POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES

Conforme au Règlement (UE) 2016/679 (RGPD) et à la loi Informatique et Libertés

Document	Politique de Protection des Données
Version	1.0
Date d'entrée en vigueur	29/10/2026
Rédacteur	Soumaya DRIDI – System & Data manager
Approbateur	Alex LAMBERIO - CEO
Responsable de traitement	Alex LAMBERIO - CEO
DPO désigné	Liliane SANTOS – lsantos@godet.fr

1. Préambule et engagements

La présente politique de protection des données personnelles (ci-après « la Politique ») formalise les engagements de GROUPE GODET (ci-après « l'Entreprise ») en matière de collecte, de traitement et de protection des données à caractère personnel, conformément :

- **Au Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données (RGPD) ;**
- **À la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;**
- **LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles modifiée, notamment par l'ordonnance n° 2018 1125 du 12 décembre 2018 et la loi n° 2018 493 du 20 juin 2018**
- **Aux recommandations et référentiels de la Commission Nationale de l'Informatique et des Libertés (CNIL), et du Comité européen de la protection des données (EDPB).**

L'Entreprise reconnaît que la protection des données personnelles est un droit fondamental. Elle s'engage à traiter les données de manière licite, loyale et transparente, à ne collecter que les données strictement nécessaires, et à les protéger contre tout accès non autorisé, perte ou destruction.

L'Entreprise a désigné un Délégué à la Protection des Données (DPO), dont les coordonnées figurent en page de garde, conformément à l'article 37 du RGPD. Le DPO est l'interlocuteur privilégié de la CNIL et le point de contact interne pour toute question relative à la protection des données personnelles.

2. Champ d'application

La présente Politique s'applique :

- À l'ensemble des salariés de l'Entreprise (CDI, CDD, apprentis, stagiaires, intérimaires) sur l'ensemble des trois sites à Roissy-en-France, Selongey et Saint-Ouen-l'Aumône.
- Aux sous-traitants et prestataires traitant des données pour le compte de l'Entreprise **(sous-traitants au sens de l'article 28 du RGPD) ;**
- À toute personne physique dont l'Entreprise traite les données : salariés, clients, prospects, fournisseurs, visiteurs.

Elle couvre l'ensemble des traitements de données à caractère personnel réalisés par l'Entreprise, qu'ils soient automatisés (logiciels, bases de données) ou manuels (fichiers papier).

3. Gouvernance RGPD – Organisation et responsabilités

3.1 Responsable de traitement

GROUPE GODET, représentée par Alex LAMBERIO, en sa qualité de CEO, est responsable de traitement au sens de l'article 4(7) du RGPD. À ce titre, il détermine les finalités et les moyens des traitements de données réalisés par l'Entreprise.

3.2 Délégué à la Protection des Données (DPO)

L'Entreprise a désigné Liliane SANTOS en qualité de Délégué à la Protection des Données, conformément à l'article 37 du RGPD. **Cette désignation a été notifiée à la CNIL. Le DPO exerce ses missions en toute indépendance, sans recevoir d'instructions quant à l'exercice de ses fonctions, et ne peut être sanctionné pour l'exercice de celles-ci (article 38 du RGPD).**

Missions du DPO (article 39 du RGPD) :

- Informer et conseiller l'Entreprise et ses salariés sur leurs obligations en matière de protection des données ;
- Contrôler le respect du RGPD et de la présente Politique ;
- Conseiller sur les analyses d'impact (AIPD) et en vérifier l'exécution ;
- Coopérer avec la CNIL et être le point de contact de celle-ci ;
- Tenir le registre des activités de traitement à jour.

Contact DPO : Liliane SANTOS – lsantos@godet.fr - 06 07 56 42 46

3.3 Rôles et responsabilités

- **Direction générale :** valide la Politique, alloue les ressources nécessaires à la conformité, arbitre en dernier ressort ;
- **DPO :** pilote la conformité RGPD, tient le registre, traite les demandes de droits, gère les incidents, est l'interlocuteur de la CNIL ;

- **Responsable RH :** référent opérationnel pour les données salariés et médecine du travail, travaille en lien direct avec le DPO ;
- **Responsable commercial :** référent opérationnel pour les données clients et prospects ;
- **Responsable informatique :** garant de la sécurité technique des traitements, gestion des accès et des incidents de sécurité ;
- **Tous les salariés :** respectent la présente Politique et signalent tout incident ou doute au DPO ou à leur responsable.

4. Registre des activités de traitement

Conformément à l'article 30 du RGPD, l'Entreprise tient un registre complet et à jour de l'ensemble de ses activités de traitement, sous la responsabilité du DPO. Le tableau ci-dessous en constitue la synthèse publique. Le registre détaillé est tenu à disposition de la CNIL à tout moment.

Traitement	Finalité	Base légale	Durée de conservation	Destinataires
Gestion de la paie et des salaires	Paiement de la rémunération, déclarations sociales (URSSAF, prévoyance, retrait, épargne salariale, etc)	Obligation légale / Exécution du Contrat de travail	5 ans après départ du salarié	RH, Direction, comptabilité, organismes sociaux, expert-comptable, sous-traitant (conseil, hébergeur informatique, paie, etc)
Gestion RH (recrutement, formation, évaluation)	Gestion administrative du personnel, développement des compétences, élections professionnelles, mise à disposition d'outils de communication et informatique	Contrat / Intérêt légitime / Obligation légale	Durée du contrat + 5 ans (dossier RH)	RH, managers, organismes de formation, service informatique
Pointage et contrôle des accès	Gestion des temps de travail et sécurité des sites	Intérêt légitime / Obligation légale	1 an glissant	RH, responsables de site, Direction
Données de santé – médecine du travail	Suivi médical réglementaire, gestion des AT/MP	Obligation légale	Durée légale (dossier médical - avis d'aptitude/inaptitude, AT/MP : 50 ans min.)	Médecin du travail uniquement (secret médical)

Traitement	Finalité	Base légale	Durée de conservation	Destinataires
Gestion clients et prospects	Exécution des contrats, prospection commerciale	Contrat / Intérêt légitime	Durée du contrat + 3 ans (prospects : 3 ans)	Commercial, direction, traitants logistique
Gestion fournisseurs et sous-traitants	Gestion des achats, suivi des contrats	Contrat / Obligation légale	Durée du contrat + 5 ans	Achats, comptabilité, direction
Vidéosurveillance des sites	Sécurité des biens et des personnes	Intérêt légitime (déclaration préfecture)	1 mois maximum	Direction, responsables de site, forces de l'ordre (si incident)
Journaux informatiques (logs)	Sécurité du système d'information	Intérêt légitime	6 mois glissants	DPO, responsable informatique

Les données de santé (dossiers médicaux, arrêts maladie, AT/MP) constituent des données sensibles au sens de l'article 9 du RGPD. Leur traitement est strictement encadré : seul le médecin du travail peut accéder aux données médicales individuelles. Les données RH (jours d'absence, restrictions médicales) sont strictement séparées des données médicales.

Les Ressources Humaines ne disposent que d'informations strictement nécessaires (aptitude, inaptitude, restrictions d'aménagement de poste, durée des arrêts sans détail médical) ; ces informations sont traitées sur la base des obligations légales en matière de santé et sécurité au travail.

5. Principes fondamentaux applicables aux traitements

5.1 Licéité, loyauté et transparence

Tout traitement de données doit reposer sur l'une des bases légales prévues à l'article 6 du RGPD :

- Le consentement de la personne concernée (révocable à tout moment) ;
- L'exécution d'un contrat auquel la personne est partie ;
- Le respect d'une obligation légale ;
- La sauvegarde des intérêts vitaux ;
- L'exécution d'une mission d'intérêt public ;
- La poursuite des intérêts légitimes de l'Entreprise, sous réserve qu'ils ne prévalent pas sur les droits et libertés des personnes.

Le DPO valide la base légale de tout nouveau traitement avant sa mise en œuvre.

5.2 Limitation des finalités

Les données collectées ne peuvent être utilisées qu'aux fins explicitement définies au moment de la collecte. Toute utilisation secondaire non prévue initialement est soumise à l'avis préalable du DPO, qui réalise une analyse de compatibilité avec la finalité d'origine.

5.3 Minimisation des données

L'Entreprise ne collecte que les données strictement nécessaires à la finalité poursuivie. Avant toute nouvelle collecte ou tout nouveau traitement, une analyse de nécessité est réalisée en lien avec le DPO : « Cette donnée est-elle vraiment indispensable à l'objectif visé ? »

5.4 Exactitude

Les données doivent être exactes et tenues à jour. Des procédures de mise à jour régulière sont en place pour les données salariés (changement d'adresse, situation familiale) et les données clients. Le DPO organise une revue annuelle de la qualité des données.

5.5 Limitation de la conservation

Les données ne sont conservées que le temps nécessaire à la finalité pour laquelle elles ont été collectées, dans le respect des durées légales définies au registre. Passé le délai de conservation, les données sont supprimées ou anonymisées de manière irréversible. Des purges automatiques sont programmées en lien avec le responsable informatique.

5.6 Intégrité et confidentialité

Les données personnelles sont protégées par des mesures techniques et organisationnelles appropriées contre tout accès non autorisé, altération, divulgation ou destruction. Le détail des mesures de sécurité figure à la section 8.

6. Droits des personnes concernées

Conformément aux articles 12 à 22 du RGPD, toute personne dont l'Entreprise traite les données dispose des droits suivants :

Droit	Contenu	Délai / conditions
Droit d'accès (art. 15)	Obtenir une copie des données vous concernant	Réponse sous 1 mois (prorogeable à 3 mois)
Droit de rectification (art. 16)	Corriger des données inexactes ou incomplètes	Réponse sous 1 mois
Droit à l'effacement (art. 17)	Demander la suppression dans certains cas	Réponse sous 1 mois

Droit	Contenu	Délai / conditions
Droit à la limitation (art. 18)	Geler temporairement un traitement contesté	Réponse sous 1 mois
Droit d'opposition (art. 21)	S'opposer à un traitement fondé sur intérêt légitime	Réponse sous 1 mois
Droit à la portabilité (art. 20)	Récupérer ses données dans un format lisible	Applicable aux traitements automatisés sur consentement/contrat

6.1 Modalités d'exercice des droits

Toutes les demandes d'exercice de droits sont centralisées et traitées par le DPO :

- Par email à : lsantos@godet.fr
- Par courrier postal à : 305 rue de la Belle Etoile 95700 Roissy-en-France, à l'attention du DPO – Liliane SANTOS

Le DPO accuse réception de toute demande dans un délai de 5 jours ouvrés et y répond dans un délai d'un mois. Ce délai peut être prorogé de deux mois supplémentaires en cas de complexité ou de nombre élevé de demandes, avec information préalable de la personne. Une pièce d'identité peut être demandée pour vérifier l'identité du demandeur.

Il est possible d'organiser un échange sécurisé ou un rendez-vous sur demande.

Le DPO tient un registre des demandes de droits exercées, permettant de suivre les délais de traitement et de démontrer la conformité de l'Entreprise.

6.2 Droit d'introduction d'une réclamation

Toute personne a le droit d'introduire une réclamation auprès de la CNIL si elle estime que le traitement de ses données porte atteinte au RGPD. Le DPO reste à disposition pour tenter de résoudre toute difficulté avant recours à la CNIL :

- En ligne : www.cnil.fr/fr/plaintes
- Par courrier : CNIL – 3 Place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07

7. Information des personnes concernées

7.1 Obligations d'information

Conformément aux articles 13 et 14 du RGPD, l'Entreprise informe les personnes concernées au moment de la collecte de leurs données. Le DPO est responsable de la rédaction, de la mise à jour et de la diffusion de l'ensemble des supports d'information.

7.2 Supports d'information par catégorie

Salariés

- Notice d'information RGPD rédigée par le DPO, remise lors de l'embauche en annexe au contrat de travail ;
- Mention dans le règlement intérieur et la charte informatique ;
- Affichage obligatoire des dispositifs de vidéosurveillance (panneaux réglementaires conformes sur chaque site, validés par le DPO) ;
- Session de sensibilisation RGPD animée par le DPO à la prise de poste et rappel annuel.

Clients et prospects

- Mention RGPD dans les contrats, devis et bons de commande, rédigée et tenue à jour par le DPO ;
- Politique de confidentialité publiée sur le site internet de l'Entreprise, validée par le DPO ;
- Mention d'information lors de toute collecte (formulaires, salons professionnels).

Fournisseurs et sous-traitants

- Clause de protection des données systématiquement intégrée dans les contrats d'achat et de prestation, sous la supervision du DPO ;
- Accord de traitement des données (ATD / DPA) signé avec tout sous-traitant traitant des données pour le compte de l'Entreprise (article 28 RGPD), géré par le DPO.

8. Sécurité des données

Conformément à l'article 32 du RGPD, l'Entreprise met en œuvre des mesures techniques et organisationnelles appropriées, définies conjointement par le DPO et le responsable informatique.

8.1 Mesures techniques

- Contrôle des accès : gestion des droits par profils, principe du moindre privilège, authentification forte (MFA) pour les accès aux données sensibles ;
- Chiffrement : chiffrement des données sensibles en transit (TLS) et au repos pour les postes nomades ;
- Sauvegardes : sauvegardes régulières testées, avec copies hors site ou en cloud sécurisé ;
- Antivirus et pare-feu : déployés sur l'ensemble des postes et serveurs ;

8.2 Mesures organisationnelles

- Formation et sensibilisation : formation obligatoire de tous les salariés à la prise de poste, rappel annuel organisé par le DPO ;
- Politique de mots de passe : complexité minimale, renouvellement périodique (voir charte informatique) ;
- Gestion des tiers : le DPO audite annuellement les sous-traitants ayant accès aux données ;

- Gestion des départs : révocation immédiate des accès coordonnée entre RH, informatique et DPO lors du départ de tout salarié ou prestataire.

8.3 Analyse d'impact (AIPD / PIA)

Conformément à l'article 35 du RGPD, une Analyse d'Impact relative à la Protection des Données (AIPD) est systématiquement réalisée par le DPO avant tout traitement susceptible d'engendrer un risque élevé. Sont notamment concernés :

- La mise en place ou l'extension d'un système de vidéosurveillance ;
- Le déploiement d'un système de géolocalisation des véhicules ou des salariés ;
- Tout traitement à grande échelle de données de santé ;
- Le déploiement de tout nouvel outil numérique traitant des données personnelles à grande échelle.

Le DPO tient un registre des AIPD réalisées, consultable par la CNIL sur demande.

9. Gestion des violations de données

Conformément à l'article 33 du RGPD, le DPO pilote l'ensemble de la procédure de gestion des violations de données personnelles.

9.1 Procédure interne

1. **Détection et signalement :** Tout salarié constatant ou suspectant une violation le signale immédiatement au DPO et au responsable informatique via lsantos@godet.fr et sdridi@godet.fr.
2. **Qualification :** Le DPO, en lien avec le responsable informatique, évalue la nature, le périmètre et le niveau de risque de la violation dans les meilleurs délais ;
3. **Documentation :** Le DPO enregistre la violation dans le registre des violations (article 33(5) RGPD), quel que soit son niveau de gravité ;
4. **Notification CNIL :** Si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes, le DPO la notifie à la CNIL dans un délai de 72 heures après sa découverte (notifications.cnil.fr) ;
5. **Information des personnes :** Si la violation présente un risque élevé, le DPO coordonne l'information des personnes concernées sans délai injustifié. La Direction est informée des violations significatives et participe à la décision sur la communication externe le cas échéant (clients, autorités, médias, etc.).

⚠ Le délai de 72 heures est impératif. En cas de doute sur la nécessité de notifier, le DPO notifie de manière préventive et complète la notification ultérieurement.

9.2 Bilan annuel

Le DPO présente chaque année à la Direction un bilan des incidents et violations survenus, des mesures correctives mises en œuvre et des axes d'amélioration identifiés.

10. Sous-traitance et transferts de données

10.1 Encadrement des sous-traitants

Tout prestataire ou sous-traitant traitant des données personnelles pour le compte de l'Entreprise doit obligatoirement signer un accord de traitement des données (ATD / DPA) conforme à l'article 28 du RGPD, rédigé et suivi par le DPO. Cet accord précise notamment :

- L'objet et la durée du traitement ;
- La nature et la finalité du traitement ;
- Le type de données et les catégories de personnes concernées ;
- Le pays d'hébergement des données et le mécanisme de transfert utilisé ;
- Les obligations et droits du responsable de traitement ;
- L'interdiction pour le sous-traitant de traiter les données à des fins autres que celles prévues.

Le DPO tient à jour la liste des sous-traitants et réalise un audit annuel de leur conformité.

10.2 Transferts hors Union européenne

Tout transfert de données personnelles vers un pays hors de l'Union européenne ou de l'EEE est soumis à validation préalable du DPO, qui vérifie l'existence d'un mécanisme de transfert conforme au chapitre V du RGPD :

- Décision d'adéquation de la Commission européenne ;
- Clauses contractuelles types (CCT) adoptées par la Commission européenne ;
- Règles d'entreprise contraignantes (BCR) ;
- Consentement explicite de la personne concernée (cas exceptionnel).

Pour les transferts vers des pays sans décision d'adéquation (notamment vers les États-Unis via certains services cloud ou outils IA), le DPO réalise une analyse complémentaire (évaluation du droit local, mesures supplémentaires techniques/organisationnelles) conformément aux recommandations de l'EDPB.

Tout déploiement d'un outil cloud (Microsoft 365, Google Workspace, outils IA, etc.) est soumis à validation préalable du DPO pour vérifier l'encadrement des transferts hors EEE.

11. Durées de conservation – Tableau synthétique

Les durées ci-dessous sont définies et tenues à jour par le DPO, en conformité avec les obligations légales françaises.

Catégorie de données	Durée de conservation	Base légale
Bulletins de paie	5 ans après émission	Code du travail art. L.3243-4
Dossier salarié (contrat, avenants)	5 ans après fin du contrat	Prescription quinquennale
Documents comptables	10 ans	Code de commerce art. L.123-22
Données de candidats non retenus	2 ans maximum	Recommandation CNIL
Données clients (contrats)	5 ans après fin de relation	Prescription quinquennale
Données prospects	3 ans sans contact	Recommandation CNIL
Vidéosurveillance	1 mois maximum	Art. L.252-5 CSI
Logs informatiques	6 mois	Recommandation CNIL / ANSSI
Données de santé (dossier médical)	50 ans minimum	Code de la santé publique
Accidents du travail / maladies prof.	5 ans (déclaration), illimitée (dossier)	Code de la sécurité sociale

12. Programme de conformité RGPD – Activités récurrentes du DPO

Fréquence	Activité
En continu	Traitement des demandes de droits, gestion des violations, conseil aux équipes
Trimestrielle	Revue du registre des traitements, mise à jour si nécessaire
Semestrielle	Audit des accès aux données sensibles, revue des sous-traitants
Annuelle	Bilan RGPD présenté à la Direction, mise à jour de la Politique, formation de rappel des salariés, revue des durées de conservation et purges, audit des outils SaaS et cloud
À chaque nouveau traitement	Analyse de nécessité, validation de la base légale, mise à jour du registre, AIPD si applicable
À chaque départ salarié / prestataire	Révocation des accès, archivage ou suppression des données selon les durées légales

13. Dispositions finales

ATTESTATION D'APPROBATION ET DE DIFFUSION

Les soussigné(e)s attestent avoir approuvé la présente Politique de Protection des Données Personnelles et s'engagent à en assurer la diffusion et l'application au sein de l'Entreprise.

Alex LAMBERIO, CEO

Liliane SANTOS, Responsable QHSE - Le/La DPO

Document à conserver dans le registre de conformité RGPD de l'Entreprise.