LÉGAL · CONFIDENTIALITÉ

Politique de confidentialité

Cette politique de confidentialité vise à vous informer sur comment CoSec collecte, utilise et protège vos données personnelles, en application de la **Loi fédérale suisse sur la protection des données** (LPD du 25 septembre 2020, en vigueur depuis le 1er septembre 2023) et son ordonnance d'application (OPDo). CoSec est un service accessible dans tous les pays, mais il opère exclusivement sous droit suisse.

Dernière mise à jour : 1er mai 2026 · Version 0.1 · Langue de référence : français · Droit applicable : suisse uniquement

---

SOMMAIRE

1. Introduction et champ d'application

CoSec est un service en ligne (SaaS) de chatbot IA spécialisé pour les professionnels de la sécurité privée, de la sûreté événementielle et de la gestion de crise. La présente Politique de confidentialité décrit comment OlOxOn Sàrl (« nous », « CoSec ») collecte, utilise, conserve et protège les données personnelles que vous nous confiez en utilisant le service accessible aux adresses cosec.ch (https://cosec.ch) et app.cosec.ch (https://app.cosec.ch).

Cette Politique s'applique à toute personne qui consulte le site cosec.ch ou utilise l'application CoSec, que ce soit en tant que visiteur, utilisateur d'essai, ou client payant. Elle complète nos Conditions Générales d'Utilisation et nos Mentions légales.

CoSec est ouvert au monde entier mais opère exclusivement sous le **droit suisse**. Cela signifie concrètement que la collecte, le traitement, la conservation et la suppression de vos données sont régis par la **LPD** et l'**OPDo**, sous l'autorité du Préposé fédéral à la protection des données et à la transparence (PFPDT). Les ressortissants de l'Union européenne bénéficient en outre du fait que la Suisse est jugée par la Commission européenne comme offrant un **niveau de protection adéquat** au sens de l'article 45 du règlement (UE) 2016/679 (décision d'adéquation du 26 juillet 2000, toujours en vigueur) : leurs données peuvent donc transiter de l'UE vers nos serveurs suisses sans démarche additionnelle.

---

2. Qui est OlOxOn

OlOxOn Sàrl, 3 Chemin des Passereaux, 1226 Thônex, Suisse

Contact : legal@cosec.ch

Autorité de surveillance compétente : Préposé fédéral à la protection des données et à la transparence (PFPDT), Feldeggweg 1, 3003 Berne · www.edoeb.admin.ch (https://www.edoeb.admin.ch)

2.1 Distinction du rôle d'OlOxOn, selon les traitements effectués (Service et Contenu utilisateur)

OlOxOn joue **deux rôles distincts** selon la nature et la finalité des données traitées. Cette distinction est essentielle pour comprendre le partage de responsabilité entre OlOxOn et vous-même en application de la LPD et de l'OPDo.

Type de données et finalité	Qualité d'OlOxOn	Responsabilité
Données du Service : compte utilisateur, e-mail de connexion, authentification, sessions, secrets 2FA, clés publiques de passkey (FIDO2/WebAuthn), données de facturation, journaux techniques, métriques de consommation, pour permettre l'accès au Service.	**Responsable du traitement** (Art. 5 let. j LPD)	OlOxOn Sàrl
Contenu utilisateur : documents que vous téléversez dans le but d'utiliser le Service, conversations IA, livrables générés, notes mémoire, skills personnalisés, projets, fichiers vault, main courante, données personnelles de tiers (témoins, victimes, agents, organisateurs, intervenants…)	**Sous-traitant technique** (Art. 5 let. k et 9 LPD)	L'**Organisation cliente reste responsable** (respect des principes, information des personnes concernées, finalité, proportionnalité, durée). OlOxOn Sàrl agit uniquement sur instructions documentées (CGU, paramètres, e-mails, DPA) et ne traite ces données que pour fournir le Service technique.

En clair : **OlOxOn est responsable en tant que sous-traitant du fonctionnement, de la sécurité et de la disponibilité du Service ; vous restez responsable de traitement pour les informations que vous téléversez**. Si vous téléversez des données de tiers (données personnelles, rapport d'intervention, fiche d'incident, liste d'invités à un événement, etc.), c'est à vous de garantir que vous respectez les principes de la LPD et que vous avez informé ces personnes conformément à l'art. 19 LPD. Voir nos CGU §7.3 et notre DPA Cookies pour le détail.

---

3. Données collectées

OlOxOn applique une politique de collecte conforme au principe de **proportionnalité** (art. 6 al. 2 LPD) : nous ne collectons que les données nécessaires à la finalité du traitement, et chaque finalité est explicitement documentée. Nous distinguons les données obligatoires à l'inscription (qui forment le socle d'identification contractuelle) et les données complémentaires liées à l'usage.

3.1 Données obligatoires à la création du compte

Lorsque vous créez un compte CoSec, nous collectons les données suivantes **en tant que socle obligatoire d'identification contractuelle**. Cette collecte est justifiée par la nature même du Service : CoSec est un service B2B mis à disposition contre rémunération, ce qui crée un contrat entre OlOxOn Sàrl et vous (ou l'entité que vous représentez). Pour pouvoir prouver la formation et l'exécution du contrat en cas de litige, et pour respecter nos obligations comptables et fiscales suisses, nous devons pouvoir vous identifier formellement.

- **Nom** et **prénom** de la personne physique qui signe le contrat (vous-même si vous agissez en nom propre, ou le représentant qualifié de l'entité que vous engagez)
- **Adresse e-mail professionnelle** (utilisée pour l'authentification par lien magique, les communications transactionnelles et la notification des incidents de sécurité)
- **Adresse postale complète** de l'organisation contractuelle (rue, code postal, localité, pays) : figurera sur les factures officielles et permettra une notification formelle en cas de mise en demeure ou de réquisition
- **Numéro de téléphone** : *optionnel* sur tous les plans, fortement recommandé pour les alertes critiques de sécurité, le support technique urgent et la prévention de la fraude
- **Numéro IDE / TVA** : optionnel, recommandé pour les entités juridiques suisses ou européennes assujetties

Authentification : il n'y a aucun mot de passe statique. Trois mécanismes de connexion sont disponibles :

- **Passkey (FIDO2/WebAuthn)** : méthode recommandée. Une clé cryptographique privée est générée et stockée sur votre device (Secure Enclave Apple, TPM Windows, ou gestionnaire de mots de passe synchronisant les passkeys comme 1Password ou iCloud Keychain). Seule la clé publique est transmise à CoSec. La clé privée ne quitte jamais votre device et est protégée par votre biométrie locale (Touch ID, Face ID, Windows Hello). Phishing-resistant par construction.
- **Lien magique** à usage unique envoyé à votre adresse e-mail (validité 15 minutes) : fallback universel disponible depuis n'importe quel appareil.
- **Double authentification TOTP** (Time-based One-Time Password) : optionnelle, ajoute un code à 6 chiffres généré par votre application Authenticator au lien magique. Le secret TOTP et les codes de récupération sont stockés sous forme chiffrée AES-256-GCM.

Une connexion par passkey satisfait à elle seule les critères de l'authentification multi-facteurs (possession du device + biométrie locale). Les clés publiques de passkey sont stockées telles quelles côté serveur : la clé privée reste exclusivement sur votre device, donc rien à chiffrer côté CoSec.

3.2 Données de paiement (à la souscription d'un plan payant)

Au moment où vous souscrivez un plan payant (Solo, Team, Entreprise), des données de paiement complémentaires sont collectées via la Checkout Session sécurisée de notre partenaire **Stripe** :

- **Adresse de facturation** spécifique (si différente de l'adresse postale du compte)
- **E-mail de facturation** (si différent de l'e-mail de connexion)
- **Identifiants techniques Stripe** : customer_id, subscription_id, charge_id (rattachés à vos pièces comptables, conservés 10 ans en application du CO art. 958f)
- **Marque et 4 derniers chiffres** de la carte de paiement, à titre purement indicatif (Visa •••• 4242)

Le **numéro complet de carte bancaire n'est jamais transmis ni stocké par CoSec** : il est saisi directement dans le composant sécurisé Stripe Checkout (Stripe est certifié PCI-DSS niveau 1, le plus haut niveau de la norme).

Tant que vous restez en période d'essai gratuit, aucune donnée de paiement n'est traitée par Stripe et aucun prélèvement n'a lieu : la carte enregistrée n'est utilisée qu'à des fins de validation (SetupIntent, sans débit).

3.3 Données d'organisation et d'équipe

- **Identification org** : nom de l'organisation, slug, logo (optionnel)
- **Plan** : niveau d'abonnement (free, solo, team, entreprise), date de début, période de facturation
- **Membres** : liste des utilisateurs invités dans l'organisation, leurs rôles (owner, admin, member)

3.4 Contenu utilisateur (vos données métier)

- **Conversations IA** : messages que vous envoyez à l'assistant IA, réponses générées, skill ou template utilisé, conversation_id, projet associé
- **Documents téléversés** : nom du fichier, type MIME, taille, contenu textuel extrait, vecteurs d'embeddings (représentations numériques pour la recherche sémantique), clé S3 de stockage, somme de contrôle SHA-256
- **Notes mémoire** : titres, contenus, catégories, ordre de tri
- **Skills personnalisés** : titre, description, prompt système rédigé par vous
- **Projets** : nom, nom du client final, type de mission, description, dates, statut
- **Main courante (incidents)** : type d'incident, gravité, statut, contenu textuel, métadonnées de séance
- **Vault (stockage de fichiers)** : fichiers, versions historisées, dossiers, quotas utilisés
- **Données personnelles**
  Pour le Contenu utilisateur, OlOxOn agit en qualité de **sous-traitant technique** (cf. §2.1) : c'est vous, en tant que responsable du traitement, qui êtes responsable que les traitements sont effectués dans le respect des obligations découlant de la LPD et de l'OPDo.

3.5 Données d'usage techniques

- **Événements de consommation** : type d'événement (chat, embedding, audit, skill, transcription), modèle IA utilisé, nombre de tokens en entrée/sortie, coût en CHF, horodatage
- **Logs techniques** : adresses IP (utilisées pour la limitation de débit et la détection d'abus), user agent du navigateur, codes HTTP de réponse, temps de réponse, identifiants de requête
- **Crédits IA** : solde, historique des consommations et recharges, raison de chaque mouvement (consumption, monthly_reset, plan_change, trial_grant, admin_adjust, topup)

3.6 Données de suppression et anonymisation

- Date de demande de suppression (deleted_at)
- Date de purge planifiée (scheduled_purge_at, généralement +30 jours)
- Date d'anonymisation effective (anonymized_at)

3.7 Données sensibles (Art. 5 let. c LPD)

Nous ne traitons pas de **données sensibles au sens de l'art. 5 let. c LPD**.

Si vous téléversez de telles données dans l'application vous le faites à vos risques et sous votre seule responsabilité de responsable de traitement (cf. §2.1) :

- Données sur la santé, la sphère intime, l'origine raciale ou ethnique
- Données génétiques
- Données biométriques identifiant une personne de manière univoque
- Données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales
- Données sur les poursuites ou sanctions pénales et administratives (au-delà de ce qui est strictement nécessaire dans le cadre des activités de sécurité privée légalement autorisées)
- Données sur les mesures d'aide sociale

3.8 Newsletter (optionnelle)

CoSec propose une newsletter (« Le Brief CoSec ») permettant de recevoir périodiquement des actualités produit et des contenus métier. L'inscription est **strictement facultative** et indépendante de la création d'un compte CoSec.

Pour vous inscrire, nous collectons votre **adresse e-mail** uniquement, sur la base de votre **consentement libre et informé** (art. 6 al. 6 et 7 LPD). Aucune autre donnée n'est demandée.

Vous pouvez vous **désinscrire à tout moment** via le lien « Se désinscrire » présent en bas de chaque e-mail, ou en écrivant à legal@cosec.ch. La désinscription entraîne la suppression immédiate de votre adresse e-mail de la liste de diffusion.

---

4. Finalités et bases légales (LPD)

Nous traitons vos données pour les finalités suivantes, sur les bases légales du droit suisse de la protection des données :

Finalité	Base légale (LPD & CO)
Fournir le service (création de compte, accès, chatbot IA, stockage)	Article 30 LPD + relation directe avec exécution du contrat (Art. 31 al. 2 let. a LPD)
Authentification, sécurité, prévention des abus	Article 30 LPD et Art. 31 al. 2 LPD (intérêt privé prépondérant à protéger le Service et ses utilisateurs)
Facturation, comptabilité, recouvrement	Article 30 LPD et Art. 31 al. 1 LPD (obligation légale) en lien avec CO Art. 957 ss et 958f
Support utilisateur	Article 30 LPD et Art. 31 al. 2 let. a LPD (relation directe avec l'exécution du contrat)
Amélioration du produit (analyses agrégées anonymisées)	Art. 31 al. 2 let. e LPD (statistique, recherche et planification, à condition d'anonymisation)
Communications transactionnelles (factures, alertes sécurité, fin d'essai)	Article 30 LPD et Art. 31 al. 2 let. a LPD (exécution du contrat)
Communications commerciales (newsletters, nouveautés)	Article 31 al. 1 LPD et Art. 6 al. 6 et 7 LPD (consentement libre et informé, retirable à tout moment)
Conservation post-résiliation à des fins légales (factures, pièces comptables)	Article 30 LPD et Art. 31 al. 1 LPD (obligation légale), en lien avec CO Art. 958f (10 ans) et LTVA Art. 70 si applicable

4.1 Ce que nous ne faisons jamais

- **Aucun entraînement de modèles IA** au moyen de vos données (voir section 5)
- **Aucune revente** de données à des tiers
- **Aucun profilage publicitaire** ou comportemental
- **Aucun partage** à des fins de marketing tiers
- **Aucune décision individuelle automatisée** ayant des effets juridiques ou significatifs au sens de l'**art. 21 LPD** (voir section 12.4)
- **Aucun profilage à risque élevé** au sens de l'art. 5 let. g LPD

---

5. Traitement par intelligence artificielle

CoSec utilise des modèles de langage (LLM) et d'embeddings pour fournir son service. Tous ces modèles sont opérés par **Infomaniak Network SA en Suisse** via l'API *Infomaniak AI Services* :

- **Qwen3-VL-235B-A22B-Instruct** (modèle principal pour les conversations)
- **Mistral-Small-3.2-24B** (modèle pour le routage des skills et les brouillons)
- **BGE Multilingual Gemma 2** (embeddings pour la recherche sémantique RAG)

Important, engagement souverain : aucune requête, aucun document, aucune conversation n'est envoyée à OpenAI, Anthropic, Google, Meta, ou tout autre fournisseur étranger. L'intégralité du traitement IA a lieu sur des serveurs Infomaniak situés en Suisse.

Aucune donnée n'est utilisée pour entraîner les modèles IA. Infomaniak Network SA s'engage contractuellement, dans le cadre de son service AI Services, à ne pas réutiliser les requêtes de ses clients pour entraîner ou ré-entraîner les modèles.

Pour plus d'informations sur l'infrastructure souveraine CoSec, voir notre page Sécurité & souveraineté.

---

6. Hébergement et localisation

L'ensemble des données du service CoSec sont hébergées exclusivement en Suisse, dans les datacenters d'Infomaniak Network SA situés à Genève et à Zurich :

- **Base de données** (PostgreSQL 16 + pgvector) : VM OpenStack chez Infomaniak Public Cloud, région Zurich (az-3)
- **Stockage de fichiers** (documents téléversés, livrables exportés) : Object Storage Swift S3-compatible chez Infomaniak, région Zurich
- **Application** (Next.js) : Node.js Hosting d'Infomaniak, datacenter suisse
- **Service IA** (chatbot, embeddings) : Infomaniak AI Services, datacenter Genève
- **E-mails transactionnels** (magic links, factures, alertes) : Infomaniak Mail SMTP, datacenter suisse
- **Sauvegardes chiffrées** : Object Storage chiffré chez Infomaniak, conservées 7 jours en local + 90 jours en Object Storage

Aucune donnée du service CoSec n'est hébergée hors de Suisse. La seule exception est **Stripe** (sous-traitant facturation), dont l'infrastructure est répartie entre l'Irlande (UE) et les États-Unis. Les données transmises à Stripe sont strictement limitées aux informations de facturation (e-mail, nom, adresse, montant, identifiant de transaction). Voir section 8.

---

7. Mesures de sécurité

Nous mettons en œuvre les mesures techniques et organisationnelles suivantes pour protéger vos données :

7.1 Mesures techniques

- **Chiffrement en transit** : TLS 1.3 obligatoire (HSTS preload, certificat Let's Encrypt)

- **Chiffrement au repos** : AES-256 pour les volumes de stockage Infomaniak (base de données, Object Storage)
- **Mots de passe** : aucun mot de passe statique ; authentification par **passkey (FIDO2/WebAuthn, recommandé)** ou lien magique à usage unique (15 min de validité)
- **Passkey FIDO2/WebAuthn** : clé privée crypto-bound au device de l'utilisateur (Secure Enclave Apple, TPM Windows, gestionnaire synchronisant les passkeys), seule la clé publique est stockée côté CoSec. Phishing-resistant par construction (le browser vérifie le domaine au moment de la signature). Standard ouvert utilisé par Apple, Google, Microsoft, GitHub, Cloudflare
- **Double authentification (2FA)** : disponible via TOTP (Google Authenticator, Authy, Dashlane, etc.) en complément du lien magique ; opt-in pour tous les rôles, recommandée. Une connexion par passkey satisfait déjà l'authentification multi-facteurs et n'exige pas de TOTP additionnel
- **Sessions courtes** : durée maximum de 7 jours (vs 30 jours par défaut Auth.js), pour limiter la fenêtre d'exploitation en cas de vol de cookie ou de device compromis
- **Notification de connexion** : un e-mail est envoyé à l'utilisateur à chaque nouvelle connexion réussie, contenant la date, l'adresse IP approximative et l'appareil détecté, pour permettre la détection rapide d'une compromission de compte
- **Isolation multi-tenant** : chaque organisation est isolée logiquement par contrôle d'accès au niveau base de données (Row-Level Security applicatif)
- **Limitation de débit** (rate limiting) : par IP et par compte sur les routes sensibles (5 magic links/min/IP, 30 conversations/min/utilisateur, 10 uploads/min/utilisateur, 3 demandes de suppression de compte/heure/IP)
- **Headers HTTP sécurité** : Content-Security-Policy stricte, X-Frame-Options DENY, HSTS 2 ans + preload, Cross-Origin-Opener-Policy same-origin
- **Pare-feu applicatif** et Fail2ban sur la VM Postgres (jail SSH durcie)
- **Sauvegardes quotidiennes** automatisées vers un bucket Object Storage dédié, conservées 90 jours
- **Page d'état publique** : app.cosec.ch/status (https://app.cosec.ch/status), monitoring temps réel des composants critiques

7.2 Mesures organisationnelles

- Accès restreint aux données de production : seul le personnel d'OlOxOn Sàrl strictement habilité a accès aux serveurs (clés SSH dédiées, pas de mot de passe)
- Journal d'audit des actions sensibles (table `audit_events`) : connexions et déconnexions, activation/désactivation 2FA, enregistrement et révocation de passkeys, modifications de la configuration de l'organisation, suppressions d'éléments ; conservé pour traçabilité forensique et conformité
- Sensibilisation continue aux risques cyber et au phishing

7.3 Notification des violations de données (Art. 24 LPD)

En cas de violation de la sécurité des données au sens de l'**art. 5 let. h LPD** susceptible d'entraîner un risque pour la personnalité ou les droits fondamentaux des personnes concernées, nous nous engageons à :

- En tant que **Responsable de traitement**, si les conditions de l'article 24 al. 1 LPD sont remplies, à notifier le **Préposé fédéral à la protection des données et à la transparence (PFPDT)** dans les **meilleurs délais** après en avoir pris connaissance.
- En tant que **Sous-traitant**, à vous informer dans les meilleurs délais et à vous assister sur votre demande.
- Inclure dans les informations à transmettre la nature de la violation, le moment et la durée, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences et les mesures prises ou prévues.
- Conserver la documentation de toute violation pendant **au moins deux ans**, conformément à l'OPDo Art. 15 al. 4.

---

8. Sous-traitants et partage

Pour fournir notre service, nous faisons appel à un nombre restreint de sous-traitants triés sur le volet. La liste complète et à jour, avec les finalités, la localisation et les garanties contractuelles, est disponible sur la page Sous-traitants.

Synthèse :

Sous-traitant	Rôle	Pays	DPA signé
Infomaniak Network SA	Hébergement, base de données, IA, stockage, mail	Suisse	Oui
Stripe Payments Europe Ltd.	Paiement et facturation	Irlande (UE) + USA	DPA Stripe en vigueur (version 18 novembre 2025, applicable via le Stripe Services Agreement) · Data Transfers Addendum (SCCs UE 2021/914) · Swiss-U.S. DPF (Annexe 1 OPDo, depuis le 15 sept. 2024) · Garanties art. 16 al. 2 let. b LPD

Nous ne vendons, ne louons et ne partageons jamais vos données avec d'autres tiers. Nous ne divulguons des données qu'aux **autorités suisses compétentes** lorsque nous y sommes légalement contraints (réquisition judiciaire ou administrative de droit suisse), et après avoir vérifié la validité de la demande. Le cas échéant, nous vous informons sans délai sauf interdiction légale, et nous limitons la divulgation au strict nécessaire.

En tant que société suisse non soumise au CLOUD Act américain ni au FISA 702, nous ne pouvons légalement pas répondre à des demandes extrajudiciaires émanant d'autorités étrangères sans passage par la procédure d'entraide internationale pénale ratifiée par la Suisse.

---

9. Transferts à l'étranger (Art. 16-17 LPD)

Comme indiqué en section 6, l'ensemble des données du service CoSec est stocké en Suisse. Le seul transfert à l'étranger concerne notre sous-traitant de paiement Stripe.

9.1 Stripe Payments Europe Ltd.

Stripe Payments Europe Ltd. est établi en Irlande (UE) et son groupe est aux États-Unis. Les seules données transmises sont les **données strictement nécessaires à la facturation** (e-mail, nom, adresse de facturation, identifiant de transaction, métadonnées de l'abonnement, montants). Le numéro complet de carte n'est jamais transmis ni stocké par CoSec.

Les bases légales des transferts au sens de la LPD sont les suivantes :

- **Suisse → Irlande (UE)** : transfert autorisé sur la base de l'**art. 16 al. 1 LPD**, l'Union européenne figurant à l'**Annexe 1 OPDo** parmi les États reconnus par le Conseil fédéral comme offrant un niveau de protection adéquat
- **Suisse → Irlande (Stripe Payments Europe Ltd.) → États-Unis (Stripe LLC)** : le transfert Suisse → Irlande bénéficie de la décision d'adéquation pour l'UE (Annexe 1 OPDo, art. 16 al. 1 LPD). Le transfert Irlande → USA est couvert par l'adhésion de Stripe au **Swiss-U.S. Data Privacy Framework**, mécanisme d'adéquation reconnu par l'Annexe 1 OPDo depuis le 15 septembre 2024 (art. 16 al. 1 LPD), et complété par les **Standard Contractual Clauses UE 2021/914** intégrées au **Data Transfers Addendum Stripe** (stripe.com/legal/dta (https://stripe.com/legal/dta)), au sens de l'art. 16 al. 2 let. b LPD
- Stripe est certifiée **PCI-DSS niveau 1, SOC 1 Type II et SOC 2 Type II**. Le **DPA Stripe** (stripe.com/legal/dpa (https://stripe.com/legal/dpa), version du 18 novembre 2025) est applicable à OlOxOn Sàrl par incorporation au Stripe Services Agreement, formant un contrat électronique opposable au sens de l'art. 28 al. 9 RGPD et de l'art. 14 CO

À la demande, OlOxOn Sàrl peut fournir copie des garanties contractuelles applicables aux transferts (legal@cosec.ch).

9.2 Pas d'autre transfert

Aucune autre donnée n'est transférée hors de Suisse. Les modèles d'IA utilisés sont opérés exclusivement par Infomaniak Network SA dans ses datacenters de Genève et Zurich (cf. §5 et §6). Les e-mails transactionnels sont envoyés depuis l'infrastructure SMTP suisse d'Infomaniak. Les sauvegardes restent dans les datacenters suisses.

10. Durées de conservation et données conservées par obligation légale

En vertu du **principe de minimisation** (art. 6 al. 4 LPD), nous conservons vos données uniquement pendant la durée strictement nécessaire aux finalités décrites en section 4. Certaines données doivent toutefois être conservées au-delà de la suppression de votre compte, en raison d'obligations légales suisses impératives.

Catégorie de donnée	Durée de conservation	Base légale
Compte utilisateur (e-mail, nom, sessions)	Durée du compte + 30 jours après demande de suppression	Période de grâce contractuelle (rétractation)
Conversations IA, documents, projets, vault, main courante	Durée du compte + 30 jours après demande de suppression	Suppression effective et physique au-delà
Notes mémoire, skills personnalisés	Durée du compte + 30 jours après demande de suppression	Idem
Logs techniques (IP, requêtes, user agent)	30 jours glissants	Art. 31 al. 2 LPD (sécurité, prévention des abus)
Journaux d'audit administratifs (table audit_events)	1 an	Art. 8 LPD & OPDo Art. 4 (traçabilité forensique)
Événements de consommation IA (usage_events)	3 ans	Reporting interne et contrôle des coûts (anonymisés à la suppression)
Factures, livre des ventes, pièces comptables	10 ans	CO Art. 958f (obligation comptable)
Pièces TVA (lorsque applicable)	5 à 10 ans	LTVA Art. 70
Identifiants techniques Stripe (customer_id, subscription_id)	10 ans (rattachés aux pièces comptables)	CO Art. 958f
Données utiles à un litige en cours (notamment documents contractuels)	Fin du contrat ou Durée du litige + délais de prescription	CO Art. 127 (10 ans, créances contractuelles)
Sauvegardes Postgres chiffrées	Max 90 jours en Object Storage Infomaniak, 7 jours sur la VM	Reprise après sinistre, écrasement automatique

10.1 Données conservées après votre demande de suppression de compte

Lorsque vous demandez la suppression de votre compte (cf. section 12.3), nous procédons à un **soft-delete immédiat** qui rend vos données inaccessibles. Au-delà de la période de grâce de **30 jours**, tout est **physiquement purgé** de nos systèmes **à l'exception** des données suivantes, que le droit suisse nous impose de conserver :

- **Factures et pièces comptables (10 ans, CO Art. 958f)** : numéro de facture, date, montant brut et net, désignation du plan, pays de facturation, période couverte. Ces factures sont indispensables au respect de nos obligations comptables et fiscales suisses, ainsi qu'aux contrôles éventuels de l'Administration fiscale cantonale et fédérale.
- **Livre de comptes et documents commerciaux (10 ans, CO Art. 958f)** : toute pièce documentant la conclusion ou l'exécution du contrat (ordres de prélèvement, notifications de paiement, justificatifs de remboursement).
- **Documents contractuels (CO article 127, 10 ans après la fin du contrat)**
- **Pièces TVA (5 à 10 ans, LTVA Art. 70)** lorsqu'OlOxOn Sàrl deviendra assujettie à la TVA suisse (au-dessus de CHF 100 000 de chiffre d'affaires annuel).
- **Identifiants techniques Stripe (10 ans)** : customer_id, subscription_id, charge_id ; rattachés aux pièces comptables ci-dessus, ils servent à prouver la chaîne complète de facturation en cas de contrôle.
- **Journaux d'audit techniques (1 an glissant, art. 8 LPD & OPDo Art. 4)** : actions de sécurité (connexions, déconnexions, activation 2FA, modifications sensibles) conservées de manière anonymisée pour la traçabilité forensique en cas d'incident.
- **Données pertinentes à un litige en cours (CO Art. 127, jusqu'à 10 ans)**

---

11. Cookies et traceurs

CoSec applique une politique de cookies **minimaliste** et transparente, conforme à la **LPD** et aux recommandations du **PFPDT**. Aucun pixel publicitaire, aucun outil d'analyse comportementale tiers (pas de Google Analytics, Hotjar, Meta Pixel, Mixpanel, Cloudflare, etc.). Aucun GAFAM dans la chaîne de traitement.

11.1 Catégories de cookies utilisés

A. Cookies strictement nécessaires (toujours actifs)
Ces cookies sont indispensables au fonctionnement du Service et ne sont pas soumis à consentement (Art. 31 al. 2 let. a LPD, relation directe avec l'exécution du contrat). Vous ne peux pas les désactiver sans rendre le Service inutilisable.

- **Cookie de session Auth.js** (HttpOnly, Secure, SameSite=Lax) : durée 7 jours. Maintient votre connexion entre les pages de l'application app.cosec.ch.
- **Cookie de vérification 2FA** (HttpOnly, Secure) : durée 7 jours. Atteste que votre code TOTP a été vérifié pour cette session.

- **Cookie CSRF** (HttpOnly, Secure) : durée de session. Protection contre les attaques de type cross-site request forgery.
- **Cookie de préférence de thème** (light/dark) : durée 1 an. Stocke votre choix de mode d'affichage.
- **Cookie de préférence cookies** (`cosec_consent`) : durée 12 mois. Mémorise votre choix dans la bannière de cookies pour ne pas vous la réafficher à chaque visite.

B. Cookies de mesure d'audience technique (anonymisés, opt-out possible)
Pour **monitorer la performance technique de la navigation** et détecter les pannes éventuelles (temps de chargement, taux d'erreur HTTP, parcours techniques), nous exploitons :

- **Logs serveur Apache** standard sur cosec.ch et Node.js sur app.cosec.ch : adresse IP, user agent, URL demandée, code HTTP, temps de réponse, identifiant de requête. Conservés 30 jours glissants.
- Le cas échéant, un cookie technique anonymisé pour mesurer le parcours de navigation (durée de session, pages vues, sans tracking inter-sites). Aucun fingerprinting, aucun lien avec un identifiant publicitaire.

Finalité : exclusivement le monitoring technique de la disponibilité et de la performance du Service, ainsi que la prévention des abus et l'amélioration ergonomique sur statistiques agrégées.

Base légale : **art. 31 al. 2 let. e LPD** (statistique et planification, à condition d'anonymisation des résultats publiés) et **art. 31 al. 2 let. a LPD** (intérêt prépondérant à exploiter, sécuriser et améliorer le Service que vous utilisez).

Opt-out : vous pouvez refuser cette catégorie via la bannière de cookies affichée à votre première visite, ou la désactiver à tout moment en cliquant sur le lien « Cookies » dans le pied de page. Les logs serveur strictement techniques (sécurité, prévention d'abus) restent collectés en application de l'art. 31 al. 2 let. a LPD.

11.2 Cookies que CoSec n'utilise jamais

- Cookies publicitaires ou de retargeting
- Pixels Meta, X (Twitter), TikTok, LinkedIn ou tout réseau social
- Google Analytics, Google Tag Manager, Google Ads, Google Signals
- Cookies tiers (third-party) à finalité commerciale
- Outils de session replay (Hotjar, Mouseflow, FullStory) qui rejouent votre navigation

11.3 Position du PFPDT et cadre LPD

En droit suisse, la **LPD ne prévoit pas d'obligation générale de consentement préalable** au dépôt de cookies, contrairement à la directive ePrivacy européenne. Le PFPDT recommande toutefois la **transparence** (information claire au sens de l'art. 19 LPD) et la **proportionnalité** (art. 6 al. 2 LPD). CoSec respecte ces principes : information visible dès la première visite, choix d'opt-out possible pour toute catégorie non strictement nécessaire, opt-out durable mémorisé.

12. Vos droits selon la LPD

Vous disposez des droits suivants concernant vos données personnelles, conformément aux articles 25 à 32 LPD :

12.1 Liste des droits

- **Droit d'accès** (art. 25 LPD) : savoir si nous traitons des données vous concernant et obtenir les informations nécessaires pour faire valoir vos autres droits (identité du responsable, finalités, catégories de données, durée de conservation, origine, destinataires, existence éventuelle de décisions automatisées). Réponse dans un délai de **30 jours** (OPDo Art. 18).
- **Droit de rectification** (art. 32 al. 1 LPD) : exiger la correction de toute donnée inexacte vous concernant. Si l'exactitude d'une donnée ne peut être établie, vous pouvez demander qu'une mention de son caractère litigieux y soit ajoutée.
- **Droit à l'effacement / destruction** (art. 32 al. 2 LPD) : demander la suppression de vos données dès lors qu'elles ne sont plus nécessaires aux finalités pour lesquelles nous les avons collectées (sous réserve des conservations légales décrites en section 10.1).
- **Droit à la remise (portabilité)** (art. 28 LPD) : recevoir, dans un format électronique couramment utilisé, les données personnelles que vous nous avez confiées, dès lors que le traitement repose sur un consentement ou un contrat.
- **Droit d'opposition** (art. 30 LPD) : vous opposer à tout traitement de vos données personnelles par OlOxOn Sàrl, sous réserve d'un éventuel motif justificatif (intérêt prépondérant, contrat, obligation légale).
- **Droit de retirer votre consentement** à tout moment, pour les traitements fondés sur le consentement (par exemple les communications commerciales optionnelles), conformément à l'art. 6 al. 6 LPD.
- **Droit d'être informé d'une décision individuelle automatisée** ayant des effets juridiques ou significatifs (art. 21 LPD) et de demander une révision par une personne physique. Voir section 12.3, CoSec ne prend toutefois aucune décision de ce type.

12.2 Comment exercer vos droits

Pour exercer un droit, écrivez-nous à legal@cosec.ch en précisant votre demande et l'adresse e-mail liée à votre compte CoSec. Nous pourrons vous demander une preuve d'identité raisonnable pour éviter toute usurpation. Nous répondons dans les **30 jours** à partir de la réception de votre demande, conformément à l'OPDo Art. 18. Ce délai peut exceptionnellement être prolongé de deux mois pour les demandes complexes (Art. 25 al. 7 LPD), avec information préalable.

L'exercice de vos droits est **gratuit**. Des frais raisonnables n'excédant pas **CHF 300** peuvent être facturés en cas d'efforts disproportionnés (OPDo Art. 19), avec information préalable et faculté de retirer votre demande.

La suppression de votre compte peut être demandée directement depuis l'interface de l'application : app.cosec.ch/settings/delete-account (https://app.cosec.ch/settings/delete-account). Cette suppression

déclenche automatiquement la procédure de purge en 30 jours décrite en section 10.

12.3 Décisions automatisées et profilage

CoSec ne prend **aucune décision individuelle automatisée** au sens de l'**art. 21 LPD** et n'effectue **aucun profilage à risque élevé** au sens de l'art. 5 let. g LPD. L'IA générative produit du contenu rédactionnel d'aide (drafts de communiqués, analyses, fiches réflexes, etc.) que **vous validez, modifiez ou rejettez librement**. C'est vous, professionnel de la sécurité, qui restez seul décideur de l'usage que vous faites de ces livrables. Aucun effet juridique ni significatif ne découle automatiquement d'une réponse de CoSec.

12.4 Réclamation auprès du PFPDT

Si vous estimez qu'un traitement de vos données par cosec ne respecte pas la LPD, vous pouvez nous saisir en priorité (legal@cosec.ch) pour résolution amiable. À défaut, vous pouvez également **signaler des faits au PFPDT** (art. 49 LPD) ou ouvrir une procédure civile devant les tribunaux genevois compétents.

---

13. Mineurs

CoSec est un service B2B destiné à des professionnels. Il n'est pas conçu, ni commercialisé, ni accessible aux mineurs de moins de 18 ans. Si nous apprenons qu'un compte a été créé par un mineur, nous le supprimons sans délai. Si vous pensez qu'un mineur nous a fourni des données personnelles, contactez-nous immédiatement à legal@cosec.ch.

---

14. Modifications de la Politique

Nous pouvons mettre à jour cette Politique de confidentialité pour refléter des évolutions légales, techniques ou opérationnelles. Toute modification substantielle vous sera notifiée :

- Par e-mail à l'adresse de votre compte CoSec, au moins **30 jours avant l'entrée en vigueur**
- Par bandeau d'information sur l'application app.cosec.ch lors de votre prochaine connexion

Vous pourrez alors résilier votre abonnement sans frais avant l'entrée en vigueur si vous n'êtes pas d'accord avec les nouvelles conditions. La date de dernière mise à jour est toujours affichée en tête de cette page (« Version »).

---

15. Contact, autorité, réclamations

15.1 Nous contacter

Pour toute question relative à cette Politique de confidentialité ou à l'exercice de vos droits :

E-mail	legal@cosec.ch

Courrier postal	OlOxOn Sàrl, Protection des données 3 Chemin des Passereaux 1226 Thônex, Suisse

15.2 Autorité de surveillance

L'autorité compétente pour le service CoSec est, exclusivement :

Préposé fédéral à la protection des données et à la transparence (PFPDT)
Feldeggweg 1, 3003 Berne, Suisse
www.edoeb.admin.ch (https://www.edoeb.admin.ch)

Toute personne peut adresser une réclamation au PFPDT contre OlOxOn Sàrl pour les données traitées dans le cadre du Service CoSec. CoSec étant un service mondial opérant exclusivement sous droit suisse, le PFPDT est l'unique autorité de surveillance compétente.

Pour les conditions d'utilisation du service, voir nos Conditions Générales d'Utilisation.
Pour la liste complète et à jour de nos sous-traitants, voir la page Sous-traitants.
Pour comprendre notre infrastructure souveraine, voir la page Sécurité & souveraineté.