoužijí k trénování modelů.

Výmaz a konec spolupráce: Standardně máte 30 dní přístup pouze pro čtení k exportu. Oprávněná osoba může kdykoli požádat o dřívější výmaz vymezených nebo všech klientských dat; na konec exportní lhůty se pak nečeká. Výmaz z aktivních systémů se provádí bez zbytečného odkladu, nejen skrytím dat. Zálohy databáze zanikají v sedmidenním cyklu a zbytkové kopie Google v jeho cyklu až do 180 dní od zahájení příslušného výmazu. Pouze úzce odůvodněné zákonné údaje a minimální důkazy právních nároků mohou zůstat podle článku 14.5. Výmaz uživatelského účtu sám nevymazává data celé společnosti; označení „smazaný uživatel #id“ není automaticky anonymizace.

Co potřebujeme od vás: Uveďte každou společnost a doložte oprávnění podle DPA. Při společném jednání přijmou stejné znění a seznam společností všechny potřebné osoby; alternativou je řádná plná moc nebo podepsaná listina. Samotné členství ve skupině oprávnění nedává. Do dokončení přijetí a potřebného pověření nelze data nahrávat. Vyplňte Přílohu A, spravujte uživatele, minimalizujte data a uchovávejte vlastní účetní originály. Zásady pro uživatele: https://reporting.finance/legal/user-privacy-notice. Kontakt: privacy@reporting.finance.

Toto shrnutí (verze 1.4 ze dne 26. října 2026) je pouze orientační a není součástí smlouvy. Rozhoduje použitelné DPA verze 1.4. Česká verze má přednost.

Data protection at CFO Panorama – in brief

Who is who: Your company is normally the controller; Hospitality CEE, s.r.o. is the processor of client data under the DPA. Any processor chain must satisfy Article 2.2. The accepted DPA contains standing instructions for necessary onboarding, imports, mapping, diagnostics, support and reporting operations. Each such staff access does not require a separate ticket or consent. For limited purposes of our own, such as platform security and contract evidence, we are an independent controller under the user notice.

What data: Accounting exports, chart of accounts, cost centres, activities, jobs/projects/orders, budgets and possibly PMS statistics. These may contain suppliers', employees' and guests' personal data; their scope is not automatically insignificant. Minimise data and prefer aggregates. Do not upload special categories, Article 10 GDPR data or birth numbers without prior written agreement under Article 4.2 and appropriate measures.

Where data are: Service databases, files and backups are in Google Cloud in Frankfurt. Resend also processes transactional emails in the USA; Microsoft 365 is used for support. Overseas support and global infrastructure may involve transfers outside the EEA. Article 8 and Annex C set out the applicable mechanisms and providers; an EU region alone is insufficient. List: https://reporting.finance/legal/sub-processors.

Security and access: Client separation, roles, mandatory 2FA for admins, editors and staff, encryption and seven-day database backups. The provider's superuser has full administrator rights in every group for instructed activities, including imports and reporting setup; second-factor verification is renewed at least every 12 hours. Necessary access and material-operation records are visible under Settings → Platform access log. Routine security and diagnostic records are kept for no more than 90 days; the operational history of your reporting (imports, mapping, entries, user changes) is part of your data and is deleted with it; no separate long-term history of routine page views is maintained. Exceptions for specific incidents, duties and legal claims are narrow and documented.

Incidents: We notify you of a personal data breach without undue delay and within 48 hours of becoming aware (including notice from a sub-processor).

Sub-processors and AI: Changes are notified under DPA Article 7, normally 30 days in advance; changes to a supplier's own sub-processors and urgent situations follow the special procedure in Articles 7.2 and 7.4; the right to object and obtain a resolution remains. No client AI feature is active. A future feature through Vertex AI with an EU endpoint requires prior notice of the specific processing and your express documented instruction; data will not be used to train models.

Deletion and termination: You normally have 30 days' read-only export access. An authorised person may request earlier deletion of specified or all client data at any time; the export period then need not expire first. Active-system deletion occurs without undue delay and is more than hiding data. Database backups expire in a seven-day cycle and residual Google copies in its cycle up to 180 days from initiation of the relevant deletion. Only narrowly justified statutory data and minimal legal-claims evidence may remain under Article 14.5. Deleting a user account does not itself delete the whole company's data; "deleted user #id" is not automatically anonymisation.

What we need from you: Identify every company and establish authority under the DPA. Where joint representation is required, all necessary persons accept the same text and company schedule; alternatives are a valid power of attorney or signed document. Group membership alone gives no authority. Uploads are blocked until acceptance and necessary authorisation are complete. Complete Annex A, manage users, minimise data and retain your own original accounting records. User notice: https://reporting.finance/legal/user-privacy-notice. Contact: privacy@reporting.finance.

This summary (version 1.4 dated 26 October 2026) is guidance only and not part of the contract. The applicable DPA, version 1.4, governs. The Czech version prevails.