Plan d'Assurance Sécurité

1. Objet et statut du document

Le présent **Plan d'Assurance Sécurité** (ci-après le « **PAS** ») décrit l'ensemble des mesures techniques, organisationnelles et contractuelles mises en œuvre par **LAYAN SAS** (ci-après « **Layan** ») pour garantir la sécurité, la confidentialité, l'intégrité et la disponibilité des données traitées dans le cadre de l'exploitation de sa plateforme logicielle de gestion du recrutement (ATS — *Applicant Tracking System*), ci-après la « **Plateforme** ».

Il a pour vocation :

- de répondre aux exigences des Directions des Systèmes d'Information (DSI) des clients et prospects de Layan en matière de transparence sur les mesures de sécurité ;
- de constituer un document **unilatéral et public-ready** mobilisable lors des phases d'appel d'offres, d'audit, de référencement et de revue annuelle ;
- de compléter le **Data Processing Agreement (DPA)** signé entre Layan et chaque client en explicitant l'architecture technique, les engagements de service et les processus opérationnels qui sous-tendent les Mesures Techniques et Organisationnelles (MTO) de l'Annexe 2 du DPA.

Le PAS **ne se substitue pas** :

- à la **Politique de Sécurité des Services d'Information** (référence interne **P1 - PSI**, ci-après la « **PSSI** »), document interne de gouvernance ;
- à la **Politique de Protection des Données à caractère personnel** (référence interne **P2 - PPD**), document de gouvernance RGPD ;
- au **DPA**, contrat bilatéral signé par chaque client.

2. Articulation documentaire

Le socle documentaire de Layan en matière de sécurité et de protection des données s'articule autour de quatre documents complémentaires :

Référence	Document	Nature	Audience
P1 - PSI	Politique de Sécurité des Services d'Information (PSSI)	Politique interne, gouvernance sécurité	Collaborateurs Layan ; communiquée aux clients sur demande
P2 - PPD	Politique de Protection des Données à caractère personnel	Politique unilatérale RGPD	Clients, prospects, personnes concernées, autorités
P3 - PAS	Plan d'Assurance Sécurité (présent document)	Description opérationnelle des mesures et engagements	Clients, prospects, DSI

Référence	Document	Nature	Audience
DPA	Accord de sous-traitance (article 28 RGPD)	Contrat bilatéral	Signé par chaque client Responsable de traitement

En cas de divergence entre le PAS et le DPA signé avec un client, **le DPA prévaut**. En cas d'évolution d'un de ces quatre documents, les autres sont revus pour cohérence.

3. Présentation de Layan

Élément	Information
Raison sociale	LAYAN SAS
Forme juridique	Société par actions simplifiée
Siège social	198 avenue de France, 75013 Paris (France)
Immatriculation	RCS Nanterre 891 123 432
Activité	Édition et exploitation d'une plateforme logicielle ATS
Site institutionnel	layan.eu
Année de création	2020
Effectif	Tranche 20 à 49 salariés ; Kbis à jour communicable sur demande

4. Gouvernance et responsabilités

4.1 Organisation interne

Rôle	Responsabilités	Contact
Président — **BZM** SAS (RCS Nanterre 989 314 067), représentée par Benjamin Zerdoun	Représentant légal de Layan SAS ; signature des engagements et contrats	Via `support@layan.eu`
Directeur Général (DG / CEO) — **NCC** SAS (RCS Paris 989 385 901), représentée par Nicolas Chevalier Cohen	Garant de la sécurité et de la conformité ; supervise la chaîne hiérarchique du Technical Lead et du DPO ; valide les décisions structurantes (changement de sous-traitant, notification d'incident, AIPD)	Via `support@layan.eu`
Délégué à la Protection des Données (DPO) — Aymen Ezzayer	Pilote opérationnel de la conformité RGPD ; point de contact CNIL et personnes concernées ; indépendance fonctionnelle au sens de l'article 38 RGPD	`aymen@layan.eu`
Technical Lead — Andy Le Roy	Mise en œuvre opérationnelle des mesures de sécurité ; supervision des incidents techniques ; revue des accès	Via `support@layan.eu`

Rôle	Responsabilités	Contact
Canal client / support	Point d'entrée pour toutes les demandes opérationnelles, support, et exercice des droits	`support@layan.eu`

4.2 Chaîne d'escalade en cas d'incident

1. **Détection** — Collaborateurs Layan, outils de supervision, signalement client.
2. **Niveau 1** — Équipe technique / Technical Lead.
3. **Niveau 2** — DG et DPO (notifications RGPD, communications clients).
4. **Niveau 3** — Président (engagements légaux, plaintes auprès des autorités), représenté par BZM.

5. Périmètre du service

5.1 Service couvert

Le présent PAS couvre l'exploitation de la **Plateforme ATS Layan**, accessible via les sous-domaines `app.*.layan.eu` (back-office recruteur), `jobs.*.layan.eu` (site carrière public), `api.*.layan.eu` (API REST) et `admin.layan.eu` (back-office Layan).

Fonctionnalités principales couvertes :

- Publication et diffusion d'offres d'emploi (incluant la diffusion automatisée sur plus de 50 jobboards) ;
- Collecte, organisation et évaluation des candidatures ;
- Communication avec les candidats par courriel et SMS ;
- Gestion des viviers de talents et des campagnes de recrutement ;
- Édition et publication d'un site carrière sur un sous-domaine personnalisé ;
- Synchronisation calendrier pour la planification d'entretiens ;
- Génération de contenu et matching candidat/offre assistés par intelligence artificielle (fonctionnalités optionnelles) ;
- API REST et webhooks pour intégration avec les outils RH et SIRH du client ;
- Export et restitution des données.

5.2 Hors périmètre

Sont expressément hors du périmètre du présent PAS :

- les systèmes d'information du client (postes de travail, réseaux, annuaires d'entreprise) ;
- les terminaux d'accès des utilisateurs du client ;
- les intégrations tierces non éditées par Layan, sauf description explicite dans l'Annexe 3 du DPA ;

- les éventuels développements spécifiques sur devis, qui font l'objet d'un cahier des charges et d'un avenant dédiés.

6. Engagements de service (SLA)

6.1 Disponibilité

Layan s'engage sur un **taux de disponibilité annuel cible de 99,9 %** sur le périmètre de production de la Plateforme, calculé sur l'année civile et hors fenêtres de maintenance planifiée.

Les **maintenances planifiées** sont annoncées par notification écrite (via la Plateforme et / ou par courriel à l'administrateur client) au moins **soixante-douze (72) heures à l'avance** et sont privilégiées sur des plages horaires à faible trafic.

Les **maintenances d'urgence** rendues nécessaires par un correctif de sécurité critique peuvent être déclenchées sans préavis ; le client en est informé dans les meilleurs délais.

6.2 Support et engagements de prise en charge

Le support utilisateur est assuré via **Intercom** (chat in-app et courriel), avec gestion des tickets, historique et notifications, en complément du canal `support@layan.eu`.

Horaires d'ouverture du support :

- **Du lundi au vendredi**
- **9h00 — 12h30** et **14h00 — 17h30** (heure de Paris)
- Hors jours fériés français

Engagements de prise en charge selon la sévérité (mesurée en heures ouvrées sur la plage d'ouverture précitée) :

Sévérité	Définition	Prise en charge	Résolution cible
Critique	Service totalement indisponible ou inaccessible pour l'ensemble des utilisateurs	≤ 1 heure ouvrée	Best effort 24/7 jusqu'à rétablissement
Majeur	Fonction clé dégradée affectant l'usage normal	≤ 4 heures ouvrées	≤ 2 jours ouvrés
Mineur	Anomalie sans contournement notable, impact limité	≤ 1 jour ouvré	Programmation dans une release
Demande d'évolution / question	Question fonctionnelle ou suggestion	≤ 2 jours ouvrés	Étude au cas par cas

6.3 Communication d'incident

Tout incident affectant la disponibilité de la Plateforme fait l'objet :

- d'une **première communication** dans le ticket d'origine ou par notification proactive aux administrateurs clients impactés ;
- d'une **communication d'avancement** au moins toutes les deux (2) heures pour les incidents de sévérité critique ;
- d'un **rapport d'incident (RFO — Reason For Outage) transmis dans les dix (10) jours ouvrés** suivant la clôture d'un incident critique, comprenant chronologie, cause racine, mesures correctives immédiates et plan de prévention.

7. Hébergement et infrastructure

7.1 Localisation

La Plateforme est hébergée chez **Scaleway SAS**, sur la région **France** — code `fr-par` (Paris).

L'ensemble des données de production (bases de données, stockage objet, journaux applicatifs) demeure dans l'Union européenne. Les sauvegardes ne sortent pas de l'EEE.

La diffusion périphérique, la résolution DNS, le pare-feu applicatif et la protection anti-DDoS sont assurés par **Cloudflare** ; le trafic transite par ses points de présence, dont ceux situés dans l'Union européenne.

Hébergement antérieur. Jusqu'au 1er août 2026, la Plateforme était hébergée chez **Amazon Web Services EMEA SARL** (régions `eu-west-3` Paris et, pour un compartiment historique, `eu-west-1` Irlande). Ces compartiments sont désormais **en lecture seule**, sans écriture nouvelle, et leur suppression définitive est prévue au plus tard le **31 octobre 2026**.

7.2 Certifications de l'hébergeur

L'hébergeur publie les certifications et attestations dont il dispose au niveau de ses centres de données et des services utilisés, au premier rang desquelles la norme **ISO/IEC 27001** (management de la sécurité de l'information).

La liste à jour et le périmètre exact de ces certifications sont publiés par l'hébergeur sur son espace de conformité, qui prévaut sur toute reproduction dans le présent document. Layan communique sur demande motivée du client les attestations qu'elle détient de ses propres sous-traitants ultérieurs, dans la limite des conditions de diffusion imposées par ces derniers.

7.3 Architecture haute disponibilité

L'architecture de production met en œuvre :

- un **orchestrateur de conteneurs managé** (Kubernetes) hébergeant les composants applicatifs, avec redémarrage automatique et mise à l'échelle horizontale des services exposés ;
- une **base de données managée** (MySQL 8) déployée en **cluster à haute disponibilité**, avec bascule automatique et accès restreint au réseau privé ;
- un **stockage objet** redondé pour les pièces jointes et CV, en classe multi-zones de disponibilité ;
- une **distribution de contenu** via réseau de diffusion périphérique pour les ressources statiques publiques.

7.4 Conformité Layan

Layan n'est pas, à la date d'édition du présent PAS, titulaire d'une certification ISO/IEC 27001 à titre propre. Layan est engagée dans une **démarche d'alignement sur le référentiel ISO/IEC 27001:2022 et son amendement 2024**, déjà matérialisée par :

- la rédaction d'une PSSI (P1) validée par la Direction ;
- la rédaction d'une PPD (P2) validée par la Direction et le DPO ;
- la tenue d'un registre des activités de traitement (article 30 RGPD) ;
- la formalisation des MTO en Annexe 2 du DPA ;
- la mise en œuvre des contrôles techniques décrits au § 8 du présent PAS.

La démarche d'alignement ISO 27001 n'engage pas Layan à obtenir une certification dans un délai déterminé ; toute évolution de cet engagement sera communiquée aux clients.

8. Sécurité technique

Layan met en œuvre, en cohérence avec l'Annexe 2 du DPA et la PSSI, les mesures techniques suivantes.

8.1 Authentification et contrôle d'accès

- **Authentification individuelle** obligatoire pour tout accès à la Plateforme ; aucun compte partagé.
- **Mots de passe** stockés sous forme hachée à l'aide d'un algorithme à fonction de hachage adaptative résistant aux attaques par force brute (Argon2id ou bcrypt selon l'environnement).
- **Authentification multi-facteur (MFA)** : déploiement **prévu** pour les comptes à privilèges et les administrateurs clients. Dans l'attente, l'accès au plan de contrôle de l'infrastructure est restreint par réseau privé et authentification forte, et l'authentification SSO d'entreprise permet au client d'appliquer sa propre politique de facteurs multiples.
- **Single Sign-On (SSO)** d'entreprise via OAuth2 / OpenID Connect : prise en charge native de Google Workspace, Microsoft 365 / Azure AD / Entra ID, et d'un gateway multi-IdP (Cryptr) supportant également SAML 2.0.

- **Cloisonnement strict** des données entre clients par identifiant d'organisation, contrôlé applicativement à chaque requête.
- **Sessions** à durée limitée ; cookies de session marqués `Secure`, `HttpOnly`, `SameSite`.
- **Revue annuelle** des comptes utilisateurs et des habilitations.

8.2 Chiffrement

- **En transit** : ensemble des flux Internet entrants et sortants chiffrés via TLS 1.2 minimum, avec préférence pour TLS 1.3. Les certificats sont gérés automatiquement avec rotation programmée.
- **Au repos** : stockage objet chiffré au niveau du compartiment en **AES-256**, les clés étant gérées par l'hébergeur ; bases de données et sauvegardes exploitées sur un service managé assurant le chiffrement des volumes au repos.
- **Secrets et identifiants techniques** : conservés dans le **gestionnaire de secrets** de l'hébergeur et projetés dans les environnements d'exécution par un opérateur disposant d'un accès en lecture seule, jamais en clair dans le code source ou les images applicatives.
- **Rotation périodique** des secrets sensibles et des clés d'API techniques.

8.3 Sécurité réseau et infrastructure

- **Réseau privé cloisonné** ; les bases de données et systèmes internes ne sont pas accessibles depuis Internet.
- **Segmentation** stricte entre l'exposition publique (uniquement l'équilibreur de charge) et les sous-réseaux privés (applications, bases de données).
- **Politiques réseau en refus par défaut** au niveau des conteneurs, avec liste d'autorisations explicite des flux sortants (base de données, cache, SMTP, IMAP, partenaires de diffusion).
- **Pare-feu applicatif (WAF) déployé en production** au niveau du réseau de diffusion périphérique, pour la protection contre les attaques courantes (OWASP Top 10) et la limitation de débit.
- **Protection anti-DDoS** fournie au niveau du réseau de diffusion périphérique.
- **Filtrage de l'origine** : l'équilibreur de charge de production n'accepte que le trafic provenant des plages d'adresses du réseau de diffusion périphérique, de sorte que l'origine ne peut être atteinte directement.
- **Protection anti-robot** (*Turnstile*) sur les formulaires de candidature publics.
- **Accès administrateur** au plan de contrôle via réseau privé avec authentification forte ; aucun accès SSH direct depuis Internet.

8.4 Sécurité applicative

- **Cycle de développement sécurisé** : revues de code obligatoires, analyse statique, analyse de composition logicielle (SCA) sur les dépendances, contrôle de qualité (PHPStan niveau 9+, ESLint).

- **Validation des entrées** au niveau des limites du système (formulaires, API) ; requêtes paramétrées exclusivement (aucune interpolation SQL).
- **Protection** contre les attaques OWASP Top 10 (injection, XSS, CSRF, SSRF, désérialisation, etc.).
- **En-têtes de sécurité** HTTP : `Strict-Transport-Security` est appliqué à l'ensemble du domaine au niveau du réseau de diffusion périphérique (durée de deux ans, sous-domaines inclus, avec préchargement). Le déploiement des en-têtes complémentaires (`Content-Security-Policy`, `X-Frame-Options`, `X-Content-Type-Options`, `Referrer-Policy`) est **en cours**.

8.5 Journalisation et supervision

- **Journalisation** des accès aux données et des actions sensibles (qui a accédé à quoi, quand), conservée pendant la durée requise par les obligations légales et opérationnelles (cf. PPD § 10).
- **Centralisation** des journaux applicatifs et systèmes.
- **Supervision applicative** en temps réel avec alertes automatisées sur incidents (erreurs, latence anormale, pics de trafic).
- **Détection** des anomalies d'accès (tentatives de connexion répétées en échec, accès hors horaires habituels, modifications de configuration sensibles).
- **Suivi des erreurs** via un outil de supervision applicative (Sentry).

8.6 Sauvegardes

- **Sauvegardes automatiques quotidiennes** des bases de données via le service managé de l'hébergeur, durant une fenêtre nocturne.
- **Rétention** : minimum sept (7) jours pour les sauvegardes de la base managée, dans tous les environnements. Le renforcement de cette durée en production, ainsi que la conservation d'instantanés manuels au-delà de la fenêtre de rotation, sont en cours de déploiement.
- **Chiffrement** des sauvegardes au repos avec les mêmes garanties que les bases de production.
- **Tests de restauration** périodiques documentés.
- **Stockage objet** redondé en classe multi-zones de disponibilité pour les fichiers candidats.

9. Sécurité organisationnelle et ressources humaines

9.1 Avant l'embauche

- Vérification des références dans la mesure permise par le droit applicable.
- Engagement contractuel de confidentialité (clauses dans les contrats de travail et de prestation).
- Sensibilisation préalable à l'accès à des données sensibles.

9.2 Pendant le contrat

- **Sensibilisation annuelle** obligatoire à la sécurité de l'information et à la protection des données pour l'ensemble des collaborateurs.
- **Formation à l'embauche** dans les trente (30) jours suivant l'arrivée, 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 d'évolutions réglementaires ou d'incidents significatifs.
- **Application du moindre privilège** : les habilitations sont attribuées sur la base du besoin d'en connaître et revues périodiquement.

9.3 Fin de contrat

- **Procédure formalisée de départ** : révocation immédiate des accès, restitution des équipements, rappel des obligations résiduelles de confidentialité.
- **Inventaire** des comptes et accès à clôturer (interne, sous-traitants, partenaires).

10. Continuité d'activité (PCA / PRA)

10.1 Architecture

- **Multi-AZ** sur les composants critiques de production (cf. § 7.3).
- **Bascule automatique** de la base de données entre zones de disponibilité en cas de défaillance d'une zone.
- **Distribution géographique** des sauvegardes au sein de la région européenne pour résilience.

10.2 Objectifs cibles en production

Indicateur	Définition	Objectif
RPO (*Recovery Point Objective*)	Volume maximal de données pouvant être perdues	≤ 24 heures
RTO (*Recovery Time Objective*)	Délai maximal de remise en service après incident majeur	≤ 4 heures

10.3 Tests

- Tests périodiques de restauration des sauvegardes et de bascule, documentés et tracés.
- Revue annuelle du PCA / PRA et mise à jour au regard des évolutions d'architecture.

11. Gestion des incidents de sécurité

11.1 Détection

- **Outils automatisés** : supervision applicative, suivi des erreurs, détection d'anomalies réseau et d'accès, scanners de vulnérabilités.
- **Signalement humain** : collaborateurs, clients, chercheurs en sécurité, tiers.

11.2 Réponse

Procédure conforme à la PSSI (§ 7) et au DPA (Article 8) :

1. **Détection** et qualification initiale par l'équipe technique ;
2. **Remontée immédiate** au Technical Lead et au DPO ;
3. **Cellule de crise** activée selon la gravité (Technical Lead + DPO + DG) ;
4. **Confinement** technique et collecte des éléments de preuve (journaux, traces réseau) ;
5. **Notification au client** sous **soixante-douze (72) heures** au plus tard à compter de la prise de connaissance, en cas de violation de Données traitées pour son compte (Annexe 4 du DPA — modèle de notification) ;
6. **Notification CNIL** par le DPO si Layan agit en qualité de Responsable de traitement et qu'il existe un risque pour les personnes, sous soixante-douze (72) heures ;
7. **Information des personnes concernées** si le risque est élevé (article 34 RGPD) ;
8. **Post-mortem** dans les trente (30) jours suivant la clôture, avec analyse de la cause racine, mesures correctives et mises à jour de procédures ;
9. **Tenue d'un registre des violations** par le DPO.

11.3 Couverture assurance

Layan dispose d'une **assurance cyber** couvrant les incidents portant atteinte à son système d'information, dont les attestations sont communicables sur demande motivée du client.

12. Gestion des vulnérabilités et tests de sécurité

12.1 Veille et correctifs

- **Veille active** sur les vulnérabilités CVE des composants logiciels et de l'infrastructure.
- **Suivi automatisé** des dépendances logicielles (analyse de composition logicielle) avec alerte sur publication de vulnérabilités.
- **Application des correctifs de sécurité critiques** sans délai indu après qualification (objectif : ≤ 7 jours pour les CVE critiques d'exposition externe, sauf contraintes opérationnelles documentées).

12.2 Tests de sécurité

- **Analyse statique du code (SAST)** intégrée aux pipelines de développement.
- **Analyse de composition logicielle (SCA)** sur les dépendances ouvertes.
- **Scans périodiques de vulnérabilités** de l'infrastructure exposée.
- **Tests d'intrusion (pentest)** réalisés à la demande du client dans le cadre de son droit d'audit (cf. § 14), ou périodiquement par des prestataires indépendants à l'initiative de Layan. Les conditions opérationnelles (fenêtre, périmètre, intensité) sont convenues préalablement par écrit pour ne pas affecter le service.

12.3 Isolation des environnements

- **Environnements** de développement, de test et de production strictement isolés (projets cloud, réseaux privés et identifiants distincts).
- **Données de production non utilisées** en environnement de développement sans anonymisation ou pseudonymisation préalable.
- **Politique de séparation des droits** entre les administrateurs des environnements.

13. Sous-traitance ultérieure

13.1 Principes

Layan recourt à des sous-traitants ultérieurs (au sens de l'article 28 §2 du RGPD) pour réaliser une partie de ses activités de traitement, notamment l'hébergement, la messagerie, l'analyse de CV, la supervision applicative, l'authentification SSO et la diffusion d'offres d'emploi.

Chaque sous-traitant ultérieur est :

- **encadré contractuellement** par un accord prévoyant des obligations en matière de protection des données équivalentes à celles imposées à Layan ;
- **sélectionné** sur la base de critères de sécurité et de conformité, avec revue périodique de la relation ;
- **listé** à l'**Annexe 3 du DPA**, mise à jour selon les modalités de l'Article 6.3 du DPA (notification écrite avec préavis minimum de trente (30) jours et droit d'objection motivé du client).

13.2 Liste actuelle

La liste à jour des sous-traitants ultérieurs nommément désignés, avec leur rôle, leur pays d'établissement et le cas échéant le mécanisme d'encadrement des transferts hors EEE, figure à l'**Annexe 3 du DPA** signé avec chaque client. Elle inclut notamment, à la date d'édition du présent PAS :

- **Scaleway SAS** — hébergement, base de données managée, stockage objet, diffusion de contenu (France, `fr-par`) ;
- **Cloudflare, Inc.** — DNS, diffusion périphérique, pare-feu applicatif et anti-DDoS, protection anti-robot (États-Unis, DPF + CCT) ;
- **Amazon Web Services EMEA SARL** — hébergement antérieur en lecture seule jusqu'au 31 octobre 2026 (UE : France et Irlande) ;
- **Brevo SAS** — routage courriel et SMS (France) ;
- **OpenAI Ireland Limited** — analyse de CV et génération de contenu, active par défaut (Irlande / États-Unis, DPF + CCT) ;
- **HRflow.ai (Riminder SAS)** — analyse de CV en solution de repli (France) ;
- **Cryptr SAS** — SSO optionnel (France) ;
- **Google Ireland Limited** — SSO Google, reCAPTCHA, autocomplétion d'adresse et cartographie, gestionnaire de balises (Irlande / États-Unis, DPF) ;
- **Microsoft Ireland Operations Limited** — SSO Microsoft / Azure AD / Entra ID (Irlande / États-Unis, DPF) ;
- **Cronofy Limited** — synchronisation calendrier optionnelle (Royaume-Uni, décision d'adéquation) ;
- **Sentry (Functional Software, Inc.)** — supervision applicative (États-Unis, CCT + DPF) ;
- **PostHog, Inc.** — analytics du back-office recruteur, *PostHog Cloud EU* (Union européenne, Francfort) ;
- **Content Square SAS** — mesure d'audience et rejeu de session du back-office recruteur (France) ;
- **ip-api.com** — géolocalisation d'adresse IP des visiteurs du site carrière (Australie, CCT) ;
- **Jawg SAS** — fond cartographique du site carrière (France) ;
- **OpenStreetMap Foundation** — fond cartographique du site carrière (Royaume-Uni, décision d'adéquation) ;
- **AssessFirst SAS** — évaluation prédictive optionnelle (France) ;
- **HubSpot Ireland Limited** — synchronisation CRM optionnelle (Irlande / États-Unis, DPF) ;
- **Lucca SAS**, **Eurécia SAS**, **Skello SAS** — synchronisations SIRH optionnelles (France) ;
- **Intercom R&D Unlimited Company** — support utilisateur et gestion des tickets (Irlande / États-Unis, DPF) ;
- **Slack Technologies Limited** — notifications opérationnelles internes (Irlande / États-Unis, DPF).

13.3 Transferts hors EEE

Les données sont traitées et stockées au sein de l'Union européenne. Lorsqu'un sous-traitant ultérieur est établi hors EEE ou y accède depuis un pays tiers, le transfert est encadré par l'un des mécanismes prévus aux articles 44 à 49 du RGPD (décision d'adéquation, Clauses Contractuelles Types 2021/914, EU-US Data Privacy Framework). Le détail figure à l'Annexe 3 du DPA.

14. Audit et droit de contrôle client

Conformément à l'**Article 5.8 du DPA**, le client peut faire procéder à un audit, par lui-même ou par un tiers indépendant mandaté et soumis à un engagement de confidentialité, dans les conditions suivantes :

- préavis écrit raisonnable, en principe de trente (30) jours ;
- audit réalisé pendant les heures ouvrables, sans perturber l'activité de Layan ;
- périmètre de l'audit limité aux données et systèmes du client demandeur (aucune information sur les autres clients de Layan) ;
- coût à la charge du client demandeur, sauf si l'audit révèle un manquement substantiel de Layan, auquel cas les frais sont supportés par Layan ;
- fréquence limitée à une (1) fois par année civile, sauf incident de sécurité avéré ou demande motivée d'une autorité de contrôle.

À l'issue de l'audit, Layan met en œuvre, à ses frais et dans un délai raisonnable, toute mesure corrective nécessaire pour remédier aux non-conformités constatées.

En complément, Layan met à la disposition du client, sur demande motivée :

- la documentation relative aux MTO (Annexe 2 du DPA et présent PAS) ;
- la liste à jour des sous-traitants ultérieurs (Annexe 3 du DPA) ;
- les rapports d'audit et attestations de conformité de ses propres sous-traitants ultérieurs lorsqu'ils sont disponibles, dans la limite des conditions de diffusion imposées par ces derniers ;
- l'attestation d'assurance cyber en cours.

15. Réversibilité et restitution des données

15.1 Pendant le contrat

Le client dispose à tout moment, depuis l'interface administrateur de la Plateforme, des fonctionnalités d'export suivantes :

- **Export des candidats** au format **CSV** ;
- **Export des offres** publiées et de leurs données associées ;
- **Téléchargement** des documents et CV stockés (par candidat).

Pour des besoins spécifiques (exports massifs, format alternatif), le client peut solliciter le support à `support@layan.eu`.

15.2 En fin de contrat

Conformément à l'**Article 5.7 du DPA**, à l'expiration ou à la résiliation du contrat principal, Layan procède, au choix du client exprimé par écrit dans un délai de **trente (30) jours** suivant la fin du contrat :

- à la **restitution** des données dans un format structuré, couramment utilisé et lisible par machine (export téléchargeable depuis la Plateforme : CSV pour les données structurées, archive des documents et CV pour le stockage objet, *dump* SQL de la base de données pour un export complet de l'organisation cliente) ; et / ou
- à la **suppression** définitive des données et de toutes les copies existantes.

À défaut d'instruction du client dans le délai de trente (30) jours, Layan procède à la **suppression définitive** des données trente (30) jours après cette échéance, sauf obligation légale contraire.

15.3 Coût

La restitution des données dans les formats standards mentionnés ci-dessus est **gratuite**. Les demandes spécifiques nécessitant un développement particulier peuvent faire l'objet d'un devis.

15.4 Sauvegardes résiduelles

Les sauvegardes contenant les données du client sont supprimées dans le cadre du cycle naturel de rotation des sauvegardes, dans un délai maximal correspondant à la durée de conservation des sauvegardes (cf. § 8.6). Pendant cette période résiduelle, les sauvegardes restent isolées, chiffrées et inaccessibles à toute utilisation autre que la restauration en cas d'incident.

15.5 Attestation

Une **attestation de suppression** peut être délivrée au client sur demande écrite à `support@layan.eu`.

16. Conformité réglementaire et normative

16.1 Cadre réglementaire

- **Règlement (UE) 2016/679 (RGPD)** ;
- **Loi française n° 78-17 du 6 janvier 1978 « Informatique et Libertés »** modifiée ;
- **Recommandations CNIL** applicables au secteur du recrutement ;
- **Directive ePrivacy** (2002/58/CE modifiée) et article 82 de la loi Informatique et Libertés (cookies et traceurs).

16.2 Référentiels d'alignement

Les mesures techniques et organisationnelles décrites au présent PAS sont alignées sur :

- les principes de la norme **ISO/IEC 27001:2022** et son amendement 2024 (Annexe A) ;
- les contrôles de l'**ISO/IEC 27002:2022** pour leur mise en œuvre détaillée ;

- les recommandations de l'**ANSSI** (notamment guides d'hygiène informatique et bonnes pratiques cloud) ;
- les bonnes pratiques de l'**OWASP** pour la sécurité applicative ;
- les **recommandations CNIL** spécifiques au recrutement (durée de conservation, droits des candidats).

16.3 Certifications

À la date d'édition du présent document :

- **Layan** n'est pas titulaire à titre propre d'une certification ISO 27001 ; une démarche d'alignement est en cours (cf. § 7.4).
- L'**hébergeur** est certifié ISO/IEC 27001 ; le périmètre exact et la liste à jour de ses certifications sont publiés par lui (cf. § 7.2).
- Les certifications des autres sous-traitants ultérieurs sont celles que ces derniers publient ; Layan communique sur demande motivée les attestations qu'elle détient.

Toute évolution de ces éléments est communiquée aux clients dans le cadre du cycle de revue annuelle du présent PAS.

17. Validation, communication et mise à jour

- Le présent PAS est **validé** par la Direction de Layan (Directeur Général et DPO).
- Il est **communiqué** aux clients et prospects sur demande, et tenu à disposition des autorités de contrôle.
- Il est **revu au minimum une fois par an** par le Technical Lead et le DPO, et systématiquement en cas de :
  - modification substantielle de l'architecture ;
  - évolution réglementaire majeure ;
  - incident de sécurité significatif ayant donné lieu à des mesures correctives durables ;
  - mise à jour de la PSSI (P1) ou de la PPD (P2).
- L'historique des versions est tenu en interne et communicable sur demande.

Pour toute question relative au présent Plan d'Assurance Sécurité, les contacts privilégiés sont :

- **Canal client / support** : `support@layan.eu`
- **Délégué à la Protection des Données (DPO)** : Aymen Ezzayer — `aymen@layan.eu`