FAQ Sécurité, Conformité & Identité numérique

Tout ce que vous devez savoir sur la sécurité, la confidentialité et la conformité de nos produits.

1. Général

Q1. Vos solutions sont-elles sécurisées ?

Oui. Nos services reposent sur des standards de sécurité éprouvés, une infrastructure résiliente, et un cadre de gouvernance robuste. Chaque produit est soumis à des analyses de risques, audits indépendants, et tests d'intrusion réguliers.

Q2. Êtes-vous conforme à toutes les lois applicables, incluant les lois sur la vie privée ?

Oui. Nous respectons les lois applicables dans toutes les juridictions où nous opérons, incluant :

- Loi 25 (Québec)
- LPRPDE (Canada fédéral)
- RGPD (Europe)
- CAN-SPAM / Loi canadienne anti-pourriel.
- Nous avons désigné un Délégué à la protection des renseignements personnels.

Q3. Avez-vous une politique de confidentialité publique ?

Oui. Notre politique est facilement accessible sur notre site web. Elle explique comment nous recueillons, utilisons, partageons et protégeons les renseignements personnels.

Q4. Obtenez-vous le consentement explicite des utilisateurs avant de recueillir leurs données ?

Toujours. Nous utilisons des mécanismes de consentement éclairé, avec preuve journalisée, adaptés à chaque cas d'usage.

Q5. Qui peut accéder à mes données ?

Seules les personnes autorisées, selon le principe du moindre privilège, peuvent accéder à vos données, et uniquement si c'est nécessaire. Tous les accès sont journalisés, surveillés, et revus régulièrement.

Q6. Vos pratiques sont-elles encadrées par des politiques et procédures documentées ?

Oui. Nous maintenons :

- Un corpus de politiques de sécurité et de vie privée approuvées par la direction
- Des plans de réponse aux incidents
- Des matériels de formation pour nos employés
- Des procédures avec tiers, incluant des clauses contractuelles avec nos sous-traitants
- Des revues de conformité internes et externes

Q7. Êtes-vous inscrits auprès d'un organisme de réglementation ou d'autoréglementation ?

Oui. En fonction de nos produits, nous collaborons avec :

- L'OQLF (pour l'usage du français au Québec)
- Des organismes de certification (ex. ETSI/eIDAS, ISO)
- Les autorités réglementaires lorsque requis

2. Cybersécurité technique

Q8. Protégez-vous les données en transit et au repos ?

Oui. Nous utilisons des mécanismes comme le chiffrement (AES-256, TLS), la pseudonymisation et l'anonymisation, notamment dans les environnements de test ou préproduction.

Q9. Avez-vous des standards de durcissement pour vos serveurs, réseaux et postes ?

Oui. Nous appliquons des standards stricts incluant :

- Gestion de correctifs (patching)
- MFA obligatoire
- Politique zéro compte générique ou partagé
- Sécurisation des routeurs, firewalls, points d'accès, postes, serveurs physiques et virtuels

Q10. Employez-vous des systèmes de détection d'intrusion (IDS) ?

Oui. Nous utilisons des outils de surveillance réseau (IDS/IPS) pour détecter les comportements anormaux ou malveillants.

Q11. Réalisez-vous des tests d'intrusion et gérez-vous les vulnérabilités ?

Oui. Nous faisons des tests d'intrusion annuels réalisés par des firmes spécialisées. Nous avons aussi un programme formel de gestion des vulnérabilités (scanner automatique, registre, plans correctifs).

Q12. Vos postes utilisateurs sont-ils protégés (chiffrement, antivirus, etc.) ?

Oui. Tous les ordinateurs portables et de bureau sont dotés de :

- Chiffrement intégral du disque
- Tous les postes sont protégés par un EDR avec gestion centralisée
- Possibilité de suppression à distance des données en cas de perte ou de vol.

Q13. Les journaux d'activités sont-ils détaillés et exploitables ?

Oui. Nos journaux contiennent des métadonnées complètes (accès, modification, signature, consentement) et sont utilisés dans nos enquêtes d'incidents, audits et vérification

3. Protection des données

Q14. Où sont hébergées mes données ?

Vos données sont hébergées au Canada. Aucun transfert hors de cette zone sans votre consentement explicite.

Q15. Chiffrez-vous les données ?

Oui. Toutes les données sont chiffrées au repos et en transit, avec des algorithmes éprouvés (AES-256, TLS 1.2+). Nous appliquons également des mécanismes d'intégrité, des signatures numériques et des protections contre la falsification.

Q16. Conservez-vous mes données après la fin de notre relation commerciale ?

Nous ne conservons vos données que le temps nécessaire à des fins contractuelles, légales ou réglementaires. Vous pouvez demander leur suppression définitive, sauf obligation contraire.

4. Signatures et identité numérique

Q17. Que garantit CertifiO sur l'identité d'un signataire ?

CertifiO lie un certificat numérique émis au nom d'une personne à son identité vérifiée. Cette identité est :

- Validée via des preuves officielles
- Revue par un agent autorisé ou par vidéo automatisée
- Reliée à une clé cryptographique contrôlée par l'usager

Q18. Vos certificats CertifiO sont-ils reconnus en justice ?

Nos certificats respectent le cadre juridique du Québec et du Canada, et certains sont qualifiés sous eIDAS en Europe. Les signatures produites sont :

- Juridiquement opposables
- Reliées à une preuve d'identité vérifiable
- Horodatées à la seconde près
- Scellées par une autorité de certification accréditée

Q19. Quelle est la différence entre CertifiO et les autres signatures électroniques ?

CertifiO s'appuie sur une PKI (infrastructure à clés publiques) certifiée, une preuve de possession de la clé et une identité authentifiée. Contrairement aux signatures "dessinées" ou "cliquées", elle permet une vérification cryptographique après la signature.

5. Infrastructure et cybersécurité

Q20. Avez-vous une politique de sécurité de l'information ?

Oui. Notre politique de sécurité est encadrée et fait l'objet d'audits internes trimestriels et de tests d'intrusion annuels par des firmes spécialisées.

Q21. Que se passe-t-il si un incident de sécurité survient ?

Nous avons un processus rigoureux de réponse aux incidents :

- Détection et confinement rapide
- Notification des clients selon la gravité et la loi applicable
- Registre centralisé et post-mortem systématique
- Engagement de transparence et amélioration continue

Q22. Quels audits subissez-vous annuellement ?

Nous sommes audités sur :

- ISO 9001 : système de gestion de la qualité
- ISO 27001 : système de gestion de la sécurité
- SOC 2 type II : sécurité
- Tests d'intrusion et revues de code par des firmes externes
- Audit eIDAS pour nos services de confiance

Q23. Vos journaux sont-ils admissibles comme preuve en cas de litige ?

Oui. Nos journaux sont :

- Scellés numériquement

- Immuables
- Horodatés par une autorité de temps certifiée.
- Ils sont produits dans un format vérifiable par tiers.

6. Consentement et vie privée

Q24. Comment recueillez-vous le consentement des utilisateurs ?

Nos interfaces incluent des mécanismes explicites de consentement, adaptés à chaque usage. Pour les cas ponctuels, nous utilisons des preuves de consentement journalisées.

Q25. Puis-je exercer mes droits (accès, retrait, rectification…) ?

Oui. Vous ou vos utilisateurs pouvez en tout temps exercer vos droits en nous écrivant. Nous répondons dans les délais légaux prévus (généralement sous 30 jours).

7. Intégration, API et SLA

Q26. Est-ce que vos produits peuvent s'intégrer à nos systèmes existants ?

Oui. Nos produits offrent des API sécurisées, une documentation technique complète, et des connecteurs avec des systèmes tiers.

Q27. Proposez-vous des contrats de niveau de service (SLA) ?

Oui. En plus des SLA disponibles sur notre site web, nos ententes de service particulières peuvent inclure des SLA garantis pour la disponibilité, les temps de réponse et le support.

Q28. Offrez-vous des preuves juridiques en cas de litige ?

Oui. Nous sommes en mesure de fournir des preuves techniques, documents d'horodatage et relevés de transactions certifiés, à la demande d'un tribunal ou d'un arbitre.

8. À propos des utilisateurs finaux

Q29. Comment vos services protègent-ils les utilisateurs vulnérables ?

Nous portons une attention particulière à la clarté des interfaces, au langage simple, aux alternatives non biométriques lorsque requis, et à la possibilité de retrait ou de refus sans coercition.

9. Gouvernance et conformité

Q30. Avez-vous un Responsable de la protection des renseignements personnels (RPRP) ?

Oui. Notre RPRP supervise la conformité à la Loi 25, aux lois canadiennes et internationales. Il agit comme point de contact pour tout exercice de droits ou enquête réglementaire.

Q31. Avez-vous des chartes de comité ou un programme de gouvernance ?

Oui. Notre programme ISO/SOC2 repose sur :

- Des comités internes (sécurité & conformité, produit)
- Des revues de direction
- Un cycle de planification stratégique basé sur l'analyse de risque
- Des indicateurs qualité et KPIs de sécurité suivis chaque mois

10. Conformité et auditabilité

Q32. Êtes-vous certifiés ou audités par des tiers indépendants ?

Oui. Nos pratiques sont vérifiées régulièrement, incluant :

- ISO/IEC 27001 : gestion de la sécurité de l'information
- SOC 2 Type II : sécurité, confidentialité, intégrité
- ISO 9001 : gestion de la qualité
- eIDAS : pour nos certificats et processus de vérification de l'identité
- Nous partageons les résultats de ces audits (ou leur synthèse) avec nos clients sur demande et sous certaines conditions.

Q33. Vos politiques de sécurité sont-elles accessibles à vos clients ?

Nos politiques internes sont confidentielles, mais nous fournissons sur demande un sommaire exécutif ou une table des matières des politiques clés, ainsi que des preuves de conformité.

Q34. Avez-vous souscrit à une assurance cybersécurité ?

Oui. Nous détenons des polices d'assurance couvrant les risques liés aux incidents de sécurité, fuites, erreurs humaines, pertes de données et interruptions de services.

Q35. Vos systèmes sont-ils auditables ?

Oui. Tous les événements critiques (authentification, signature, consentement) sont journalisés avec horodatage dans des journaux inviolables. Ces traces peuvent être utilisées pour des fins de preuve ou d'audit.

Q36. Puis-je auditer vos pratiques ou demander une preuve de conformité ?

Absolument. Nous partageons sur demande :

- Résumés exécutifs de nos rapports d'audit ou preuves de nos certifications (SOC 2, ISO…)
- Registres de traitement
- Évaluations des risques et des impacts (PIA)
- Politiques encadrantes (sous NDA si nécessaire)

11. Incidents, litiges et antécédents

Q37. Avez-vous subi des incidents de sécurité récents ?

Non. Aucun incident matériel ou significatif n'a été enregistré dans les 24 derniers mois. Notre processus de détection et de réponse a démontré son efficacité.

Q38. Avez-vous été visés par des enquêtes gouvernementales, plaintes ou audits externes en matière de protection des données ?

Non, aucun cas n'a été enregistré dans les 24 derniers mois. Nous collaborerons pleinement avec les autorités en cas de demande.

Date de publication : 2025-07-04

Avis de non-responsabilité