FACSTOX

Politique de Confidentialité

Version 1.0.0 En vigueur le 11/05/2026

□DOCUMENT EN COURS DE RÉDACTION — BROUILLON v1.0

Ce document est un projet soumis à la validation d'un avocat IT **avant toute mise en production**. Les champs entre crochets ▫ [...] sont des variables à remplir après immatriculation de la SAS.

Date de rédaction : 11/05/2026

Politique de Confidentialité

Version : 1.0 — Date d'effet : à définir

Document RGPD opposable. Acceptation obligatoire à l'inscription.

---

1. Préambule

La présente Politique de Confidentialité décrit les conditions dans lesquelles □ **[NOM_SAS]** (« l'**Éditeur** ») collecte, traite et protège les données à caractère personnel dans le cadre de la fourniture du Service **Facstox**.

L'Éditeur s'engage à respecter le **Règlement (UE) 2016/679** du 27 avril 2016 (« **RGPD** ») et la **loi n° 78-17 du 6 janvier 1978** modifiée, dite « **Informatique et Libertés** ».

---

2. Double rôle de l'Éditeur

L'Éditeur intervient à un double titre :

2.1 Responsable de traitement

L'Éditeur est **responsable de traitement** pour les données personnelles relatives :

- Aux comptes des Utilisateurs (employés ou mandataires du Client) : nom, prénom, email, téléphone, identifiants, journaux de connexion, rôle
- Aux contacts commerciaux (prospects, demandes via formulaire de contact)
- À la facturation du Client (raison sociale, SIREN/SIRET, contacts, factures)

2.2 Sous-traitant

L'Éditeur est **sous-traitant** au sens de l'article 28 du RGPD pour les données personnelles que le Client traite via le Service, notamment :

- Données des clients finaux du Client (BtoB et BtoC)
- Données des fournisseurs du Client
- Données des salariés du Client (si module Planning)

Les modalités de sous-traitance sont précisées dans l'**Accord de Sous-Traitance (DPA)** annexé.

---

3. Données collectées (en tant que responsable de traitement)

Catégorie	Données	Finalité	Base légale	Durée
Identification	Nom, prénom, email, mot de passe (haché)	Création et gestion du compte	Exécution du contrat	Durée du contrat + 1 an
Contact pro	Téléphone, fonction	Support, communication	Intérêt légitime	Durée du contrat + 1 an
Société	Raison sociale, SIREN, SIRET, adresse	Facturation, conformité légale	Obligation légale	10 ans (art. L123-22 C. com)
Connexion	Adresse IP, user-agent, horodatage	Sécurité, traçabilité légale	Intérêt légitime / obligation légale	12 mois
Acceptation contractuelle	IP, horodatage, version, hash document	Preuve légale	Obligation légale	5 ans après fin contrat
Facturation	Factures émises, paiements	Comptabilité, fiscalité	Obligation légale	10 ans
Support	Échanges avec le support	Suivi qualité	Intérêt légitime	3 ans

---

4. Destinataires

Les données sont accessibles aux :

- Personnels habilités de l'Éditeur (tenus à la confidentialité)
- Sous-traitants énumérés à l'article 9
- Autorités publiques sur réquisition légale

Aucune donnée n'est cédée, vendue ou louée à des tiers à des fins commerciales.

---

5. Localisation et transferts

Les données sont hébergées en **Union Européenne** par **OVH SAS** (data centers en France).

Aucun transfert hors UE n'est effectué pour les données techniques. Si un sous-traitant ponctuel implique un tel transfert (par exemple Stripe pour le paiement), il est encadré par les **Clauses Contractuelles Types** approuvées par la Commission européenne (décision 2021/914).

---

6. Sécurité

L'Éditeur met en œuvre des mesures techniques et organisationnelles appropriées au sens de l'article 32 du RGPD :

- Chiffrement TLS 1.2+ pour toutes les communications
- Chiffrement au repos des sauvegardes
- Hachage des mots de passe (algorithme robuste, salage, itérations)
- Contrôle d'accès par rôles (RBAC) et audit des actions sensibles
- Sauvegardes régulières et plan de reprise d'activité
- Tests de sécurité réguliers et veille sur les vulnérabilités
- Formation du personnel à la protection des données
- **Déconnexion automatique** après 30 minutes d'inactivité afin de limiter le risque d'accès non autorisé depuis un poste laissé sans surveillance (mesure de sécurité au sens de l'article 32 du RGPD)

---

7. Droits des personnes

Conformément aux articles 15 à 22 du RGPD, toute personne dispose des droits suivants :

- **Accès** : obtenir la confirmation que des données la concernant sont traitées et en obtenir copie
- **Rectification** : demander la correction de données inexactes
- **Effacement** : demander la suppression dans les cas prévus par le RGPD
- **Limitation** : demander la limitation du traitement dans les cas prévus
- **Portabilité** : recevoir ses données dans un format structuré
- **Opposition** : s'opposer au traitement pour motif légitime
- **Retrait du consentement** : à tout moment lorsque le traitement repose sur le consentement
- **Directives post-mortem** : définir le sort des données après son décès

Ces droits s'exercent par email à □ **[EMAIL_DPO]** ou □ **[EMAIL_CONTACT]**, accompagné d'un justificatif d'identité si nécessaire.

L'Éditeur répond dans un délai d'un mois (prorogeable de deux mois en cas de complexité).

En cas de réponse insatisfaisante, la personne concernée peut introduire une réclamation auprès de la **CNIL** (https://www.cnil.fr).

---

8. Cookies

Le site utilise les cookies suivants :

Cookie	Type	Finalité	Durée
`sessionid`	Strictement nécessaire	Authentification	Session
`csrftoken`	Strictement nécessaire	Sécurité (anti-CSRF)	1 an
Préférences	Fonctionnel	Mémorisation thème, langue	6 mois

Aucun cookie publicitaire ni cookie tiers de mesure d'audience n'est déposé sans consentement préalable. Si des cookies analytiques sont introduits, un bandeau de consentement conforme aux recommandations CNIL sera mis en place.

---

9. Sous-traitants ultérieurs

Les sous-traitants principaux à la date des présentes :

Sous-traitant	Rôle	Pays	Encadrement
OVH SAS	Hébergement	France	Contrat OVH + DPA
Stripe Payments Europe Ltd	Paiement	Irlande (UE) + transferts US (CCT)	DPA Stripe + CCT
□[Prestataire email]	Email transactionnel	□[À préciser]	DPA + CCT si hors UE

La liste à jour est consultable sur □**[URL_SITE]/sous-traitants**.

---

10. Violation de données

En cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, l'Éditeur :

- Notifie la **CNIL** dans un délai de **72 heures** après en avoir pris connaissance
- Informe sans délai les Clients concernés lorsqu'agit en tant que sous-traitant
- Documente la violation, ses effets et les mesures correctives

11. Délégué à la protection des données

L'Éditeur a désigné (le cas échéant) un Délégué à la Protection des Données (DPO) joignable à □ **[EMAIL_DPO]**.

À défaut de désignation formelle, le point de contact RGPD est □**[EMAIL_CONTACT]**.

---

12. Modification de la Politique

L'Éditeur peut faire évoluer la présente Politique. Toute modification substantielle est notifiée 30 jours avant son entrée en vigueur. La date de dernière mise à jour figure en tête du document.

---

13. Contact

Pour toute question relative à la présente Politique : □**[EMAIL_DPO]** ou □**[EMAIL_CONTACT]**.

Document rédigé par [NOM_SAS] — SIREN [en cours d'immatriculation] Éditeur du service Facstox — [URL_SITE]