

# Dossier sécurité fournisseur

Réponses aux questions des questionnaires de sécurité fournisseurs, dans l'ordre des rubriques habituelles (inspirées du CAIQ-Lite et du SIG-Lite).

Version 1.1 du 27 octobre 2026

Contact sécurité et données personnelles : [contact@finozio.com](mailto:contact@finozio.com)

Ce dossier décrit le service Finozio à la date de sa version. Chaque réponse a été vérifiée dans le code source, la configuration ou la documentation technique du service. Quand la réponse est « non » ou « pas encore », nous l'écrivons tel quel. La politique de confidentialité ([www.finozio.com/fr/politique-confidentialite](http://www.finozio.com/fr/politique-confidentialite)) fait foi pour la liste des sous-traitants et les durées de conservation.

- |                                                     |                                                  |
|-----------------------------------------------------|--------------------------------------------------|
| 1 Gouvernance et organisation                       | 8 Journalisation et surveillance                 |
| 2 Hébergement et localisation des données           | 9 Sauvegardes et continuité                      |
| 3 Sous-traitants et intelligence artificielle       | 10 Réponse aux incidents                         |
| 4 Chiffrement                                       | 11 Signalement et gestion des vulnérabilités     |
| 5 Accès à vos environnements Azure et Microsoft 365 | 12 Conservation, réversibilité et fin de contrat |
| 6 Authentification et contrôle d'accès              | 13 Protection des données personnelles (RGPD)    |
| 7 Cloisonnement entre clients                       | 14 Sous-traitants                                |

## 1. Gouvernance et organisation

### Qui est le fournisseur ?

FINOZIO SAS, 47 rue Vivienne, 75002 Paris, France, RCS Paris 109 096 388. Contact pour la sécurité et les données personnelles : [contact@finozio.com](mailto:contact@finozio.com).

### Détenez-vous une certification de sécurité (ISO 27001, SOC 2, HDS...) ?

EN COURS

En cours pour ISO 27001 : démarche engagée en octobre 2026 — état des lieux face aux 93 contrôles de la norme et plan d'actions réalisés —, audit de certification visé en 2027 auprès d'un organisme accrédité COFRAC. Finozio ne détient pas encore de certification et n'a pas encore été audité par un tiers indépendant. SOC 2 : non prévu à ce stade.

### Un test d'intrusion a-t-il été réalisé par un tiers ?

PAS ENCORE

Pas encore. Aucun test d'intrusion n'a été mené par un prestataire indépendant. Une revue de sécurité interne du code et de la configuration a été conduite en octobre 2026 ; ses correctifs sont suivis dans le dépôt de code.

### Avez-vous désigné un DPO (RGPD, article 37) ?

NON

Non, aucun DPO n'est désigné. Les demandes relatives aux données personnelles s'adressent à [contact@finozio.com](mailto:contact@finozio.com).

Disposez-vous d'une politique de sécurité de l'information écrite ?

PARTIEL

Partiellement. Il n'existe pas de politique de sécurité formalisée et publiée. Les règles et procédures de sécurité (rotation des clés, protection de l'accès aux serveurs, sauvegarde, restauration) sont écrites dans la documentation technique du service, et une partie d'entre elles est vérifiée par des tests automatisés.

Les changements du code sont-ils contrôlés avant la mise en production ?

OUI

Oui. Chaque changement passe par une demande de fusion et par une chaîne de vérification automatisée avant d'être déployé : tests unitaires, d'intégration et de bout en bout, analyse statique, recherche de secrets dans le code, audit des dépendances vulnérables connues (npm audit, pip-audit) et quarantaine de 72 heures pour toute version de dépendance trop récente.

## 2. Hébergement et localisation des données

Où sont hébergées les données ?

Dans l'Union européenne : la base de données et l'authentification chez Supabase, à Paris (région AWS eu-west-3) ; le site, la plateforme et leur cache chez Railway, à Amsterdam (Pays-Bas) ; les traces d'erreurs chez Sentry, à Francfort (Allemagne) ; la copie hors site des sauvegardes chez Microsoft Azure, région France Centre, répliquée vers la région appariée France Sud.

Des données quittent-elles l'Union européenne ?

OUI

Oui, vers certains sous-traitants (rubrique 3) : Cloudflare, par le réseau duquel passe tout le trafic du site et de la plateforme ; Anthropic, pour l'assistant IA Aurora, à partir de l'offre Pilot ; Resend, pour les e-mails ; Stripe, pour le paiement ; et, seulement avec l'accord du visiteur et sur les pages publiques du site, Google, LinkedIn et Apollo. Supabase, Railway et Sentry gardent les données dans l'UE, mais sont des sociétés établies hors de l'UE : un accès depuis l'extérieur reste possible, encadré par des clauses contractuelles types.

Le service est-il mutualisé ?

Oui : une seule instance du service et une seule base de données pour tous les clients, cloisonnées logiquement par client (rubrique 7). Il n'existe ni hébergement dédié ni instance propre à un client.

## 3. Sous-traitants et intelligence artificielle

Qui sont vos sous-traitants, et que reçoivent-ils ?

Voir le tableau en fin de dossier. Il reprend la liste de la politique de confidentialité, qui fait foi.

### Quelles données l'assistant IA Aurora envoie-t-il à Anthropic ?

Aurora est le modèle Claude d'Anthropic (États-Unis), appelé par son API depuis nos serveurs, à partir de l'offre Pilot. Partent : le contenu des conversations (questions, réponses, et contexte saisi pour évaluer une recommandation) ; le nom et l'offre du client ; les coûts Azure agrégés (total, par service, par groupe de ressources et par souscription, avec son nom ou, à défaut, son identifiant) et leur prévision ; les recommandations ; le nom, le type, le groupe de ressources, la région, la référence (SKU) et l'état des ressources inutilisées ; le nom, la taille et les métriques d'usage des machines virtuelles ; pour Microsoft 365, des nombres et des montants agrégés. Ne partent jamais : les secrets de connexion, les étiquettes (tags) des ressources, ni aucune donnée nominative des utilisateurs Microsoft 365 (ni nom, ni e-mail, ni UPN). Cadre : clauses contractuelles types.

### Le scan gratuit et l'Audit Spring envoient-ils des données à Anthropic ?

Non. Les offres Free et Audit Spring n'ont pas Aurora, et les scans gratuits n'appellent aucune IA : le serveur vérifie l'offre du client avant tout appel à Anthropic.

### Vos données servent-elles à entraîner un modèle d'IA ?

NON

Finozio n'entraîne ni n'ajuste aucun modèle : Aurora appelle le modèle Claude par l'API d'Anthropic, sans réglage fin sur vos données.

## 4. Chiffrement

### Les données sont-elles chiffrées en transit ?

OUI

Oui. HTTPS partout, avec un en-tête HSTS d'un an (sous-domaines compris) et des cookies de session httpOnly et Secure. Entre Cloudflare et nos serveurs, la connexion est chiffrée avec vérification du certificat (mode « Full (strict) »). Le serveur applicatif refuse toute connexion non chiffrée vers la base de données. Entre le site et le serveur applicatif, le trafic emprunte le réseau privé de Railway, sans adresse publique.

### Les données sont-elles chiffrées au repos ?

PARTIEL

En partie par Finozio. Les secrets de connexion Azure et les jetons Microsoft sont chiffrés champ par champ avant d'entrer en base (Fernet : AES-128-CBC et HMAC-SHA256), avec une clé gardée hors de la base, qui peut être changée sans interruption. Les codes de secours de la double authentification et les clés d'API sont stockés hachés. Les sauvegardes sont chiffrées (AES-256-GCM) avant de quitter la machine qui les produit. Les autres données (coûts, inventaire, recommandations) ne reçoivent pas de chiffrement applicatif supplémentaire : leur chiffrement au repos est celui de l'hébergeur de la base, Supabase.

### Qui gère les clés et les secrets ?

Finozio. Les clés de chiffrement et les secrets de production ne figurent pas dans le code source : ce sont des variables de configuration de l'hébergeur, et une recherche automatique de secrets bloque toute modification qui en contiendrait. La clé privée qui déchiffre les sauvegardes n'est pas sur la machine qui les produit.

## 5. Accès à vos environnements Azure et Microsoft 365

---

### Quels droits Finozio demande-t-il sur Azure ?

Deux façons de connecter une souscription. Un Service Principal créé par vous, auquel vous attribuez, par souscription, deux rôles Azure intégrés en lecture seule : Reader et Cost Management Reader ; en option, pour les engagements, deux rôles également en lecture seule : Reservations Reader (périmètre /providers/Microsoft.Capacity) et Savings plan reader (périmètre /providers/Microsoft.BillingBenefits). Ou votre compte Microsoft (OAuth, permission déléguée user\_impersonation) : Finozio agit alors avec vos propres droits. Aucun rôle personnalisé n'est demandé.

---

### Et sur Microsoft 365 ?

Des permissions Microsoft Graph de type Application, en lecture seule : Organization.Read.All, Reports.Read.All et Directory.Read.All ; en option, AuditLog.Read.All, pour la date de dernière connexion des utilisateurs. Aucun contenu de boîte aux lettres, de fichier ni de conversation n'est lu.

---

### Finozio peut-il modifier votre environnement ?

Non, sauf sur l'offre Custom. Les droits demandés sont en lecture seule. Sur Custom, les règles d'automatisation que votre administrateur active peuvent arrêter, redimensionner et redémarrer des machines virtuelles, supprimer des disques orphelins et libérer des adresses IP publiques, avec le compte connecté à la souscription : votre compte Microsoft, ou un Service Principal auquel vous avez vous-même donné des droits d'écriture. Les scripts de correction (Azure, et retrait de licences Microsoft 365) sont générés par Finozio, puis relus et exécutés par votre administrateur : Finozio ne les exécute jamais.

---

### Les accès sont-ils conservés ?

OUI

Oui. Le secret du Service Principal ou le jeton Microsoft est conservé, chiffré (rubrique 4), jusqu'à ce que vous le supprimiez ; il sert aux relevés suivants, dont celui de chaque nuit à partir de Pilot. Le scan gratuit n'en conserve aucun : il ne garde que l'identifiant du tenant et celui de la souscription, 90 jours – sauf si le prospect choisit le rapport gratuit mensuel (case décochée par défaut) : son accès est alors conservé chiffré de la même façon, pour 12 rapports au plus, et supprimé dès l'arrêt (lien d'arrêt en un clic, achat d'une offre ou échec d'accès).

---

### Installez-vous un agent dans notre environnement ?

NON

Non. Finozio lit les API d'Azure (Azure Resource Manager, Cost Management) et de Microsoft Graph ; rien n'est installé.

---

### Comment révoquer l'accès ?

À tout moment, des deux côtés : en supprimant la connexion depuis votre espace Finozio, et, chez Microsoft, en supprimant le Service Principal ou ses attributions de rôle, ou en révoquant le consentement donné à l'application.

---

## 6. Authentification et contrôle d'accès

---

### Comment les utilisateurs s'authentifient-ils ?

Par adresse e-mail et mot de passe (service d'authentification de Supabase), ou par connexion unique SAML d'entreprise (SSO), à partir de l'offre Scale Up, sur des domaines dont la propriété est vérifiée. Les mots de passe comptent au moins 12 caractères et sont stockés hachés par Supabase ; un mot de passe présent dans des fuites connues est refusé (vérification auprès de Have I Been Pwned, à qui seuls les 5 premiers caractères de son empreinte SHA-1 sont transmis).

### La double authentification est-elle disponible, et obligatoire ?

PARTIEL

Disponible pour tout compte (application d'authentification TOTP, avec 10 codes de secours stockés hachés). Obligatoire pour les comptes d'administration de Finozio, dont les pouvoirs n'existent qu'après le second facteur. Pas encore : un client ne peut pas l'imposer aux membres de son espace. Avec le SSO, ce sont les règles de votre fournisseur d'identité qui s'appliquent, double authentification comprise.

### Êtes-vous protégés contre les attaques par force brute ?

OUI

Oui. CAPTCHA (Cloudflare Turnstile) à l'inscription, à la connexion et à la réinitialisation du mot de passe ; verrouillage de la connexion après 5 échecs en 15 minutes depuis une même adresse IP, et après 50 essais en une heure sur un même compte, toutes adresses confondues — un tiers ne peut donc pas bloquer le compte d'un client depuis sa propre adresse (pour le code de double authentification : 5 en 15 minutes et 20 en 24 heures) ; limitation du nombre de tentatives de connexion par adresse IP.

### Comment les sessions sont-elles gérées ?

Par un cookie de session httpOnly, Secure et SameSite=Lax, valable 2 heures, renouvelé par un jeton de rafraîchissement de 7 jours, que Supabase remplace à chaque usage.

### Quels rôles et quelles clés d'API ?

Des rôles distincts dans chaque espace client (administrateur, lecteur), et des clés d'API à portée limitée (lecture, écriture, suppression), stockées hachées, qui ne donnent jamais les pouvoirs d'administration de Finozio.

### Le personnel de Finozio peut-il accéder à nos données ?

Oui : les super-administrateurs de Finozio, pour le support et l'exploitation, avec une double authentification obligatoire. Chaque ouverture de votre espace par un super-administrateur est inscrite au journal d'audit (qui, quand, adresse IP), conservé 2 ans.

## 7. Cloisonnement entre clients

---

### Les données des clients sont-elles séparées ?

OUI

Oui, logiquement : dans la base commune, chaque requête du serveur applicatif est filtrée côté serveur sur l'espace de l'utilisateur, et toute demande portant sur l'espace d'un autre client est refusée. En complément, la sécurité au niveau des lignes (RLS) est activée sur toutes les tables, sans aucun accès pour les clés publiques de Supabase : seul le serveur applicatif lit la base. Un test automatisé rejoue toutes les migrations et vérifie cette règle sur chaque table.

Une base ou une clé de chiffrement dédiée par client ?

NON

Non : une seule base et une seule clé de chiffrement des secrets pour tous les clients.

## 8. Journalisation et surveillance

Les actions sensibles sont-elles journalisées ?

OUI

Oui : identifiants Azure, utilisateurs, clés d'API, automatisations, double authentification et ouverture d'un espace client par un super-administrateur, avec l'auteur, la date et l'adresse IP. Le journal est conservé 2 ans, puis supprimé automatiquement.

Avons-nous accès à ces journaux ?

PARTIEL

Pas directement : le journal d'audit est réservé à l'équipe Finozio, qui vous en fournit un extrait sur demande. Pas encore d'export vers un SIEM, et les entrées ne sont pas signées.

Comment le service est-il surveillé ?

PARTIEL

Disponibilité surveillée en continu par des sondes externes (UptimeRobot) ; erreurs techniques remontées automatiquement à l'équipe (Sentry, traces nettoyées des données personnelles) ; contrôle de santé du service (base de données, migrations, secrets, IA). Pas de centre opérationnel de sécurité (SOC).

Et les journaux techniques des hébergeurs ?

Ils sont conservés selon la durée fixée par chaque prestataire.

## 9. Sauvegardes et continuité

La base de données est-elle sauvegardée ?

PARTIEL

Oui, chaque nuit : une sauvegarde complète de la base, relue avant d'être retenue (une sauvegarde illisible est rejetée et signalée), chiffrée (AES-256-GCM) avant de quitter la machine qui la produit, puis déposée sur un stockage Microsoft Azure en France avec un jeton en écriture seule, qui ne peut ni lire ni effacer. Conservation : 30 jours, plus une copie mensuelle pendant 1 an. Une alerte s'ouvre si la dernière sauvegarde a plus de 48 heures. Limite connue, pas encore levée : la sauvegarde est lancée depuis un poste d'administration de Finozio, et non depuis l'infrastructure de production.

Les restaurations sont-elles testées ?

PARTIEL

Une restauration complète a été vérifiée sur une base séparée en septembre 2026, et la procédure est documentée. Pas encore d'exercice de restauration périodique planifié.

Avez-vous des engagements de reprise (RPO, RTO) ou de disponibilité ?

NON

Non : aucun objectif de reprise ni de disponibilité n'est engagé contractuellement, et il n'existe pas de plan de continuité d'activité formalisé. Délais de réponse du support : 48 heures (Pilot), 24 heures (Scale Up), 4 heures (Custom).

## 10. Réponse aux incidents

---

### Que faites-vous en cas de violation de données personnelles ?

Pour les données dont Finozio est responsable (comptes, facturation, prospects) : notification à la CNIL dans les 72 heures après en avoir pris connaissance (art. 33 RGPD), et information des personnes concernées en cas de risque élevé (art. 34). Pour les données de votre tenant, que Finozio traite pour votre compte : information de votre organisation dans les meilleurs délais, pour vos propres notifications (art. 33.2).

### Avez-vous une procédure écrite, et l'avez-vous éprouvée ?

PAS ENCORE

Pas encore : aucune procédure de gestion des incidents n'est publiée, et aucun exercice de crise n'a été conduit.

## 11. Signalement et gestion des vulnérabilités

---

### Comment vous signaler une vulnérabilité ?

OUI

Écrivez à [contact@finozio.com](mailto:contact@finozio.com), objet « Vulnérabilité » : réponse sous 5 jours ouvrés. Le même contact figure dans le fichier `security.txt` (RFC 9116), <https://www.finozio.com/.well-known/security.txt>. Pas de programme de prime aux bogues (bug bounty).

### Suivez-vous les vulnérabilités de vos dépendances ?

OUI

Oui : audit automatique des dépendances (npm audit, pip-audit) à chaque vérification du code ; dépendances Python figées et installées avec vérification de leur empreinte.

## 12. Conservation, réversibilité et fin de contrat

---

### Que deviennent nos données à la fin de l'offre ?

À la fin d'une offre payante, le compte repasse en offre gratuite et ses données sont conservées tant qu'il existe. Les relevés Microsoft 365, nominatifs, sont supprimés 90 jours après la fin de l'accès à une offre qui les inclut, sauf rachat ; ils sont par ailleurs limités à 13 mois glissants.

### Pouvez-vous supprimer nos données ?

OUI

Oui. La suppression du compte se demande depuis la page Mon compte ; les données sont effacées 7 jours après la demande, et disparaissent des sauvegardes à leur expiration (30 jours, 1 an pour la copie mensuelle). Les données de facturation sont conservées au moins 10 ans (obligation légale), chez Stripe.

### Pouvons-nous récupérer nos données ?

PARTIEL

En partie. Vos données personnelles s'exportent au format JSON depuis la page Mon compte (art. 20 RGPD) ; selon l'offre, l'espace propose aussi un export CSV des données FinOps, un export des coûts au format FOCUS et les exports de l'audit d'Audit Spring. Pas encore d'export unique de toutes les données de l'espace.

### Quelles sont les durées de conservation ?

Toutes figurent dans la politique de confidentialité. Principales : journal d'audit 2 ans ; conversations avec Aurora 1 an ; sessions SSO 30 jours ; demandes de scan gratuit 90 jours ; accès du rapport gratuit mensuel jusqu'à son arrêt (12 rapports au plus) ; sauvegardes 30 jours, copie mensuelle 1 an.

## 13. Protection des données personnelles (RGPD)

### Quel est le rôle de Fiozio au sens du RGPD ?

Responsable du traitement pour les données de compte, de facturation, des scans gratuits, des demandes de devis et de rendez-vous, et de mesure d'audience ; sous-traitant (art. 28) pour les données Azure et Microsoft 365 lues dans votre tenant, dont votre organisation reste responsable.

### Quelles données personnelles traitez-vous dans notre tenant ?

Les données Microsoft 365 des comptes sous licence : identifiant Microsoft Entra, adresse e-mail et UPN, nom affiché, licences, statut du compte, dates de création et de dernière connexion, activité Copilot ; à partir de Pilot, fonction, service et usage des applications, d'après les rapports de Microsoft, nominatifs sauf si votre tenant masque les noms d'utilisateur. Côté Azure : des métadonnées de ressources et de coûts.

### Comment exercer les droits des personnes ?

En écrivant à [contact@fiozio.com](mailto:contact@fiozio.com) ; l'export et la suppression du compte sont aussi en libre-service depuis la page Mon compte. Une réclamation peut être adressée à la CNIL.

## 14. Sous-traitants

| PRESTATAIRE | SOCIÉTÉ ET LIEU DES DONNÉES                                                   | RÔLE                                                                           | DONNÉES REÇUES                                                                                                                                                                                                                                                                                              | CADRE DU TRANSFERT                                                                                         |
|-------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Supabase    | Supabase Pte. Ltd. (Singapour) ; données à Paris, France (UE)                 | Base de données et authentification                                            | Toutes les données enregistrées par la plateforme                                                                                                                                                                                                                                                           | Clauses contractuelles types (CCT) de son accord de traitement, pour tout accès depuis l'extérieur de l'UE |
| Railway     | Railway Corporation (États-Unis) ; serveurs à Amsterdam, Pays-Bas (UE)        | Hébergement du site et de la plateforme (interface, serveur applicatif, cache) | Tout ce qui transite par le site et la plateforme ; journaux techniques                                                                                                                                                                                                                                     | Data Privacy Framework UE-États-Unis, CCT à défaut                                                         |
| Sentry      | Functional Software, Inc. (États-Unis) ; serveurs à Francfort, Allemagne (UE) | Suivi des erreurs techniques                                                   | Traces d'erreurs nettoyées avant envoi : ni corps des requêtes, ni secrets, ni adresses e-mail, ni cookies, ni adresses IP                                                                                                                                                                                  | Data Privacy Framework UE-États-Unis, complété par les CCT de son accord de traitement                     |
| Cloudflare  | Cloudflare (États-Unis) ; réseau mondial de Cloudflare                        | DNS, relais et protection du site et de la plateforme, CAPTCHA                 | Adresse IP, en-têtes de requête, signaux techniques du navigateur ; contenu des pages et des échanges avec la plateforme, déchiffré pour être relayé puis rechiffré vers nos serveurs                                                                                                                       | Data Privacy Framework UE-États-Unis, CCT à défaut                                                         |
| Anthropic   | Anthropic Ireland, Limited (Irlande) ; traitement aux États-Unis              | Assistant IA Aurora, à partir de l'offre Pilot                                 | Conversations ; nom et offre du client ; coûts Azure agrégés et prévision ; recommandations ; ressources inutilisées et machines virtuelles (nom, type, région, référence, état, usage) ; nombres et montants Microsoft 365 agrégés. Jamais : secrets, étiquettes (tags), données nominatives Microsoft 365 | CCT (modules 2 et 3) de son accord de traitement                                                           |

| PRESTATAIRE      | SOCIÉTÉ ET LIEU DES DONNÉES                                                                              | RÔLE                                                                                                                                     | DONNÉES REÇUES                                                                                                                               | CADRE DU TRANSFERT                                                                     |
|------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>Resend</b>    | Resend (États-Unis) ; envoi depuis l'Irlande (UE)                                                        | E-mails transactionnels                                                                                                                  | Adresse du destinataire et contenu de l'e-mail (alertes, invitations, rappels, rapport PDF d'un scan gratuit)                                | Data Privacy Framework UE-États-Unis, CCT à défaut                                     |
| <b>Stripe</b>    | Stripe (États-Unis)                                                                                      | Paiement (certifié PCI DSS)                                                                                                              | Adresse e-mail, nom et adresse de facturation, numéro de TVA, offre achetée ; la carte est saisie chez Stripe et ne passe jamais par Finozio | CCT                                                                                    |
| <b>Microsoft</b> | Microsoft (UE et international) ; sauvegardes en France (région France Centre)                           | API Azure et Microsoft Graph (source des données), prise de rendez-vous, messagerie contact@finozio.com, copie hors site des sauvegardes | Métadonnées des tenants, annuaire et licences, rapports d'activité ; e-mails échangés avec Finozio ; sauvegardes chiffrées avant envoi       | Accord de traitement des données (DPA) de Microsoft                                    |
| <b>Google</b>    | Google (États-Unis)                                                                                      | Mesure d'audience, avec consentement, sur les pages publiques, l'inscription et le choix de l'offre – jamais l'espace client             | Pages consultées, provenance, interactions, type d'appareil, localisation approximative, identifiant pseudonyme                              | Data Privacy Framework UE-États-Unis, complété par des CCT                             |
| <b>LinkedIn</b>  | LinkedIn Ireland Unlimited Company (Irlande) ; transfert possible vers LinkedIn Corporation (États-Unis) | Mesure des campagnes publicitaires, avec consentement, sur les pages publiques seulement                                                 | Pages consultées, clics, adresse IP, caractéristiques de l'appareil, identifiant de cookie                                                   | CCT                                                                                    |
| <b>Apollo</b>    | ZenLeads, Inc., sous le nom Apollo.io (États-Unis)                                                       | Identification de l'entreprise qui visite le site, avec consentement, sur les pages publiques seulement – jamais de la personne          | Pages consultées, provenance, adresse IP, caractéristiques du navigateur, identifiant aléatoire                                              | Data Privacy Framework UE-États-Unis, complété par les CCT de son accord de traitement |