Registre de Traitement des Données concernant le service Airlaps

IDENTIFICATION DU TRAITEMENT

Nom du traitement	Gestion du temps de travail via l'application Airlaps
Responsable du traitement	Colabl France SAS
Représentant	FRETAY Adrian
Délégué à la protection des données	Fretay Adrian

FINALITÉS DU TRAITEMENT

Le traitement des données personnelles dans le cadre de l'utilisation de l'application Airlaps poursuit les finalités suivantes :

Suivi et gestion du temps de travail des salariés :
- Enregistrement précis des heures d'entrée et de sortie
- Calcul automatique du temps de travail effectif
- Suivi des pauses et des temps de repos
- Détection des anomalies de pointage

Optimisation de la gestion des ressources humaines :
- Suivi de la charge de travail

Gestion des absences :
- Enregistrement des absences (maladie, formation, etc.)

Conformité avec les obligations légales en matière de droit du travail :
- Respect des durées maximales de travail
- Gestion des heures supplémentaires
- Fourniture de preuves en cas de contrôle (inspection du travail, URSSAF)

Sécurisation des accès et prévention de la fraude :
- Authentification sécurisée des utilisateurs
- Traçabilité des connexions et des actions
- Détection des tentatives d'usurpation d'identité

Génération de rapports d'activité :
- Production de rapports hebdomadaires et mensuels sur le temps de travail
- Fourniture d'outils de visualisation pour les managers et les ressources humaines

Ces finalités sont mises en œuvre dans le strict respect du principe de minimisation des données, en ne collectant et en ne traitant que les informations strictement nécessaires à la réalisation de ces objectifs.

BASE LÉGALE DU TRAITEMENT

Le traitement des données personnelles dans le cadre de l'utilisation de l'application Airlaps repose sur plusieurs bases légales, conformément aux exigences du Règlement Général sur la Protection des Données (RGPD) :

1. Exécution du contrat de travail (Article 6.1.b du RGPD).
Le traitement est nécessaire à l'exécution du contrat de travail entre l'employeur et le salarié. Cela inclut : - L'enregistrement et le suivi du temps de travail, élément essentiel du contrat de travail - La gestion des congés et des absences, conformément aux dispositions contractuelles - Le calcul de la rémunération basée sur le temps de travail effectif - La fourniture d'outils nécessaires à l'exécution des tâches professionnelles, dont l'application de pointage

2. Respect des obligations légales en matière de droit du travail (Article 6.1.c du RGPD).
Le traitement est nécessaire au respect des obligations légales auxquelles l'employeur est soumis, notamment : - L'obligation de suivi du temps de travail (Article L3171-4 du Code du travail) - Le respect des durées maximales de travail et des temps de repos (Articles L3121-18 et suivants du Code du travail) - La tenue d'un registre unique du personnel (Article L1221-13 du Code du travail) - La conservation des données de paie et de temps de travail pour les contrôles administratifs (URSSAF, inspection du travail) - La mise en place du droit à la déconnexion (Article L2242-17 du Code du travail)

3. Intérêt légitime de l'employeur à organiser et gérer le temps de travail (Article 6.1.f du RGPD).

Certains aspects du traitement sont basés sur l'intérêt légitime de l'employeur, après une évaluation minutieuse de la balance entre cet intérêt et les droits et libertés fondamentaux des salariés. Cela comprend :
- L'optimisation de la gestion des ressources humaines et de la planification des équipes
- La prévention de la fraude liée au pointage

4. Consentement (Article 6.1.a du RGPD).

Bien que non systématiquement requis pour les traitements mentionnés ci-dessus, le consentement explicite du salarié peut être demandé pour certaines fonctionnalités spécifiques, telles que :
- La participation à des enquêtes de satisfaction ou des programmes d'amélioration optionnels

Il est important de noter que l'utilisation de ces bases légales est soumise au principe de proportionnalité. L'employeur s'engage à ne collecter et traiter que les données strictement nécessaires à la réalisation des finalités déclarées, dans le respect des droits et libertés des salariés. Une analyse d'impact relative à la protection des données (AIPD) peut être réalisée pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

CATÉGORIES DE DONNÉES TRAITÉES

- Données d'identification : nom, prénom, adresse email (professionnelle ou personnelle), numéro de téléphone (professionnel ou personnelle)
- Données de pointage : heures d'entrée et de sortie d'activité, pauses, temps de travail effectif
- Données d'authentification : code PIN crypté, certificat X.509
- Données de signature électronique :
    - Certificat de signature électronique avancée X.509
    - Clé privée associée au certificat (stockée de manière sécurisée)
    - Données de validation du certificat (date d'émission, date d'expiration, statut de révocation)
    - Empreintes numériques des documents signés
    - Horodatages des signatures

CATÉGORIES DE PERSONNES CONCERNÉES

Le traitement des données personnelles dans le cadre de l'utilisation de l'application Airlaps concerne plusieurs catégories de personnes au sein de l'entreprise :

1. Salariés permanents de l'entreprise :
- Employés à temps plein
- Employés à temps partiel
- Cadres et non-cadres
- Personnel administratif
- Personnel opérationnel
- Télétravailleurs
- Salariés en période d'essai

2. Intérimaires :
- Travailleurs temporaires mis à disposition par des agences d'intérim
- Intérimaires en contrat de mission
- Intérimaires en contrat à durée indéterminée intérimaire (CDI-I)

3. Stagiaires :
- Stagiaires conventionnés
- Stagiaires en alternance (contrats d'apprentissage et de professionnalisation)
- Stagiaires en observation ou découverte

4. Autres catégories (le cas échéant) :
- Consultants externes travaillant sur site
- Prestataires de services réguliers
- Salariés détachés ou mis à disposition
- Dirigeants et mandataires sociaux salariés

5. Utilisateurs spécifiques :
- Administrateurs du système Airlaps
- Gestionnaires des ressources humaines
- Managers et superviseurs ayant accès aux données de leurs équipes

Il est important de noter que le traitement des données peut varier selon la catégorie de personnes concernées, en fonction de leur statut, de leur niveau de responsabilité et des exigences légales spécifiques à chaque catégorie. L'entreprise s'engage à appliquer les principes de minimisation des données et de proportionnalité, en ne collectant et en ne traitant que les informations strictement nécessaires pour chaque catégorie de personnes concernées, dans le respect de leurs droits et de la réglementation en vigueur.

DESTINATAIRES DES DONNÉES

Les données personnelles collectées et traitées dans le cadre de l'utilisation de l'application Airlaps sont accessibles uniquement aux destinataires suivants, dans la limite de leurs attributions respectives et du besoin d'en connaître :

1. Personnel habilité de l'entreprise :
a) Service des Ressources Humaines :
- Gestionnaires RH chargés de l'administration du personnel
- Responsables de la paie pour le calcul des rémunérations
- Chargés de formation pour la gestion des temps de formation

b) Managers et superviseurs directs :
- Pour la validation des temps de travail et des congés
- Pour la gestion des plannings et l'organisation du travail

c) Direction :
- Pour l'analyse globale des données d'activité et la prise de décisions stratégiques

d) Service informatique :
- Administrateurs système pour la maintenance et la sécurité de l'application

e) Représentants du personnel (le cas échéant) :
- Dans le cadre de leurs missions légales et conventionnelles

2. Prestataire Airlaps (COLABL FRANCE) :
- Équipe de développement pour la maintenance et l'amélioration du service
- Support technique pour la résolution des problèmes signalés par les utilisateurs
- Équipe de sécurité pour la protection des données et la prévention des fraudes
- Administrateurs système pour la gestion de l'infrastructure cloud
- Service client pour l'assistance aux entreprises clientes

3. Sous-traitants d'Airlaps :
a) SAS NDA Media : pour l'envoi de SMS d'authentification (TOTP)
b) OVH et Amazon Web Services EMEA SARL : pour l'hébergement et l'infrastructure cloud
c) Mailgun Technologies, Inc. : pour l'envoi d'emails liés au service

4. Autorités compétentes en cas de contrôle :
- Inspection du travail dans le cadre de ses missions de contrôle
- URSSAF pour la vérification des déclarations sociales
- Administration fiscale en cas de contrôle fiscal
- Tribunaux et auxiliaires de justice en cas de litige

5. Auditeurs externes :
- Commissaires aux comptes dans le cadre de leur mission légale
- Organismes de certification pour les audits de conformité (ex : ISO 27001)

6. Tiers autorisés :
- Experts-comptables de l'entreprise pour l'établissement des états financiers
- Avocats en cas de contentieux lié au temps de travail

L'accès aux données est strictement encadré et limité aux seules informations nécessaires à l'accomplissement des missions de chaque destinataire. Des mesures techniques et organisationnelles sont mises en place pour garantir la confidentialité et la sécurité des données, notamment :

- Politique de gestion des droits d'accès basée sur le principe du moindre privilège
- Journalisation des accès et des actions effectuées sur les données
- Engagement de confidentialité signé par tous les destinataires ayant accès aux données
- Chiffrement des données en transit et au repos
- Formation régulière des utilisateurs aux bonnes pratiques de sécurité et de protection des données

Tout transfert de données à des tiers non mentionnés ci-dessus nécessitera le consentement préalable de l'entreprise cliente et/ou des personnes concernées, sauf obligation légale.

TRANSFERTS DE DONNÉES HORS UE

Les données sont hébergées sur les serveurs de la société OVH en Union Européenne. En cas de transfert hors UE (ex: support technique), des garanties appropriées sont mises en place (clauses contractuelles types de la Commission européenne).

DURÉE DE CONSERVATION DES DONNÉES

Airlaps applique une politique de conservation des données stricte, conforme aux obligations légales et au principe de minimisation des données du RGPD. Les durées de conservation sont définies comme suit :

1. Données de pointage et rapports d'activité :
- Durée de conservation : 5 ans à compter de leur enregistrement
- Base légale : Article L3171-3 du Code du travail et Article L243-16 du Code de la sécurité sociale
- Détails :
  - Heures de début et de fin de journée
  - Pauses et temps de repos
  - Absences et leurs motifs
  - Rapports hebdomadaires et mensuels générés

2. Données du compte utilisateur :
- Durée de conservation : Durée du contrat de travail + 5 ans
- Base légale : Prescription quinquennale en matière de salaires (Article L3245-1 du Code du travail)
- Détails :
  - Informations d'identification (nom, prénom, email professionnel)
  - Historique des modifications du compte

3. Logs de connexion :
- Durée de conservation : 1 an
- Base légale : Article 6 II de la LCEN (Loi pour la Confiance dans l'Économie Numérique)
- Détails :
  - Dates et heures de connexion
  - Adresses IP utilisées
  - Actions effectuées sur l'application

4. Données de signature électronique :
- Durée de conservation : 7 ans après l'expiration ou la révocation du certificat
- Base légale : Règlement eIDAS (UE) n° 910/2014, Article 24, paragraphe 2, point h
- Détails :
  - Certificats X.509
  - Clés publiques associées
  - Historique des signatures effectuées

6. Données relatives aux absences :
- Durée de conservation : Année en cours + 5 ans
- Base légale : Prescription quinquennale en matière de congés payés (Article L3245-1 du Code du travail)

7. Données d'authentification :
- Durée de conservation : Jusqu'à la suppression du compte + 3 mois
- Base légale : Intérêt légitime (sécurité du système)
- Détails :
  - Codes PIN cryptés
  - Tokens d'authentification

À l'issue de ces périodes de conservation, les données sont soit supprimées de manière sécurisée, soit anonymisées pour des fins statistiques, conformément aux recommandations de la CNIL.

Procédure d'archivage et de suppression :
- Les données sont d'abord archivées dans un espace de stockage sécurisé à accès limité.
- Une procédure automatisée vérifie quotidiennement les données ayant atteint leur durée de conservation maximale.
- Les données concernées sont ensuite supprimées de manière irréversible ou anonymisées.
- Un journal d'audit de ces opérations est maintenu pour assurer la traçabilité du processus.

MESURES DE SÉCURITÉ

Airlaps met en œuvre un ensemble complet de mesures de sécurité pour protéger les données des utilisateurs et garantir l'intégrité du système de pointage et de signature électronique. Ces mesures comprennent :

1. Authentification forte à deux facteurs (2FA) :
   - Utilisation d'un système TOTP (Time-Based One-Time Password) pour la génération de mots de passe à usage unique.
   - Vérification du numéro de téléphone de l'utilisateur lors de l'inscription.
   - Liaison du compte utilisateur à un appareil physique spécifique pour prévenir la signature électronique non autorisée.

2. Chiffrement des données :
   - Utilisation de SSL/TLS pour sécuriser toutes les communications entre le client et l'API.
   - Chiffrement des données au repos dans les bases de données et les systèmes de stockage.
   - Couche supplémentaire de chiffrement pour les données sensibles avant le transfert vers le système de signature.

3. Protocole SRP-6a (Secure Remote Password) :
- Implémentation du protocole SRP-6a pour la gestion sécurisée des codes PIN.
- Authentification mutuelle entre le client et le serveur sans transmission du mot de passe sur le réseau.
- Calcul complexe de preuves cryptographiques pour valider l'authenticité de l'utilisateur.

4. Stockage sécurisé des clés privées :
- Chiffrement automatique de toutes les informations des clés privées des certificats X.509.
- Contrôle d'accès granulaire et journaux d'audit détaillés pour surveiller l'accès aux informations sensibles.

5. Blockchain privée pour l'enregistrement des signatures et certificats :
- Utilisation d'une blockchain privée pour garantir l'immuabilité des signatures électroniques et des certificats.
- Processus de vérification en bloc pour confirmer l'intégrité de chaque nouveau bloc ajouté à la chaîne.
- Système de validation pour vérifier l'authenticité et la validité des documents signés et des certificats.

6. Contrôles d'accès et journalisation :
- Mise en place de politiques d'accès basées sur le principe du moindre privilège.
- Journalisation détaillée de toutes les actions effectuées sur le système, y compris les accès et les modifications.
- Surveillance en temps réel des activités suspectes et des tentatives d'accès non autorisées.

7. Gestion des tokens d'authentification :
- Utilisation de Bearer Tokens pour sécuriser les échanges entre les clients et l'API.
- Politiques strictes concernant la durée de vie des tokens, avec renouvellement régulier.
- Invalidation immédiate des tokens en cas de déconnexion ou d'activité suspecte.

8. Signature électronique avancée :
- Implémentation du format PAdES-Baseline-B pour les signatures électroniques, conforme aux normes eIDAS.
- Génération et gestion sécurisée des certificats X.509 pour chaque utilisateur.
- Processus de signature incluant la vérification de l'intégrité du document et l'authentification du signataire.

9. Vérification de l'authenticité des documents :
- Outil de vérification en ligne permettant aux utilisateurs de confirmer l'authenticité des documents signés.
- Analyse des signatures utilisant les données de la blockchain pour valider leur intégrité.

10. Mises à jour et maintenance :
- Mises à jour régulières de sécurité pour corriger les vulnérabilités potentielles.
- Audits de sécurité périodiques pour identifier et corriger les failles potentielles.
- Veille technologique continue pour adapter les mesures de sécurité aux nouvelles menaces.

11. Formation et sensibilisation :
- Programmes de formation réguliers pour les employés d'Airlaps sur les meilleures pratiques de sécurité.
- Guides et documentation pour les utilisateurs finaux sur l'utilisation sécurisée de l'application.

Ces mesures de sécurité sont constamment évaluées et mises à jour pour garantir le plus haut niveau de protection des données et l'intégrité du système Airlaps, en conformité avec les réglementations en vigueur et les meilleures pratiques de l'industrie.

DROITS DES PERSONNES CONCERNÉES

Les salariés disposent des droits suivants en vertu du Règlement Général sur la Protection des Données :
- Droit d'accès : obtenir une copie de leurs données personnelles traitées.
- Droit de rectification : corriger ou compléter les données inexactes ou incomplètes.
- Droit à l'effacement (droit à l'oubli) : demander la suppression de leurs données, dans les limites des obligations légales de conservation.
- Droit à la limitation du traitement : restreindre le traitement de leurs données dans certaines circonstances.
- Droit à la portabilité des données : recevoir leurs données dans un format structuré et les transmettre à un autre responsable de traitement.
- Droit d'opposition : s'opposer au traitement de leurs données, notamment pour les traitements basés sur l'intérêt légitime de l'entreprise.

Pour exercer ces droits, les salariés peuvent s'adresser :

- Au service des Ressources Humaines de l'entreprise
- Au Délégué à la Protection des Données (DPO) désigné, le cas échéant
- À COLABL FRANCE (Airlaps), en tant que sous-traitant, via l'adresse dpo@airlaps.com

En cas de difficulté pour exercer leurs droits auprès des sous-traitants, les salariés peuvent utiliser l'outil mis à disposition par l'association allemande ***Datenfragen.de e. V***. : https://www.demandetesdonnees.fr/

L'entreprise s'engage à traiter les demandes dans un délai d'un mois, conformément aux exigences du RGPD.

SOUS-TRAITANTS

COLABL FRANCE (Airlaps) SIRET : 953 740 743 00026 - RCS SAINT-ETIENNE Siège social : 83 A rue des alliés, 42100 Saint-Etienne – France Tél. : +33 (0)4 28 04 47 20	Fournisseur principal de la solution de gestion du temps de travail, COLABL FRANCE, opérant sous le nom commercial Airlaps, est le prestataire principal fournissant la solution complète de gestion du temps de travail. Ses responsabilités incluent : - Développement, maintenance et mise à jour de l'application Airlaps - Gestion de l'infrastructure technique nécessaire au fonctionnement du service - Traitement et stockage sécurisés des données de pointage et des informations utilisateurs - Mise en place des mécanismes de signature électronique avancée - Support technique et assistance aux clients - Garantie de la conformité du service avec les réglementations en vigueur, notamment le RGPD et les normes eIDAS
SAS NDA Media SIRET : 805 010 386 00011 – RCS PARIS Siège social : 30 rue de Saint-Pétersbourg, 75008 Paris – France Tél. : + 33 (0)1 85 09 27	Envoi de SMS pour l'authentification à deux facteurs (TOTP). NDA Media est chargé de l'envoi des SMS contenant les codes TOTP (Time-Based One-Time Password) utilisés pour l'authentification à deux facteurs. Ses responsabilités spécifiques comprennent : - L'envoi sécurisés des codes TOTP uniques - Garantie de la livraison rapide et fiable des SMS d'authentification - Maintien d'une infrastructure sécurisée pour la gestion des numéros de téléphone et l'envoi des messages - Respect des normes de protection des données dans le traitement des numéros de téléphone
OVH SIRET : 424 761 419 00045 - RCS LILLE Siège social : 2 rue Kellermann 59100 Roubaix – France Tél. : 1007	Hébergement et infrastructure cloud pour les services principaux. OVH fournit l'infrastructure cloud principale pour l'hébergement de l'application Airlaps. Ses responsabilités incluent : - Mise à disposition de serveurs sécurisés pour l'hébergement de l'application et des bases de données - Garantie de la haute disponibilité et de la performance du service - Fourniture de solutions de sauvegarde et de reprise après sinistre - Mise en place de mesures de sécurité physiques et logiques pour protéger l'infrastructure - Conformité avec les normes de sécurité et de protection des données européennes
AMAZON WEB SERVICES EMEA SARL SIRET : 831 001 334 00018 – RCS Nanterre Siège social : 38 Avenue John F. Kennedy 1855 Luxembourg – Luxembourg Email: aws-EU-privacy@amazon.com	Hébergement et infrastructure cloud spécifique à la signature électronique. AWS fournit une infrastructure cloud dédiée pour les composants liés à la signature électronique. Ses responsabilités spécifiques comprennent : - Fourniture de services de les clés cryptographiques (HMS)
Mailgun Technologies, Inc. 112 E Pecan St #1135 San Antonio	Gestion et envoi des communications par email. Mailgun est responsable de l'envoi des emails liés au service Airlaps. Ses responsabilités détaillées incluent :

TX 78205 United States of America Email : privacy@mailgun.com	- Envoi sécurisé et fiable des emails de notification, de confirmation et d'alerte aux utilisateurs - Gestion des listes de diffusion et respect des préférences de communication des utilisateurs - Suivi et analyse des taux de livraison et d'ouverture des emails pour optimiser la communication - Mise en place de mécanismes anti-spam et de sécurité pour protéger les adresses email des utilisateurs - Conformité avec les réglementations sur la protection des données et le marketing par email

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

Bien qu'une Analyse d'Impact relative à la Protection des Données (AIPD) complète ne soit pas requise pour le traitement des données dans le cadre de l'utilisation de l'application Airlaps, nous avons néanmoins procédé à une évaluation approfondie des risques potentiels. Cette démarche s'inscrit dans notre engagement à assurer le plus haut niveau de protection des données personnelles et à respecter pleinement les principes du RGPD.

1. Évaluation de la nécessité d'une AIPD :

Conformément aux lignes directrices du Comité Européen de la Protection des Données (CEPD) et aux recommandations de la CNIL, nous avons évalué la nécessité d'une AIPD en considérant les critères suivants :

a) Nature des données traitées : Les données traitées sont principalement des données professionnelles et de pointage, qui ne sont pas considérées comme des données sensibles au sens de l'article 9 du RGPD.

b) Échelle du traitement : Bien que le traitement concerne potentiellement un grand nombre d'employés, il reste limité au contexte professionnel et n'implique pas de traitement à grande échelle de données sensibles.

c) Utilisation de nouvelles technologies : L'application Airlaps utilise des technologies avancées comme la blockchain privée et la signature électronique, mais ces technologies sont mises en œuvre avec des garanties de sécurité robustes.

d) Évaluation ou notation : Le traitement n'implique pas d'évaluation systématique et approfondie d'aspects personnels.

e) Prise de décision automatisée : Le système ne prend pas de décisions automatisées produisant des effets juridiques ou similaires.

f) Surveillance systématique : Bien que le système enregistre les temps de travail, il ne constitue pas une surveillance systématique à grande échelle.

2. Mesures de protection mises en place :

Malgré l'absence de nécessité d'une AIPD complète, Airlaps a mis en place plusieurs mesures pour atténuer les risques potentiels :

a) Chiffrement robuste : Utilisation de protocoles de chiffrement avancés pour protéger les données en transit et au repos.

b) Authentification forte : Mise en place d'une authentification à deux facteurs et utilisation du protocole SRP-6a pour la gestion sécurisée des codes PIN.

c) Contrôle d'accès granulaire : Mise en œuvre de politiques d'accès basées sur le principe du moindre privilège.

d) Journalisation et audit : Enregistrement détaillé de toutes les actions effectuées sur le système pour détecter toute activité suspecte.

e) Protection des données par conception : Intégration des principes de protection des données dès la conception de l'application.

3. Surveillance continue et réévaluation :

Bien qu'une AIPD complète ne soit pas requise actuellement, Airlaps s'engage à :

a) Surveiller en permanence l'évolution des risques liés au traitement des données.

b) Réévaluer régulièrement la nécessité d'une AIPD, notamment en cas de modifications significatives du traitement ou de l'environnement réglementaire.

c) Effectuer des audits de sécurité périodiques pour s'assurer de l'efficacité des mesures de protection mises en place.

d) Maintenir une documentation détaillée sur les pratiques de protection des données, facilitant ainsi la démonstration de conformité en cas de contrôle.

MESURES POUR ASSURER LA CONFORMITÉ

Airlaps met en œuvre un ensemble complet de mesures pour garantir et maintenir la conformité avec le RGPD et les autres réglementations applicables en matière de protection des données. Ces mesures visent à créer une culture de la conformité et à assurer une vigilance continue dans la protection des données personnelles.

1. Formation régulière des utilisateurs sur la protection des données :
   - Programme de formation initiale obligatoire pour tous les nouveaux employés d'Airlaps et des entreprises clientes.
   - Sessions de mise à jour trimestrielles sur les évolutions réglementaires et les bonnes pratiques.
   - Modules e-learning interactifs couvrant les principes du RGPD, la sécurité des données et les procédures spécifiques à Airlaps.
   - Ateliers pratiques sur la gestion des incidents de sécurité et l'exercice des droits des personnes concernées.
   - Évaluations régulières des connaissances des employés avec suivi des résultats.

2. Audits internes périodiques de conformité :
   - Audits trimestriels des processus de traitement des données, incluant la vérification des accès, des durées de conservation et des mesures de sécurité.
   - Revue annuelle complète de la conformité RGPD, couvrant tous les aspects du traitement des données.
   - Utilisation d'outils automatisés pour surveiller en continu les accès aux données et détecter les anomalies.
   - Évaluation régulière de l'efficacité des mesures techniques et organisationnelles mises en place.
   - Collaboration avec des experts externes pour des audits indépendants bisannuels.

3. Mise à jour régulière du registre de traitement :
   - Révision mensuelle du registre pour refléter tout changement dans les processus de traitement.
   - Procédure formelle pour documenter et approuver toute modification des activités de traitement.
   - Intégration automatique des mises à jour du registre dans le système de gestion de la conformité d'Airlaps.
   - Vérification trimestrielle de l'exactitude et de l'exhaustivité du registre par le DPO.
   - Rapport annuel sur l'évolution du registre de traitement présenté à la direction.

4. Procédure de notification en cas de violation de données :
   - Protocole détaillé pour la détection, l'évaluation et la notification des violations de données.
   - Formation spécifique pour l'équipe de réponse aux incidents sur la gestion des violations de données.
   - Système d'alerte 24/7 pour signaler les incidents potentiels.
   - Processus de triage rapide pour évaluer la gravité des violations et déterminer la nécessité de notification.
   - Modèles préétablis pour la notification aux autorités de contrôle et aux personnes concernées.
   - Exercices de simulation de violation de données biannuels pour tester l'efficacité de la procédure.

5. Gestion des sous-traitants :
   - Évaluation rigoureuse de la conformité RGPD des sous-traitants avant tout engagement.
   - Clauses contractuelles détaillées sur la protection des données dans tous les contrats avec les sous-traitants.
   - Audits réguliers des pratiques de protection des données des sous-traitants.
   - Procédure de validation pour tout transfert de données hors UE, incluant la vérification des garanties appropriées.

6. Mise en œuvre de la protection des données dès la conception et par défaut :
   - Intégration systématique des principes de protection des données dans le développement de nouvelles fonctionnalités.
   - Réalisation d'analyses d'impact sur la protection des données (AIPD) pour tout nouveau traitement à risque élevé.

- Paramètres de confidentialité par défaut les plus restrictifs pour toutes les fonctionnalités de l'application.

7. Gestion des droits des personnes concernées :
- Procédure claire et accessible pour l'exercice des droits RGPD (accès, rectification, effacement, etc.).
- Système automatisé pour traiter les demandes d'exercice des droits dans les délais légaux.
- Formation spécifique du personnel de support client sur la gestion des demandes liées aux droits RGPD.

8. Veille réglementaire et adaptation continue :
- Suivi constant des évolutions législatives et jurisprudentielles en matière de protection des données.
- Participation active aux groupes de travail et associations professionnelles du secteur.
- Processus d'adaptation rapide des pratiques et de l'application en fonction des nouvelles exigences réglementaires.

9. Documentation et traçabilité :
- Maintien d'une documentation exhaustive sur toutes les mesures de conformité mises en place.
- Journalisation détaillée de toutes les activités liées au traitement des données personnelles.
- Système de gestion des versions pour suivre l'évolution des politiques et procédures de protection des données.

10. Revue et amélioration continue :
- Comité de gouvernance des données se réunissant mensuellement pour évaluer l'efficacité des mesures de conformité.
- Processus d'amélioration continue basé sur les retours d'expérience, les résultats d'audit et les évolutions technologiques.
- Révision annuelle de la stratégie globale de conformité en matière de protection des données.

PROCÉDURE D'EXERCICE DES DROITS

Airlaps s'engage à faciliter l'exercice des droits des personnes concernées conformément au Règlement Général sur la Protection des Données (RGPD). La procédure suivante a été mise en place pour garantir une gestion efficace et transparente des demandes d'exercice des droits :

1. Moyens de contact :
Les salariés peuvent exercer leurs droits par deux moyens principaux :
a) Par email : en contactant directement le Délégué à la Protection des Données (DPO) à l'adresse dpo@airlaps.com
b) Par courrier postal : en envoyant une demande écrite à l'adresse suivante :
SERVICE JURIDIQUE,
COLABL FRANCE SAS,
83 A RUE DES ALLIES, 42100 SAINT-ETIENNE

2. Identification du demandeur :
Pour garantir la sécurité et la confidentialité des données, une vérification de l'identité du demandeur sera effectuée. Cela peut inclure :
- La fourniture d'une copie d'une pièce d'identité valide
- L'utilisation du système d'authentification à deux facteurs d'Airlaps pour les demandes en ligne

3. Traitement de la demande :
- Un accusé de réception sera envoyé au demandeur dans un délai de 48 heures ouvrables.
- La demande sera traitée par l'équipe dédiée à la protection des données, sous la supervision du DPO.
- Une réponse sera apportée dans un délai maximal d'un mois à compter de la réception de la demande.
- En cas de demande complexe ou de volume important de demandes, ce délai peut être prolongé de deux mois supplémentaires. Dans ce cas, le demandeur en sera informé dans le mois suivant la réception de la demande initiale.

4. Types de droits pouvant être exercés :
- Droit d'accès : obtenir une copie des données personnelles traitées
- Droit de rectification : corriger les données inexactes ou incomplètes
- Droit à l'effacement (droit à l'oubli) : demander la suppression des données dans certaines conditions
- Droit à la limitation du traitement : restreindre le traitement des données dans certains cas
- Droit à la portabilité : recevoir ses données dans un format structuré et les transmettre à un tiers
- Droit d'opposition : s'opposer au traitement des données pour des raisons tenant à sa situation particulière

5. Format de la réponse :
- Les réponses seront fournies par écrit, y compris par voie électronique lorsque cela est approprié.
- Les informations seront fournies dans un format clair, concis et facilement accessible.

6. Gratuité et exceptions :
- L'exercice des droits est gratuit.
- Des frais raisonnables basés sur les coûts administratifs peuvent être demandés pour toute copie supplémentaire ou pour des demandes manifestement infondées ou excessives.

7. Registre des demandes :
- Airlaps tient un registre de toutes les demandes d'exercice des droits, incluant la date de réception, la nature de la demande, les actions entreprises et la date de résolution.

8. Formation du personnel :
- Le personnel d'Airlaps, en particulier l'équipe de support client et le service juridique, est régulièrement formé pour reconnaître et traiter efficacement les demandes d'exercice des droits.

9. Révision et amélioration continue :
- La procédure d'exercice des droits est régulièrement revue et mise à jour pour s'assurer de son efficacité et de sa conformité avec les évolutions réglementaires.

10. Recours :
- En cas d'insatisfaction quant au traitement de leur demande, les personnes concernées sont informées de leur droit de déposer une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

INFORMATION DES PERSONNES CONCERNÉES

Les salariés sont informés du traitement de leurs données via :
- Une mention dans leur contrat de travail
- Une notice d'information RGPD spécifique à l'utilisation d'Airlaps
- L'affichage de la politique de confidentialité dans l'application

Date de création du registre	01/07/2024
Date de dernière mise à jour	01/07/2024