Zásady ochrany osobních údajů uživatelů

CFO Panorama · Hospitality CEE, s.r.o. · verze 1.2 ze dne 27. října 2026 (nahrazuje verzi 1.0 ze dne 30. září 2026 a verzi 1.1 ze dne 26. října 2026)

Tyto zásady včetně informací podle článků 13 a 14 GDPR vysvětlují, jak společnost Hospitality CEE zpracovává osobní údaje fyzických osob, které mají uživatelský účet ve službě CFO Panorama (app.cfopanorama.com), a osob, jejichž jméno a e-mail se objeví v pozvánkách, při obnově hesla nebo ve zprávách o přijetí smlouvy. Liší-li se jazykové verze, má přednost česká. Tyto zásady se týkají zpracování, při kterém je Hospitality CEE samostatným správcem (článek 2.3 smlouvy o zpracování osobních údajů). Účetní obsah a data z PMS, která nahraje klient, zpracováváme jako zpracovatel pro tohoto klienta; dotazy k tomuto obsahu směřujte na klienta.

1. Správce

Hospitality CEE, s.r.o., IČO 19489617, sídlo Kaprova 42/14, Staré Město, 110 00 Praha 1, zapsaná u Městského soudu v Praze, oddíl C, vložka 387413. Statutární orgán: Anna Dempsey, jednatelka. Kontakt: <privacy@cfopanorama.com>. Pověřenec pro ochranu osobních údajů není jmenován.

2. Kdo je subjekt údajů

Uživatelé Služby (administrátor, editor, prohlížející), osoby pozvané k účtu a osoby, které jménem klienta přijímají Smlouvu o zpracování osobních údajů nebo Hlavní smlouvu. Zaměstnavatel nebo klient, který vám účet zřídil, je samostatným správcem svého rozhodnutí dát vám přístup. Patří sem také žadatelé o účet, jehož aktivaci schvalují pracovníci poskytovatele.

3. Účely a právní základy

Uzavření, správa a prokázání smlouvy s klientem, ověření oprávnění zástupců, schválení registrace, správa uživatelských účtů, podpora a nezbytné transakční zprávy: u zástupců a uživatelů firemního klienta čl. 6 odst. 1 písm. f) GDPR – oprávněný zájem na poskytování a správě Služby a ochraně právních nároků; je-li smluvní stranou přímo podnikající fyzická osoba, pro nezbytné uzavření a plnění její smlouvy čl. 6 odst. 1 písm. b). Zabezpečení platformy a diagnostika, včetně přihlášení, 2FA, omezení pokusů, přiměřených bezpečnostních záznamů a odhalení zneužití: čl. 6 odst. 1 písm. f) – ochrana platformy a klientských dat. Uplatnění a obhajoba právních nároků: čl. 6 odst. 1 písm. f). Údaje povinně vedené v účetních a daňových dokladech: čl. 6 odst. 1 písm. c), podle použitelných účetních a daňových předpisů; běžné obchodní kontakty mimo tyto povinnosti: čl. 6 odst. 1 písm. f). Neprovádíme rozhodování založené výhradně na automatizovaném zpracování, včetně profilování, s právními nebo obdobně významnými účinky podle článku 22 GDPR.

4. Kategorie údajů

Jméno, e-mail, funkce, organizace, role, jazyk a identifikátor účtu; údaje potřebné pro registraci, ověření oprávnění a komunikaci s podporou; čas a výsledek přihlášení, IP adresa, identifikace prohlížeče a stav dvoufázového ověření; minimální bezpečnostní a diagnostické záznamy přístupů a významných úkonů; obsah transakčních zpráv a doručenky; záznamy o přijetí smluv, jejich verzi a hashi a o oprávnění přijímajících osob. Klientská provozní historie se zpracovává pro klienta podle DPA; jako samostatný správce z ní používáme pouze nezbytné údaje pro účely v bodě 3. Hesla ukládáme jako solené hashe a tajné klíče TOTP šifrovaně. Pro uživatelský účet nežádáme rodné číslo ani zvláštní kategorie údajů.

5. Účetní a PMS data klienta

Obsah, který klient nahraje (deník, doklady, mzdy, statistiky hotelu, jména dodavatelů nebo hostů), zpracováváme jako zpracovatel podle DPA. K těmto údajům se zásady v bodech 3–4 nevztahují jako k našemu správcovskému zpracování. Žádost o přístup, opravu nebo výmaz takového obsahu směřujte na klienta (vašeho zaměstnavatele nebo objednatele). My mu poskytneme součinnost funkcemi Služby. Žádost doručenou nám předáme příslušnému klientovi a poskytneme zákonnou součinnost; sami nerozhodujeme o výmazu účetních dat celé společnosti na žádost jednotlivého uživatele. Naši pověření pracovníci mohou podle DPA přistupovat k datům také při nezbytném zavedení, diagnostice importů a provozu reportingu.

6. Příjemci

Google Cloud EMEA Limited a přidružené společnosti (infrastruktura, region europe-west3 Frankfurt). Plus Five Five, Inc. – Resend (transakční e-maily; odesílání může jít z EU, správa účtu a záznamy v USA).

Microsoft Ireland Operations Limited (schránka podpory Microsoft 365, pokud nám napíšete). Naši zaměstnanci s potřebou přístupu, vázaní mlčenlivostí. Dozorové orgány, kde to ukládá právo. V nezbytném rozsahu také profesionální poradci vázaní mlčenlivostí a soudy při ochraně právních nároků. Aktuální poskytovatelé technických služeb jsou uvedeni na https://cfopanorama.com/legal/sub-processors.

7. Předání mimo EHP

Databáze, soubory a zálohy Služby jsou uloženy ve Frankfurtu. Resend zpracovává údaje také v USA; Google a Microsoft mohou v rámci podpory, globální infrastruktury nebo výjimek ze svých regionálních závazků zpracovávat údaje či k nim přistupovat mimo EHP. Pro příjemce s platnou certifikací DPF pokrývající předání se použije rozhodnutí Komise (EU) 2023/1795. V ostatních případech použijeme před předáním odpovídající záruky, zejména sjednané standardní smluvní doložky podle rozhodnutí (EU) 2021/914 a potřebné posouzení a doplňková opatření. Kopii použitelných záruk nebo informaci o nich si můžete vyžádat na privacy@cfopanorama.com; důvěrné údaje jiných osob mohou být přiměřeně zakryty. Podrobnosti o příjemcích a místech jsou v aktuálním seznamu poskytovatelů.

8. Doba uložení

Uživatelský účet uchováváme po dobu oprávněného používání; při jeho výmazu odstraníme profil a přihlašovací prostředky bez zbytečného odkladu, i když uživatel dříve prováděl úkony. Neúspěšnou nebo opuštěnou žádost o účet mažeme do 30 dní od zamítnutí, odvolání nebo posledního kontaktu. Samostatnou dlouhodobou historii běžných zobrazení stránek nevedeme. Nezbytné bezpečnostní a diagnostické záznamy uchováváme nejdéle 90 dní od události. Případné zbývající záznamy po výmazu uživatele zobrazují jen interní označení, např. „smazaný uživatel #id“, a mažou se v příslušné lhůtě. Toto označení je pseudonymizace a může stále představovat osobní údaj. Klientské účetní a provozní záznamy se řídí pokyny klienta a DPA; výmaz uživatelského účtu sám nevymazává účetnictví klienta.
Minimální doklady o smlouvě, oprávnění, pokynech a provedeném výmazu uchováváme po dobu smlouvy a zpravidla nejdéle 3 roky po jejím skončení pro ochranu právních nároků. Konkrétní spor, zákonná povinnost nebo doložená delší použitelná lhůta odůvodní pouze nezbytné delší uchování; pravidelně posuzujeme, zda důvod trvá. Záznamy konkrétního incidentu uchováváme odděleně po dobu nezbytnou k vyřešení a souvisejícím povinnostem nebo nárokům. Výjimky neznamenají plošné uchování klientských účetních dat.
Dočasné pracovní kopie podpory mažeme po odpadnutí potřeby, minimální korespondenci k uzavřenému požadavku do 90 dní, není-li potřebná pro uvedenou konkrétní povinnost nebo nárok. Resend: obsah zpráv a doručenky po dobu nastavenou v našem účtu 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); bez zadržení (hold) a archivace. Povinné účetní a daňové doklady uchováváme po dobu stanovenou právem pro daný typ dokladu. Automatické databázové zálohy zanikají v sedmidenním cyklu; zbytkové kopie Google mohou být odstraněny až do 180 dní od zahájení příslušného výmazu u Google. Zbylé kopie zůstávají chráněny a při obnově se výmazy znovu uplatní.

9. Vaše práva

Máte právo na přístup, opravu, výmaz, omezení, námitku proti zpracování založenému na čl. 6 odst. 1 písm. f) a na přenositelnost tam, kde zpracování probíhá automatizovaně na základě smlouvy. Práva uplatněte na privacy@cfopanorama.com. Můžete podat stížnost u Úřadu pro ochranu osobních údajů (ÚOOÚ), Pplk. Sochora 27, 170 00 Praha 7, uoou.gov.cz. Jste-li v jiném členském státě EU, můžete jít i k tamnímu dozorovému úřadu. Výmaz není absolutní: nezbytné údaje lze ponechat zejména pro splnění právní povinnosti nebo určení, výkon či obhajobu právních nároků podle článku 17 odst. 3 GDPR. Žádost posoudíme a odpovíme bez zbytečného odkladu, zpravidla do jednoho měsíce; zákonné prodloužení oznámíme s důvody. Totožnost ověříme jen v přiměřeném rozsahu.

10. Oprávněný zájem a námitka

Oprávněné zájmy jsou popsány u jednotlivých účelů v bodě 3. Proti zpracování podle čl. 6 odst. 1 písm. f) můžete kdykoli vznést námitku z důvodů týkajících se vaší konkrétní situace. V dotčeném zpracování nebudeme pokračovat, neprokážeme-li závažné oprávněné důvody převažující nad vašimi zájmy, právy a svobodami nebo potřebu určení, výkonu či obhajoby právních nároků. Námitka se neposuzuje jako automatické vzdání se práv nebo obecný souhlas s uchováním.

11. Zdroj údajů

Údaje získáváme od vás (registrace, přihlášení, 2FA), od administrátora klienta, který vás pozve, a automaticky ze zařízení při používání Služby. Údaje o uzavření smlouvy vznikají ve Službě. Poskytnutí jména, e-mailu a nezbytných přihlašovacích a bezpečnostních údajů je podmínkou zřízení a bezpečného používání účtu; bez nich účet nelze zřídit nebo provozovat. Nejde o obecnou zákonnou povinnost mít účet. Údaje nutné k ověření oprávnění jsou podmínkou přijetí za společnost. Nepovinné údaje nemusíte poskytnout. Při získání údajů od klienta vám tyto informace poskytneme nejpozději při prvním kontaktu, jinak v zákonné lhůtě podle článku 14 GDPR.

12. Změny

Aktuální znění je na https://cfopanorama.com/legal/user-privacy-notice. Podstatnou změnu oznámíme e-mailem na účet nebo oznámením ve Službě. O novém účelu zpracování poskytneme potřebné informace předem; změna těchto zásad sama nevytváří právní základ a nevyžaduje od uživatele souhlas, pokud zpracování stojí na jiném právním základě.

User privacy notice

CFO Panorama · Hospitality CEE, s.r.o. · version 1.2 dated 27 October 2026 (supersedes version 1.0 dated 30 September 2026 and version 1.1 dated 26 October 2026)

This notice, including information under Articles 13 and 14 GDPR, explains how Hospitality CEE processes personal data of natural persons who have a user account in CFO Panorama (app.cfopanorama.com), and of persons whose name and email appear on invitations, password resets or contract-acceptance messages. Czech text prevails if the language versions differ. This notice covers processing where Hospitality CEE is an independent controller (DPA Article 2.3). Accounting and PMS content uploaded by a client is processed as a processor for that client; requests about that content go to the client.

1. Controller

Hospitality CEE, s.r.o., company ID 19489617, registered office Kaprova 42/14, Staré Město, 110 00 Prague 1, Czech Republic, registered at the Municipal Court in Prague, section C, file 387413. Statutory body: Anna Dempsey, executive director. Contact: <privacy@cfopanorama.com>. No data protection officer has been appointed.

2. Who this notice is for

Users of the Service (admin, editor, viewer), persons invited to an account, and persons who accept the Data Processing Agreement or the Main Agreement for a client. The employer or client that granted you access is a separate controller of that access decision. This also includes applicants for accounts whose activation is approved by provider staff.

3. Purposes and legal bases

Concluding, administering and evidencing the client contract, checking representatives' authority, approving registrations, managing user accounts, support and necessary transactional messages: for corporate-client representatives and users, Article 6(1)(f) GDPR – legitimate interests in delivering and administering the Service and protecting legal claims; where a sole trader is personally the contracting party, Article 6(1)(b) for steps and performance necessary for that contract. Platform security and diagnostics, including sign-in, 2FA, rate limiting, proportionate security records and abuse detection: Article 6(1)(f) – protecting the platform and client data. Establishing and defending legal claims: Article 6(1)(f). Data required in accounting and tax records: Article 6(1)(c), under applicable accounting and tax laws; ordinary business contacts outside those duties: Article 6(1)(f). We do not make decisions based solely on automated processing, including profiling, with legal or similarly significant effects under Article 22 GDPR.

4. Categories of data

Name, email, position, organisation, role, language and account identifier; data needed for registration, authority checks and support communications; sign-in time and result, IP address, browser identification and two-factor status; minimal security and diagnostic records of access and material operations; transactional-message content and delivery records; contract-acceptance records, versions and hashes and accepting persons' authority. Client operational history is processed for the client under the DPA; as an independent controller we use only data necessary for section 3 purposes. Passwords are salted hashes and TOTP secrets are encrypted. We do not request a birth number or special-category data for a user account.

5. Client accounting and PMS data

Content the client uploads (journal, documents, payroll, hotel statistics, supplier or guest names) is processed by us as processor under the DPA. Sections 3–4 do not treat that content as our controllership. Address access, rectification or erasure requests for that content to the client (your employer or contracting company). We assist the client through the Service. We forward a request received by us to the relevant client and provide legally required assistance; we do not decide to delete an entire company's accounting data on an individual user's request. Our authorised staff may also access data under the DPA for necessary onboarding, import diagnostics and reporting operations.

6. Recipients

Google Cloud EMEA Limited and affiliates (infrastructure, region europe-west3 Frankfurt). Plus Five Five, Inc. – Resend (transactional email; sending may be from the EU, account administration and logs in the

USA). Microsoft Ireland Operations Limited (Microsoft 365 support mailbox if you email us). Our employees who need access, bound by confidentiality. Public authorities where the law requires it. Where necessary, also professional advisers bound by confidentiality and courts for protecting legal claims. Current technical service providers are listed at https://cfopanorama.com/legal/sub-processors.

7. Transfers outside the EEA

Service databases, files and backups are stored in Frankfurt. Resend also processes data in the USA; Google and Microsoft may process or access data outside the EEA through support, global infrastructure or exceptions to regional commitments. For recipients with valid DPF certification covering the transfer, Commission Decision (EU) 2023/1795 applies. Otherwise, before transfer we use appropriate safeguards, in particular agreed standard contractual clauses under Decision (EU) 2021/914 and necessary assessment and supplementary measures. You may request a copy of applicable safeguards or information about them at privacy@cfopanorama.com; others' confidential information may be proportionately redacted. Recipient and location details appear in the current provider list.

8. Retention

We retain a user account while its use is authorised; on deletion, we remove the profile and sign-in credentials without undue delay, even where the user previously performed operations. Unsuccessful or abandoned account applications are deleted within 30 days of rejection, withdrawal or the last contact. We do not keep a separate long-term history of routine page views. Necessary security and diagnostic records are retained for no more than 90 days from the event. Any records remaining after user deletion display only an internal label, such as "deleted user #id", and are deleted within the applicable period. This is pseudonymisation and may still constitute personal data. Client accounting and operational records follow the client's instructions and the DPA; deleting a user account does not itself delete the client's accounts.
We retain minimal evidence of the contract, authority, instructions and completed deletion during the contract and normally for no more than 3 years after it ends to protect legal claims. A specific dispute, legal obligation or documented longer applicable period justifies only necessary longer retention; we regularly assess whether the reason continues. Records of a specific incident are kept separately as necessary for resolution and associated duties or claims. These exceptions do not mean blanket retention of client accounting data.
Temporary support working copies are deleted when no longer needed, and minimal correspondence on a closed request within 90 days unless needed for a specific duty or claim above. Resend: message content and delivery records for the period configured in our 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); no hold or archiving. Mandatory accounting and tax records are kept for the period legally required for their document type. Automatic database backups expire in a seven-day cycle; residual Google copies may be erased up to 180 days from initiation of the relevant deletion at Google. Remaining copies stay protected and deletions are reapplied on restoration.

9. Your rights

You have the rights of access, rectification, erasure, restriction, objection to Article 6(1)(f) processing, and portability where processing is automated and based on contract. Use privacy@cfopanorama.com. You may complain to the Czech Office for Personal Data Protection (ÚOOÚ), Pplk. Sochora 27, 170 00 Prague 7, uoou.gov.cz, or to the supervisory authority in another EU Member State where you live or work. Erasure is not absolute: necessary data may be retained in particular to comply with a legal obligation or establish, exercise or defend legal claims under Article 17(3) GDPR. We assess and respond without undue delay, normally within one month; any statutory extension is notified with reasons. Identity checks are proportionate.

10. Legitimate interests and objection

Legitimate interests are stated for each purpose in section 3. You may object at any time to Article 6(1)(f) processing on grounds relating to your particular situation. We will stop the processing concerned unless we demonstrate compelling legitimate grounds overriding your interests, rights and freedoms or a need to establish, exercise or defend legal claims. An objection is not treated as an automatic waiver of rights or general consent to retention.

11. Source of data

We obtain data from you (registration, sign-in, 2FA), from the client administrator who invites you, and automatically from your device when you use the Service. Contract-conclusion data are generated in the Service. Providing your name, email and necessary authentication and security data is a condition for creating and securely using an account; without them the account cannot be created or operated. There is no general legal duty to have an account. Data necessary to verify authority are a condition for accepting on a company's behalf. Optional data need not be provided. When data come from a client, we provide this information no later than our first contact, otherwise within the statutory Article 14 GDPR

period.

12. Changes

The current text is at https://cfopanorama.com/legal/user-privacy-notice. We will notify a material change by email to the account or by a notice in the Service. We provide required information before processing for a new purpose; changing this notice does not itself create a legal basis and does not require user consent where processing relies on another legal basis.