Security & Compliance Policy

CallCenterRate

Version du 13 mai 2026

---

1. Objet

La présente Security & Compliance Policy décrit les mesures techniques, organisationnelles et opérationnelles mises en œuvre par **Confluent Digital SAS** dans le cadre de l'exploitation de la plateforme SaaS **CallCenterRate**.

Cette politique a pour objectif :

- d'assurer la sécurité des Services ;
- de protéger les données traitées via la plateforme ;
- de renforcer la confidentialité des informations ;
- d'assurer la continuité des Services ;
- de promouvoir une utilisation responsable des technologies d'intelligence artificielle.

---

2. Présentation de la plateforme

CallCenterRate est une plateforme SaaS permettant notamment :

- l'importation d'enregistrements téléphoniques ;
- l'analyse automatisée de conversations ;
- la génération de scores qualité ;
- l'évaluation de conformité à des scripts ;
- la production de rapports et indicateurs ;
- l'utilisation de traitements automatisés et technologies d'intelligence artificielle.

---

3. Principes de sécurité

Confluent Digital SAS applique des mesures de sécurité raisonnables et proportionnées visant à garantir :

- la confidentialité des données ;
- l'intégrité des systèmes ;

- la disponibilité des Services ;
- la résilience des infrastructures ;
- la traçabilité des accès ;
- la limitation des risques de compromission.

---

4. Hébergement et infrastructure

Les Services sont hébergés sur des infrastructures professionnelles disposant de mesures de sécurité adaptées.

Les données sont hébergées prioritairement au sein de l'Union européenne lorsque cela est possible.

Les infrastructures utilisées peuvent notamment inclure :

- hébergement cloud ;
- services de stockage sécurisés ;
- outils de supervision ;
- services de sauvegarde ;
- infrastructures d'intelligence artificielle.

---

5. Contrôle des accès

L'accès aux systèmes et données est limité aux seules personnes habilitées dans le cadre de leurs fonctions.

Les mesures de sécurité peuvent inclure :

- authentification sécurisée ;
- gestion des habilitations ;
- limitation des privilèges ;
- segmentation des accès ;
- renouvellement des identifiants ;
- journalisation des connexions.

Les accès administrateurs sont limités et contrôlés.

---

6. Sécurité des données

Confluent Digital SAS met en œuvre des mesures techniques raisonnables afin de protéger les données contre :

- les accès non autorisés ;
- les pertes ;
- les divulgations ;
- les altérations ;
- les destructions accidentelles ;
- les usages frauduleux.

Les mesures mises en œuvre peuvent inclure :

- chiffrement des flux ;
- sécurisation des API ;
- sauvegardes ;
- contrôle des accès ;
- surveillance des infrastructures ;
- détection d'anomalies ;
- cloisonnement logique des données.

---

7. Sauvegardes et continuité d'activité

Des mécanismes de sauvegarde peuvent être mis en œuvre afin de limiter les risques de perte accidentelle de données.

Toutefois :

- aucun système ne peut garantir un risque zéro ;
- le Client demeure responsable de ses propres sauvegardes et exports.

Confluent Digital SAS met en œuvre des mesures raisonnables visant à assurer la continuité des Services en cas d'incident technique majeur.

---

8. Surveillance et journalisation

Les systèmes peuvent faire l'objet :

- d'une surveillance technique ;
- d'une journalisation des accès ;

- d’une détection d’événements de sécurité ;
- d’un monitoring des performances et incidents.

Les journaux techniques peuvent être utilisés afin :

- d’assurer la sécurité ;
- de diagnostiquer les incidents ;
- d’améliorer les Services ;
- de répondre aux obligations légales.

---

9. Sécurité des développements

Confluent Digital SAS applique des pratiques raisonnables visant à renforcer la sécurité des développements logiciels, notamment :

- séparation des environnements ;
- limitation des accès techniques ;
- contrôle des mises en production ;
- correctifs de sécurité ;
- mises à jour des composants critiques lorsque nécessaire.

---

10. Sous-traitants et services tiers

Confluent Digital SAS peut recourir à des prestataires tiers pour :

- l’hébergement ;
- l’analyse IA ;
- la supervision ;
- l’envoi d’emails ;
- les outils analytiques ;
- les sauvegardes ;
- la sécurité.

Les prestataires sont sélectionnés selon des critères raisonnables de sécurité et de conformité.

Toutefois, Confluent Digital SAS ne peut garantir l’absence totale d’incident affectant des services tiers.

---

11. Gestion des incidents de sécurité

Confluent Digital SAS met en œuvre des procédures internes visant à :

- détecter les incidents ;
- limiter leur impact ;
- restaurer les Services ;
- notifier les violations de données lorsque la réglementation l'exige.

En cas de violation de données personnelles, les notifications seront réalisées conformément au RGPD.

---

12. Confidentialité

Les collaborateurs et prestataires habilités à accéder aux données sont soumis à des obligations de confidentialité appropriées.

Les accès aux données sont limités aux besoins strictement nécessaires à l'exécution des Services.

---

13. Protection des données personnelles

Les traitements de données personnelles réalisés via la plateforme sont encadrés :

- par le RGPD ;
- par les Conditions Générales de Vente ;
- par le DPA (Data Processing Agreement) ;
- par la Politique de Confidentialité.

Le Client demeure responsable :

- de la licéité des données importées ;
- des obligations d'information ;
- des consentements nécessaires ;
- du respect des réglementations applicables.

Pour toute question relative aux données personnelles : dpo@confluent-digital.com ou par courrier 15 rue des cuirassiers 69003 Lyon France

14. Intelligence artificielle et sécurité

Certaines fonctionnalités de CallCenterRate reposent sur des technologies d'intelligence artificielle.

Confluent Digital SAS met en œuvre des mesures raisonnables afin :

- de limiter les risques d'accès non autorisé ;
- de protéger les données traitées ;
- d'encadrer les traitements automatisés ;
- de réduire les risques de biais ou d'usage inapproprié.

Toutefois :

- les traitements automatisés peuvent comporter des erreurs ;
- les résultats doivent faire l'objet d'une validation humaine ;
- aucune décision sensible ne doit être prise exclusivement sur la base des résultats générés.

---

15. Responsabilité du Client

Le Client demeure responsable :

- de la gestion de ses accès utilisateurs ;
- de la confidentialité de ses identifiants ;
- de la sécurité de ses équipements ;
- des données importées ;
- de ses propres sauvegardes ;
- du respect des obligations réglementaires applicables.

Le Client s'engage à signaler sans délai toute suspicion :

- d'accès frauduleux ;
- de compromission ;
- d'usage abusif ;
- ou d'incident de sécurité.

---

16. Limitation de garantie

Confluent Digital SAS met en œuvre des moyens raisonnables afin d'assurer la sécurité des Services.

Toutefois :

- aucun système informatique ne peut garantir une sécurité absolue ;
- aucune garantie d'absence totale de vulnérabilité ne peut être fournie ;
- les Services sont fournis selon une obligation générale de moyens.

---

17. Évolutions de la politique

La présente Security & Compliance Policy peut être modifiée à tout moment afin :

- de tenir compte des évolutions techniques ;
- des évolutions réglementaires ;
- ou des améliorations des Services.

---

18. Contact

Pour toute question relative à la sécurité ou à la conformité :

contact@confluent-digital.com

---

19. Droit applicable

La présente politique est soumise au droit français.

Tout litige relatif à son interprétation ou son exécution relève des juridictions françaises compétentes.