

Politique de Protection des Données à caractère personnel

1. Contexte

Objectifs

La présente politique (ci-après la « **Politique** » ou « **PPD** ») formalise les engagements de **LAYAN SAS** en matière de protection des données à caractère personnel, en application du Règlement (UE) 2016/679 du 27 avril 2016 (« **RGPD** ») et de la loi française n° 78-17 du 6 janvier 1978 modifiée (« **Informatique et Libertés** »).

Elle a pour objectifs de :

- Établir l'approche générale de Layan en matière de protection des données ;
- Documenter les principes, les rôles et les procédures internes ;
- Garantir le respect des droits des personnes concernées ;
- Démontrer la conformité de Layan (principe d'*accountability* — article 24 RGPD) ;
- Compléter, sur le volet protection des données personnelles, la **Politique de Sécurité des Services d'Information** de référence interne **P1 - PSI**, à laquelle elle renvoie pour tout ce qui relève des mesures techniques de sécurité.

Articulation avec la PSSI (P1)

La présente PPD et la PSSI (P1) constituent ensemble le socle documentaire de la conformité de Layan :

- **P1 - PSI** couvre la sécurité technique et organisationnelle des systèmes d'information (contrôle d'accès, hébergement, tests, gestion des incidents, sécurité physique, ressources humaines).
- **P2 - PPD** couvre la gouvernance RGPD : principes, droits des personnes, durée de conservation, sous-traitance, transferts hors UE, rôle du DPO.

Elles sont complémentaires. En cas d'évolution de l'une, l'autre est revue.

2. Définitions

- **Données à caractère personnel (« Données »)** : toute information se rapportant à une personne physique identifiée ou identifiable (article 4 (1) RGPD).
- **Traitement** : toute opération ou ensemble d'opérations portant sur des Données (article 4 (2) RGPD).
- **Responsable de traitement** : la personne morale qui détermine les finalités et les moyens du Traitement (article 4 (7) RGPD).

- **Sous-traitant** : la personne morale qui traite des Données pour le compte du Responsable de traitement (article 4 (8) RGPD).
- **Personne concernée** : la personne physique à laquelle se rapportent les Données.
- **Violation de données** : violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des Données (article 4 (12) RGPD).
- **DPO (Délégué à la Protection des Données)** : personne désignée par Layan pour piloter la conformité RGPD (articles 37 à 39 RGPD).
- **AIPD (Analyse d'Impact relative à la Protection des Données)** : analyse formalisée des risques d'un traitement à risque élevé (article 35 RGPD).
- **EEE** : Espace Économique Européen.

Pour les autres définitions (collaborateurs, prestataires, société, actifs essentiels), il est renvoyé à la PSSI (P1, § 1).

3. Périmètre d'application

La présente Politique s'applique :

- à l'ensemble des **collaborateurs** de Layan SAS (salariés, alternants, stagiaires, dirigeants, contractuels) ;
- à l'ensemble des **prestataires et fournisseurs** de Layan ayant accès, même ponctuellement, à des Données traitées par Layan ;
- aux **clients** de Layan dans le cadre de leur utilisation de la plateforme ATS (Applicant Tracking System) éditée par Layan ;
- à l'ensemble des **traitements de Données** réalisés par Layan, qu'elle agisse en qualité de **Responsable de traitement** (par exemple : Données de ses propres collaborateurs, prospects et clients) ou de **Sous-traitant** (par exemple : Données candidats traitées pour le compte des clients).

4. Engagement de la Direction

La Direction de Layan SAS, représentée par son Président, la société **BZM** (RCS Nanterre 989 314 067), elle-même représentée par **Benjamin Zerdoun**, et son Directeur Général, la société **NCC** (RCS Paris 989 385 901), elle-même représentée par **Nicolas Chevalier Cohen**, conjointement avec le Délégué à la Protection des Données, **Aymen Ezzayer**, s'engage à :

- placer la protection des Données au cœur de la gouvernance de l'entreprise ;
- doter le Délégué à la Protection des Données des moyens nécessaires à l'exercice de ses missions ;
- intégrer la protection des Données dès la conception des produits et des processus (*privacy by design*) et par défaut (*privacy by default*) ;
- coopérer pleinement avec la Commission Nationale de l'Informatique et des Libertés (« **CNIL** ») et toute autre autorité de contrôle compétente ;

- réviser annuellement la présente Politique et la PSSI (P1).

Cette procédure a été revue et validée par la Direction en septembre 2026.

5. Gouvernance et responsabilités

Rôle	Personne	Responsabilités
Président	BZM SAS (RCS Nanterre 989 314 067), représentée par Benjamin Zerdoun	Représentant légal de Layan SAS ; signataire des engagements et des contrats au nom de la société.
Directeur Général (DG)	NCC SAS (RCS Paris 989 385 901), représentée par Nicolas Chevalier Cohen	Garant de la bonne application de la présente Politique ; chaîne hiérarchique du Technical Lead et du DPO ; valide les décisions structurantes (changement de sous-traitant, AIPD, notifications de violation) ; signe le rapport annuel de conformité.
Délégué à la Protection des Données (DPO)	Aymen Ezzayer — aymen@layan.eu	Pilote opérationnel de la conformité RGPD : registre des traitements (Art. 30), AIPD (Art. 35), formation des collaborateurs, gestion des demandes de droits, point de contact CNIL et personnes concernées. Rapporte au DG, avec indépendance fonctionnelle dans l'exercice de ses missions (Art. 38).
Technical Lead	Andy Le Roy	Mise en œuvre opérationnelle des mesures de sécurité (cf. PSSI § 2) ; remontée des incidents au DPO et à la Direction ; sensibilisation technique des équipes. Rapporte au DG.
Ensemble des collaborateurs	Tous	Respect de la présente Politique et de la PSSI ; remontée des incidents ; participation à la sensibilisation annuelle.

Le DPO est désigné en application de l'article 37 RGPD. Bien qu'Aymen Ezzayer porte également le titre de **Directeur des Systèmes d'Information (DSI)**, il n'a pas de responsabilité opérationnelle dans la définition des moyens de traitement (qui relèvent du Technical Lead sous l'autorité du DG). Sa fonction de DPO est exercée de manière indépendante, conformément à l'article 38 (3) RGPD.

Pour les questions courantes des personnes concernées et des clients, le canal de contact privilégié est support@layan.eu. Pour toute question impliquant directement le DPO, l'adresse est aymen@layan.eu.

6. Principes appliqués (article 5 RGPD)

Layan applique les principes suivants à l'ensemble de ses traitements :

Principe	Application chez Layan
Licéité, loyauté, transparence	Chaque traitement repose sur une base légale identifiée (cf. § 7). Les personnes concernées sont informées préalablement à toute collecte (politique de confidentialité accessible, mentions sur les formulaires).

Principe	Application chez Layan
Limitation des finalités	Les Données sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas réutilisées de manière incompatible.
Minimisation	Seules les Données strictement nécessaires aux finalités sont collectées. Les formulaires sont régulièrement revus pour retirer les champs superflus.
Exactitude	Les personnes concernées peuvent rectifier leurs Données à tout moment via la plateforme ou par demande au DPO.
Limitation de la conservation	Des durées de conservation sont définies par finalité (cf. § 10). À l'expiration, les Données sont supprimées ou anonymisées.
Intégrité et confidentialité	Mise en œuvre des mesures techniques et organisationnelles décrites dans la PSSI (P1 § 6, § 7 et § 8).
Responsabilité (<i>accountability</i>)	Tenue d'un registre des activités de traitement (Art. 30), réalisation d'AIPD lorsque requis (Art. 35), formation des collaborateurs, audits internes et externes.

7. Bases légales mobilisées (article 6 RGPD)

Selon la nature du traitement, Layan mobilise l'une des bases légales suivantes :

Traitement	Base légale	Justification
Mise à disposition de la plateforme aux clients	Exécution du contrat	Article 6 (1) (b) — exécution des Conditions Générales d'Utilisation.
Traitement de Données candidats pour le compte des clients (Sous-traitance)	Sous-traitance	Article 28 — Layan agit en qualité de Sous-traitant ; la base légale est celle invoquée par le client Responsable de traitement. Le détail figure dans le Data Processing Agreement (DPA) signé avec chaque client.
Gestion administrative des collaborateurs Layan	Exécution du contrat de travail / Obligations légales	Article 6 (1) (b) et (c) — contrats, paie, déclarations sociales.
Prospection commerciale B2B	Intérêt légitime	Article 6 (1) (f) — démarchage de personnes morales sur leur fonction professionnelle, avec droit d'opposition garanti.
Newsletter et communications marketing à des contacts B2C ou candidats	Consentement	Article 6 (1) (a) — opt-in explicite, retrait possible à tout moment.
Gestion des cookies du site vitrine et de la plateforme	Consentement (cookies non strictement nécessaires) / Intérêt légitime (cookies strictement nécessaires)	Articles 6 (1) (a) et (f), et article 82 de la loi Informatique et Libertés.

Le registre des traitements (Art. 30, voir § 14) précise pour chaque traitement la base légale retenue.

8. Catégories de Données et de personnes concernées

Layan traite les catégories de Données suivantes :

8.1 Données traitées en qualité de Sous-traitant (pour le compte des clients)

- **Personnes concernées** : candidats à des offres d'emploi, utilisateurs internes des clients (recruteurs, managers, administrateurs), visiteurs des sites carrière édités via la plateforme, et personnes de référence désignées par un candidat lorsque le client recourt à la prise de références.
- **Catégories de Données** : identification (civilité, genre — champ requis sur le formulaire de candidature public —, nom, prénom), contact (e-mail, téléphone, adresse), parcours professionnel (CV, formation, expériences, compétences, prétentions salariales), candidature (lettre, réponses, statut, commentaires des recruteurs, résultats d'évaluation prédictive en option), connexion (identifiant, IP, horodatage, journal d'activité), authentification (mots de passe hachés, jetons SSO), communications (e-mails et SMS échangés via la plateforme).
- **Catégories particulières (Art. 9)** : aucune n'est requise ; la plateforme déconseille leur saisie. Si un client en collecte sous sa propre responsabilité, il en informe Layan préalablement et garantit l'existence d'une base juridique appropriée.
- **Données relatives aux condamnations pénales (Art. 10)** : néant.

8.2 Données traitées en qualité de Responsable de traitement (pour le compte propre de Layan)

- **Collaborateurs Layan** : Données nécessaires à l'exécution du contrat de travail et aux obligations sociales ;
- **Prospects et clients (B2B)** : Données de contact professionnel des interlocuteurs (nom, fonction, e-mail professionnel, historique des échanges) ;
- **Visiteurs du site `layan.eu`** : Données de connexion, statistiques de visite, traceurs après consentement le cas échéant.

9. Droits des personnes concernées (articles 12 à 23 RGPD)

Toute personne concernée dispose des droits suivants :

- **Information** (Art. 13-14) : mentions d'information lors de la collecte ;

- **Accès** (Art. 15) : obtenir la confirmation que ses Données sont traitées et en obtenir une copie ;
- **Rectification** (Art. 16) : faire corriger des Données inexactes ;
- **Effacement / oubli** (Art. 17) : faire supprimer ses Données dans les conditions prévues par le RGPD ;
- **Limitation** (Art. 18) ;
- **Portabilité** (Art. 20) : récupérer ses Données dans un format structuré ;
- **Opposition** (Art. 21), notamment à la prospection ;
- **Décisions individuelles automatisées** (Art. 22) : Layan ne pratique pas de scoring automatique produisant des effets juridiques ; les recommandations de la plateforme assistent le recruteur sans s'y substituer ;
- **Réclamation auprès de la CNIL** (Art. 77) : via www.cnil.fr.

Procédure d'exercice des droits

Étape	Délai	Responsable
Réception de la demande	—	Canal client : support@layan.eu ; canal DPO : aymen@layan.eu
Accusé de réception	Sous 5 jours ouvrés	DPO
Vérification de l'identité du demandeur	Sous 5 jours ouvrés	DPO
Si la demande porte sur des Données traitées en qualité de Sous-traitant : transmission au client Responsable de traitement	Sous 5 jours ouvrés à compter de la vérification	DPO
Si la demande porte sur des Données traitées en qualité de Responsable de traitement : réponse	Sous 1 mois (extensible à 3 mois en cas de complexité, avec information de la personne) — Art. 12 (3) RGPD	DPO
Suivi et journalisation de la demande	—	DPO (registre des demandes de droits)

10. Durée de conservation

Les durées sont définies par finalité, dans le respect des recommandations de la CNIL applicables au secteur du recrutement :

Catégorie de Données	Durée de conservation
Données candidats (en qualité de Sous-traitant pour les clients)	Définie par chaque client Responsable de traitement et précisée dans son DPA. Paramétrable en années (1 an ou 2 ans) ; durée par défaut : 2 ans à compter de la date de candidature, réinitialisée par un consentement renouvelé (recommandation CNIL).
Comptes et activité des utilisateurs internes des clients	Pendant la durée du contrat client, supprimés ou anonymisés dans les 30 jours suivant la fin du contrat.
Données de suivi de visite des sites carrière (IP, ville, code postal)	48 heures, puis anonymisation irréversible quotidienne.
Journaux techniques (logs applicatifs, accès)	12 mois (recommandation CNIL pour les logs de connexion). Certains journaux applicatifs internes ne sont pas encore purgés automatiquement : l'écart est consigné au registre des traitements.
Données collaborateurs Layan	Selon obligations légales : 5 ans après fin du contrat de travail pour les bulletins de paie (Code du travail), 10 ans pour la comptabilité (Code de commerce).
Prospection commerciale B2B	3 ans à compter du dernier contact, sauf opposition antérieure.
Cookies	Durée maximale 13 mois (recommandation CNIL).

À l'expiration de ces durées, les Données sont supprimées ou anonymisées de manière irréversible. Les sauvegardes sont chiffrées et purgées dans le cycle de rotation décrit dans la PSSI § 4.

Effacement à la demande. Lorsqu'un client exerce, pour le compte d'une personne concernée, une demande d'effacement depuis l'interface RGPD de la plateforme, la candidature est immédiatement marquée comme supprimée et retirée des offres et viviers ; la suppression matérielle des enregistrements et des fichiers associés intervient par tâche planifiée trois (3) mois après ce marquage.

11. Sous-traitants ultérieurs

Layan recourt à des sous-traitants ultérieurs pour réaliser une partie de ses activités de traitement, notamment l'hébergement, l'envoi d'e-mails, l'analyse de CV, la supervision applicative, l'authentification SSO et la diffusion d'offres d'emploi.

- La **liste à jour** des sous-traitants nommément désignés et catégorisés figure à l'**Annexe 3 du DPA** signé avec chaque client.
- Chaque sous-traitant ultérieur est encadré par un contrat écrit prévoyant des obligations équivalentes à celles imposées à Layan en matière de protection des Données.
- Toute évolution de cette liste est notifiée aux clients ayant signé un DPA, avec un préavis d'au moins 30 jours et un droit d'objection motivé (cf. DPA Art. 6.3).

L'hébergement de la plateforme est assuré par **Scaleway**, sur la région **France — `fr-par` (Paris)**. Un hébergement antérieur chez Amazon Web Services subsiste **en lecture seule**, sans écriture nouvelle, dans les régions européennes France (Paris) et Irlande, jusqu'à sa suppression définitive prévue au plus tard le **31 octobre 2026**.

12. Transferts de Données hors EEE

Layan traite et stocke les Données au sein de l'Union européenne (région France — fr-par, Paris), sous réserve du reliquat historique en lecture seule mentionné au § 11.

Certains sous-traitants ultérieurs peuvent toutefois être établis dans des pays tiers ou y accéder à des Données. Dans ce cas, Layan veille à ce que le transfert soit encadré par l'un des mécanismes prévus aux articles 44 à 49 RGPD :

- Décision d'adéquation de la Commission européenne (par exemple, le Royaume-Uni) ;
- Clauses Contractuelles Types (décision (UE) 2021/914 du 4 juin 2021) ;
- *EU-US Data Privacy Framework* pour les sous-traitants établis aux États-Unis qui en sont certifiés.

Aucun transfert hors EEE n'est réalisé sans encadrement par l'un de ces mécanismes.

13. Mesures techniques et organisationnelles

Les mesures de sécurité mises en œuvre par Layan sont décrites de manière détaillée dans la **Politique de Sécurité des Services d'Information (P1 - PSI)**, à laquelle la présente Politique renvoie expressément.

Sont notamment couverts :

Domaine	Référence PSSI
Contrôle des accès, authentification, surveillance, encadrement du développement, suivi des erreurs	PSSI § 6
Gestion des risques et des incidents	PSSI § 7
Sécurité physique des locaux et des équipements	PSSI § 8
Sécurité des ressources humaines (avant, pendant, fin de contrat)	PSSI § 9
Hébergement (Scaleway, région France fr-par)	PSSI § 10
Plan de Continuité d'Activité (PCA)	PSSI § 4
Tests de pénétration et de vulnérabilité	PSSI § 5
Niveaux de contrôle (opérationnel, permanent, périodique)	PSSI § 3

Pour le volet *protection des données* spécifiquement, Layan applique en complément :

- la pseudonymisation et la minimisation appliquées par défaut dans les formulaires et exports ;
- des mécanismes de suppression et d'anonymisation à l'expiration des durées de conservation ;
- des exports structurés au format lisible par machine pour le droit à la portabilité ;
- des engagements contractuels de confidentialité avec chaque sous-traitant ultérieur traitant des Données.

14. Registre des activités de traitement (article 30 RGPD)

Layan tient un **registre des activités de traitement** maintenu par le DPO. Ce registre recense :

- la dénomination de chaque traitement et sa finalité ;
- les catégories de personnes concernées et de Données ;
- les destinataires (internes et sous-traitants ultérieurs) ;
- les transferts éventuels hors EEE et leur encadrement ;
- les durées de conservation ;
- une description générale des mesures techniques et organisationnelles ;
- la qualité dans laquelle Layan agit (Responsable / Sous-traitant).

Le registre est revu au moins une fois par an et tenu à disposition de la CNIL sur demande.

15. Analyses d'impact (AIPD — article 35 RGPD)

Une AIPD est réalisée par le DPO, en concertation avec le Technical Lead et la Direction, lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, notamment en cas :

- de mise en place d'un nouveau traitement à grande échelle de Données candidats ou employés ;
- d'introduction d'une fonctionnalité de profilage ou de décision automatisée ;
- d'usage de catégories particulières de Données (Art. 9) à grande échelle.

Les AIPD sont archivées et tenues à disposition de la CNIL.

16. Gestion des violations de Données (articles 33-34 RGPD)

En cas de violation de Données, Layan applique la procédure suivante :

1. **Détection** par tout collaborateur ou outil de surveillance (cf. PSSI § 6 et § 7) ;
2. **Remontée immédiate** au Technical Lead et au DPO ;

3. **Évaluation** de la nature, du volume et du risque pour les personnes — cellule DPO + Technical Lead + DG ;
4. **Confinement** technique et collecte des preuves (cf. PSSI § 7) ;
5. **Notification au client** (lorsque Layan agit en Sous-traitant), sous 72 heures, selon le modèle figurant dans l'**Annexe 4 du DPA** ;
6. **Notification à la CNIL** (lorsque Layan agit en Responsable de traitement et qu'il existe un risque pour les personnes), sous 72 heures, par le DPO via [notifications.cnil.fr](https://www.notifications.cnil.fr) ;
7. **Information des personnes concernées** (Art. 34) si le risque est élevé ;
8. **Post-mortem** dans les 30 jours suivant la clôture, comprenant l'analyse de la cause racine, les mesures correctives et les mises à jour de procédures ;
9. **Tenue d'un registre des violations** par le DPO.

17. Sensibilisation et formation

- **Sensibilisation annuelle** de l'ensemble des collaborateurs, organisée conjointement par le Technical Lead (volet sécurité — cf. PSSI § 7 et § 9) et le DPO (volet protection des Données).
- **Formation à l'embauche** : tout nouveau collaborateur reçoit, dans les 30 jours suivant son arrivée, une formation initiale couvrant la PSSI et la PPD.
- **Engagement de confidentialité** signé par chaque collaborateur, prestataire ou intervenant ayant accès à des Données.
- **Communications ad hoc** lors de l'évolution de la réglementation ou de la survenance d'un incident significatif.

18. Contrôle, audit et amélioration continue

Le contrôle de la présente Politique repose sur les **trois niveaux de contrôle décrits dans la PSSI § 3** :

- **Opérationnel** : continu, par l'ensemble des collaborateurs, sur le respect quotidien de la confidentialité ;
- **Permanent** : annuel, par la Direction et le DPO, conduite de tests, formation, conformité aux évolutions réglementaires ;
- **Périodique** : tous les 2 à 3 ans, audit externe indépendant.

Le DPO établit un **rapport annuel de conformité** présenté à la Direction. Ce rapport inclut :

- l'état du registre des traitements (Art. 30) ;
- la liste des AIPD réalisées ou en cours ;
- les demandes d'exercice de droits reçues et leur traitement ;
- les violations éventuelles et leurs suites ;
- la liste des évolutions de sous-traitants ultérieurs et des notifications associées ;

- les actions de sensibilisation conduites ;
- les recommandations d'amélioration.

19. Validation, communication et mise à jour

- La présente Politique est **validée** par la Direction (Directeur Général et DPO).
- Elle est **communiquée** à l'ensemble des collaborateurs (intranet / espace partagé) et **mise à disposition** des clients et prospects qui en font la demande, ainsi que de toute autorité de contrôle.
- Elle est **revue au minimum une fois par an** par le DPO. Toute évolution réglementaire majeure (ex. nouveau référentiel CNIL applicable au secteur du recrutement) déclenche une revue intermédiaire.
- L'historique des versions est tenu en annexe du document maître.

Pour toute question relative à la présente Politique, contacter :

- le **Délégué à la Protection des Données** : Aymen Ezzayer — aymen@layan.eu
- le **canal client / personnes concernées** : support@layan.eu