

Registre des activités de traitement, Sous-traitant

1. Objet et statut du registre

Le présent document constitue le **registre des activités de traitement tenu par Layan SAS en qualité de sous-traitant**, en application de l'**article 30 (2) du Règlement (UE) 2016/679 (« RGPD »)** et de la loi française n° 78-17 du 6 janvier 1978 modifiée.

Il recense les traitements de données à caractère personnel que Layan effectue **pour le compte de ses clients**, lesquels agissent en qualité de **responsables de traitement**, dans le cadre de la mise à disposition de sa plateforme logicielle de gestion du recrutement (ATS — *Applicant Tracking System*).

Ce registre :

- **complète** la Politique de Protection des Données (P2 - PPD) § 14, qui en pose le principe ;
- est un **document interne d'accountability** (**article 24 RGPD**), non publié** aux clients ;
- est **tenu à la disposition de la CNIL** et communiqué sur demande (article 30 (4) RGPD) ;
- ne couvre **que** le volet **sous-traitant (article 30 (2))**. Les traitements pour lesquels Layan agit en **responsable de traitement** (données de ses collaborateurs, prospects B2B, visiteurs du site layan.eu) relèvent d'un **registre responsable (article 30 (1))** distinct, hors du présent document.

La **liste maîtresse des sous-traitants ultérieurs** est tenue à l'**Annexe 3 du DPA** ; le présent registre la reproduit (§ 7) et doit être maintenu en cohérence avec elle.

2. Identité et coordonnées du sous-traitant

Élément	Information
Sous-traitant	Layan SAS, société par actions simplifiée
Immatriculation	RCS Nanterre 891 123 432
Siège social	198 avenue de France, 75013 Paris (France)
Représentant légal	BZM , société par actions simplifiée (RCS Nanterre 989 314 067), Président, elle-même représentée par Benjamin Zerdoun
Direction générale	NCC , société par actions simplifiée (RCS Paris 989 385 901), Directeur Général, elle-même représentée par Nicolas Chevalier Cohen
Délégué à la Protection des Données (DPO)	Aymen Ezzayer — aymen@layan.eu
Canal client / personnes concernées	support@layan.eu

Le DPO est désigné en application de l'article 37 RGPD et exerce ses missions avec indépendance fonctionnelle (article 38 RGPD). Le registre est tenu et mis à jour sous sa responsabilité.

3. Responsables de traitement pour le compte desquels Layan agit

Layan agit en qualité de sous-traitant pour le compte de **l'ensemble de ses clients** ayant souscrit au Contrat Principal (Conditions Générales d'Utilisation et conditions particulières) et, le cas échéant, signé un Data Processing Agreement (DPA, article 28 RGPD).

Compte tenu du modèle SaaS multi-clients, la **liste nominative des responsables de traitement** (avec leurs coordonnées et, le cas échéant, celles de leur représentant et de leur DPO) n'est pas reproduite ici : elle est tenue dans le **référentiel contractuel / CRM de Layan** et communiquée à la CNIL sur demande. Chaque **DPA signé identifie nominativement** le responsable de traitement concerné.

4. Catégories de traitements effectués pour le compte des responsables

Le traitement consiste en la mise à disposition d'une plateforme ATS permettant au responsable de traitement de gérer ses opérations de recrutement. Il recouvre les catégories d'opérations suivantes (cf. DPA, Annexe 1 § 1) :

Activité de traitement	Description
Publication et diffusion d'offres	Création, publication et diffusion d'offres d'emploi, y compris vers des plateformes de diffusion tierces.
Collecte et gestion des candidatures	Réception, organisation, qualification et évaluation des candidatures ; gestion des statuts et des viviers de talents.
Communication avec les candidats	Échanges par courriel et SMS via la plateforme.
Campagnes et viviers	Gestion des campagnes de recrutement et des viviers de talents.
Site carrière	Édition et publication d'un site carrière sur un sous-domaine personnalisé du responsable.
Exports et restitution	Export et restitution des données traitées, dans un format structuré lisible par machine.
Options activées par le responsable	Analyse structurée de CV, authentification SSO d'entreprise, synchronisation de calendrier pour la planification d'entretiens, assistance à la rédaction de contenu.

Finalité générale : permettre au responsable de traitement de conduire ses processus de recrutement. Layan **ne traite pas** ces données pour ses propres finalités, à l'exception des données strictement techniques nécessaires à la sécurité, à la facturation et à la fourniture du service, qui relèvent d'un traitement distinct dont Layan est responsable (cf. registre Art. 30 (1), hors périmètre).

5. Catégories de personnes concernées et de données

5.1 Personnes concernées

- **Candidats** : personnes ayant postulé à une offre du responsable ou créé un profil sur son site carrière ;
- **Utilisateurs internes du responsable** : recruteurs, managers et administrateurs de l'organisation cliente ;
- **Visiteurs du site carrière** édité par le responsable (données techniques de connexion / statistiques) ;
- **Personnes de référence** désignées par un candidat lorsque le responsable recourt à la prise de références : leurs coordonnées et leur appréciation sont traitées alors qu'elles n'ont pas postulé.

5.2 Catégories de données traitées

Catégorie	Exemples
Identification	Civilité, genre (champ requis sur le formulaire de candidature public), nom, prénom
Contact	Adresse postale, courriel, numéro de téléphone
Données professionnelles	CV (texte et fichier), parcours, formation, expériences, compétences, langues, prétentions salariales
Candidature	Lettre de motivation, réponses aux questions de pré-qualification, statut, commentaires et évaluations des recruteurs, comptes-rendus d'entretien, résultats d'évaluation prédictive lorsque le responsable active cette option
Connexion	Identifiant utilisateur, adresse IP, horodatage, métadonnées de session, journal d'activité
Authentification	Mots de passe (uniquement sous forme hachée), jetons d'authentification SSO le cas échéant
Communication	Historique des courriels et SMS échangés via la plateforme

Catégories particulières (article 9 RGPD) : aucune n'est requise par la plateforme et aucun champ n'y est dédié. Les champs libres et les questionnaires configurés par le responsable (réponses de pré-qualification, réponses d'entretien, commentaires et notes des recruteurs) sont toutefois à format libre et leur contenu n'est ni restreint ni contrôlé par Layan : un responsable peut donc y faire figurer, sous sa propre responsabilité, des données relevant de l'article 9. Le contenu de ces champs est susceptible d'être transmis aux sous-traitants ultérieurs d'analyse de CV et de génération de contenu (cf. § 7.1). Si un responsable en collecte sous sa propre responsabilité, il en informe préalablement Layan et garantit l'existence d'une base juridique appropriée.

Données relatives aux condamnations pénales (article 10 RGPD) : néant.

6. Durées de conservation

La durée de conservation est **déterminée par chaque responsable de traitement** et paramétrée dans la plateforme, dans le respect des recommandations de la CNIL applicables au secteur du recrutement (cf. PPD § 10 et DPA, Annexe 1 § 4) :

Données	Durée
Données candidats	Paramétrée par le responsable, exprimée en années (1 an ou 2 ans proposés dans l'interface) ; valeur par défaut : 2 ans à compter de la date de candidature, le compteur étant réinitialisé par un consentement renouvelé. En l'absence de paramétrage, la valeur de repli appliquée est de 1 an .
Comptes et activité des utilisateurs internes du responsable	Durée du contrat client ; suppression ou anonymisation dans les 30 jours suivant la fin du contrat.
Données de suivi de visite du site carrière (adresse IP, ville, code postal)	48 heures , puis anonymisation irréversible par tâche planifiée quotidienne.
Journaux techniques et de connexion	12 mois visés (recommandation CNIL). Voir le § 11 pour l'écart constaté sur certains journaux applicatifs internes.

Modalités effectives de l'effacement. Une demande d'effacement traitée depuis l'interface RGPD appose un marqueur de suppression sur la candidature et la détache des offres et des viviers. La suppression matérielle des enregistrements et des fichiers associés (CV, pièces jointes, photo) est réalisée par une tâche planifiée **trois (3) mois** après ce marquage. Aucune étape d'anonymisation n'est appliquée aux enregistrements candidats : ils sont supprimés, non anonymisés.

Rappel périodique. Le rappel adressé aux responsables dont des candidats dépassent la durée de conservation est **inopérant à ce jour** (cf. § 11) ; la purge relève donc d'une action manuelle du responsable depuis l'interface RGPD.

À l'expiration, les données sont supprimées de manière irréversible ; les sauvegardes sont purgées dans leur cycle de rotation (cf. DPA, Annexe 2 § 6).

7. Destinataires et sous-traitants ultérieurs

Les données sont accessibles, dans la limite du besoin d'en connaître :

- aux **utilisateurs habilités du responsable de traitement** (recruteurs, managers, administrateurs) ;
- au **personnel habilité de Layan** soumis à une obligation de confidentialité (support, exploitation) ;
- aux **sous-traitants ultérieurs** ci-dessous, encadrés par contrat (article 28 (4) RGPD).

Source unique : la liste ci-dessous reproduit l'**Annexe 3 du DPA**, qui en constitue la version maîtresse. Toute évolution est portée d'abord à l'Annexe 3 (avec changement de version), puis répercutée ici. Toute modification est notifiée aux responsables avec un préavis de **30 jours** et un droit d'objection motivé (DPA, article 6.3).

7.1 Sous-traitants ultérieurs nommément désignés

Nom	Rôle	Pays / Région	Catégories de données concernées	Transfert hors EEE
Scaleway SAS	Hébergement, base de données managée, stockage objet, diffusion de contenu, gestion des secrets	France — région fr-par (Paris)	Toutes catégories (cœur du service)	N/A (UE)
Cloudflare, Inc.	DNS, diffusion de contenu, pare-feu applicatif et anti-DDoS, protection anti-robot (<i>Turnstile</i>)	États-Unis — réseau mondial, points de présence UE	Adresse IP et métadonnées de requête de tout visiteur, y compris candidats	EU-US Data Privacy Framework et Clauses Contractuelles Types
Amazon Web Services EMEA SARL	Hébergement antérieur conservé en lecture seule , sans écriture nouvelle, jusqu'à suppression définitive prévue au plus tard le 31 octobre 2026	Union européenne — régions France (Paris) et Irlande	Fichiers et pièces jointes antérieurs à la migration	N/A (UE)
Brevo SAS (anciennement Sendinblue)	Routage des courriels transactionnels et des SMS	France	Identification, contact, numéro de téléphone, contenu de la communication	N/A (UE)
OpenAI Ireland Limited	Analyse structurée de CV et génération de contenu — active par défaut lors du dépôt d'un CV	Irlande / États-Unis	Texte intégral du CV, identification, adresse postale, courriel, numéro de téléphone	EU-US Data Privacy Framework et / ou Clauses Contractuelles Types
HRflow.ai (Riminder SAS)	Analyse structurée de CV, en solution de repli lorsque l'extraction locale échoue	France	Fichier de CV et son contenu	N/A (UE)
CrypTr SAS	Authentification SSO d'entreprise (option)	France	Identification, courriel, jetons d'authentification	N/A (UE)

Nom	Rôle	Pays / Région	Catégories de données concernées	Transfert hors EEE
Google Ireland Limited	SSO Google (option), reCAPTCHA, autocomplétion d'adresse et fond cartographique du formulaire de candidature, gestionnaire de balises	Irlande / États-Unis	Identification, courriel, adresse IP, saisies partielles d'adresse	EU-US Data Privacy Framework
Microsoft Ireland Operations Limited	SSO Microsoft / Azure AD / Entra ID (option)	Irlande / États-Unis	Identification, courriel, jetons d'authentification	EU-US Data Privacy Framework
Cronofy Limited	Synchronisation calendrier pour la planification d'entretiens (option)	Royaume-Uni	Évènements de calendrier, courriels des participants	Décision d'adéquation Royaume-Uni
Sentry (Functional Software, Inc.)	Supervision applicative et suivi des erreurs	États-Unis	Identifiant utilisateur, courriel, adresse IP, métadonnées de requête HTTP	Clauses Contractuelles Types et EU-US Data Privacy Framework
PostHog, Inc.	Analytics produit du back-office recruteur (<i>PostHog Cloud EU</i>)	Union européenne — Francfort	Identifiant pseudonyme, adresse IP, évènements d'usage des utilisateurs internes	N/A (UE)
Content Square SAS	Mesure d'audience et rejeu de session du back-office recruteur	France	Adresse IP, évènements d'interface et enregistrements d'écran des utilisateurs internes, susceptibles de faire apparaître des données candidat affichées	N/A (UE)
ip-api.com	Géolocalisation de l'adresse IP des visiteurs du site carrière (statistiques de visite)	Australie	Adresse IP du visiteur	Clauses Contractuelles Types
Jawg SAS	Fond cartographique du site carrière (version 1)	France	Adresse IP du visiteur	N/A (UE)
OpenStreetMap Foundation	Fond cartographique du site carrière (version 2, par défaut)	Royaume-Uni	Adresse IP du visiteur	Décision d'adéquation Royaume-Uni

Nom	Rôle	Pays / Région	Catégories de données concernées	Transfert hors EEE
AssessFirst SAS	Évaluation prédictive et psychométrique des candidats (option)	France	Identification, courriel, résultats d'évaluation conservés sur la fiche candidat	N/A (UE)
HubSpot Ireland Limited	Synchronisation CRM (option)	Irlande / États-Unis	Identification, courriel, numéro de téléphone, situation professionnelle	EU-US Data Privacy Framework
Lucca SAS	Synchronisation SIRH (option)	France	Identification, courriel	N/A (UE)
Eurécia SAS	Synchronisation SIRH (option)	France	Nom, courriel, numéros de téléphone	N/A (UE)
Skello SAS	Synchronisation SIRH — intégration présente mais non sélectionnable à ce jour dans l'interface de connexion	France	Nom, courriel, données de contrat	N/A (UE)
Intercom R&D Unlimited Company	Support utilisateur (messagerie intégrée et courriel), gestion des tickets	Irlande / États-Unis	Identification et courriel des utilisateurs internes du responsable, contenu des échanges de support	EU-US Data Privacy Framework
Slack Technologies Limited	Notifications opérationnelles internes du sous-traitant	Irlande / États-Unis	Métadonnées techniques et, pour certaines alertes, nom et courriel d'un utilisateur interne	EU-US Data Privacy Framework

7.2 Sous-traitants ultérieurs catégorisés

Catégorie	Description	Données concernées
Plateformes de diffusion d'offres d'emploi	Réception et publication des offres diffusées par le responsable depuis la plateforme. Aucune donnée candidat n'est transmise, sauf : (i) flux d'« easy apply » explicitement activé par le responsable ; (ii) retour du statut de candidature vers la plateforme d'origine lorsque celle-ci le prévoit — à ce jour Indeed , à qui sont transmis un identifiant pseudonyme et l'issue du recrutement.	Données de l'offre publiée ; le cas échéant, données candidat en cas d'« easy apply » ; identifiant pseudonyme et issue du recrutement
Fournisseur de courrier entrant (IMAP)	Récupération des courriels candidats dans le compte de messagerie configuré par le responsable.	Données du compte de messagerie configuré par le responsable

8. Transferts de données hors EEE

Le traitement et le stockage principaux sont réalisés **au sein de l'Union européenne — région France, zone `fr-par` (Paris)**. Un hébergement antérieur subsiste **en lecture seule** dans les régions européennes **France (Paris) et Irlande**, jusqu'à sa suppression définitive prévue au plus tard le **31 octobre 2026**.

Certains sous-traitants ultérieurs (cf. § 7) sont établis hors EEE ou y accèdent à des données : États-Unis (diffusion périphérique et pare-feu applicatif, supervision applicative, CRM optionnel), Royaume-Uni (synchronisation calendrier, fonds cartographiques) et Australie (géolocalisation d'adresse IP). Dans ce cas, le transfert est encadré par l'un des mécanismes des articles 44 à 49 RGPD (cf. DPA, article 7 et PPD § 12) :

- **décision d'adéquation** de la Commission européenne (par exemple le Royaume-Uni — article 45) ;
- **Clauses Contractuelles Types** (décision (UE) 2021/914 du 4 juin 2021 — article 46) ;
- pour les États-Unis : **EU-US Data Privacy Framework** lorsque le sous-traitant en est certifié, à défaut **Clauses Contractuelles Types**.

Aucun transfert hors EEE n'est réalisé sans l'un de ces encadrements.

9. Description générale des mesures techniques et organisationnelles (article 32 RGPD)

Les mesures de sécurité sont décrites en détail à l'**Annexe 2 du DPA** et dans la **PSSI (P1 - PSI)**. En synthèse :

- **Chiffrement** : en transit (TLS 1.2 minimum, préférence TLS 1.3) ; au repos, stockage objet chiffré au niveau du compartiment en **AES-256** avec clés gérées par l'hébergeur, bases de données et sauvegardes sur service managé chiffrant les volumes au repos ; secrets en coffre-fort chiffré, jamais en clair dans le code.
- **Contrôle d'accès** : authentification individuelle, moindre privilège, revue périodique, **cloisonnement strict des données par organisation cliente**. MFA : déploiement **prévu** pour les comptes à privilèges.
- **Réseau** : réseau privé cloisonné, pare-feu applicatif (WAF) et anti-DDoS **déployés** au niveau du réseau de diffusion périphérique, politiques réseau en refus par défaut, absence d'accès SSH direct depuis Internet.
- **Journalisation et supervision** : journal d'activité (qui a accédé à quoi, quand), détection d'anomalies.
- **Sauvegardes et continuité** : sauvegardes quotidiennes chiffrées, rétention 7 jours (renforcement en production en cours de déploiement), tests de restauration, PCA/PRA (RPO ≤ 24 h, RTO ≤ 4 h).
- **Gestion des violations** : notification au responsable sous **72 heures** (DPA, article 8).
- **Personnel** : engagement de confidentialité, sensibilisation annuelle, révocation des accès au départ.

10. Tenue et révision du registre

Élément	Valeur
Version	1.2
Date de mise à jour	Septembre 2026
Responsable de la tenue	Aymen Ezzayer (DPO) — aymen@layan.eu
Fréquence de révision	Au minimum annuelle ; révision déclenchée par tout ajout/retrait de sous-traitant ultérieur, évolution des catégories de traitement, des durées de conservation ou des mécanismes de transfert.
Mise à disposition	Tenu à la disposition de la CNIL et communiqué sur demande (article 30 (4) RGPD).

11. Risques résiduels identifiés

Les écarts suivants entre la mesure décrite et la mesure effectivement appliquée sont consignés ici au titre de l'*accountability* (article 24 RGPD). Ils sont suivis dans le backlog de conformité et revus à chaque révision du présent registre.

11.1 Documents candidats accessibles publiquement

Les préfixes de stockage objet contenant les **CV, lettres de motivation, pièces jointes, photos et vidéos d'entretien** sont servis en lecture anonyme, avec une mise en cache longue durée. Le seul contrôle d'accès est l'imprévisibilité de la clé d'objet, dérivée d'un identifiant fondé sur l'horodatage de dépôt à la microseconde : l'entropie réelle est donc voisine de celle de l'instant de dépôt, et non celle d'une clé aléatoire. Un tiers connaissant la date de candidature dispose d'un espace de recherche exploitable, sans avoir besoin d'un oracle puisqu'une clé correcte renvoie directement le document.

Les fichiers d'export destinés aux recruteurs incorporent ces adresses sous forme de liens directs, ce qui constitue une capacité d'accès non authentifiée circulant par courriel.

Le passage de ces préfixes en accès privé est planifié et conditionné à la réécriture du chemin de lecture applicatif. **Mesure compensatoire actuelle** : refus d'énumération du compartiment, exclusion des exports complets par tenant de tout accès anonyme, et expiration automatique de ces exports à **30 jours**.

11.2 Journaux applicatifs internes sans purge

La durée de **12 mois** visée au § 6 est appliquée aux journaux techniques et de connexion. En revanche, le journal d'activité produit, le journal des appels aux plateformes de diffusion et les journaux d'envoi de courriels et de SMS **ne font l'objet d'aucune tâche de purge à ce jour** et croissent sans limite. Le journal des appels aux plateformes de diffusion conserve le corps intégral des requêtes et des réponses.

11.3 Délai et portée de l'effacement

Comme indiqué au § 6, l'effacement matériel intervient **trois (3) mois** après la demande. Par ailleurs, lorsqu'une candidature est supprimée, le **nom du candidat subsiste dans le libellé textuel** des lignes du journal d'activité qui la mentionnaient, ces libellés étant construits par interpolation au moment de l'événement. Il s'agit d'une donnée personnelle résiduelle postérieure à l'effacement.

11.4 Rappel de conservation inopérant

Le rappel périodique destiné aux responsables dont des candidats dépassent la durée de conservation ne s'exécute pas, en raison d'une incohérence entre la valeur attendue et la valeur enregistrée pour le mode de conservation. Conséquence : **aucun mode de purge automatique n'est actif** et la purge dépend d'une action manuelle du responsable.

11.5 Accès par délégation non journalisé

Le personnel habilité de Layan peut ouvrir une session sous l'identité d'un utilisateur client à des fins de support. **Cette opération ne produit pas d'entrée dans le journal d'activité**, ce qui limite la portée de la traçabilité « qui a accédé à quoi, quand » décrite au § 9 et à l'Annexe 2 § 5 du DPA.

11.6 Champs libres et catégories particulières

Comme indiqué au § 5.2, les champs libres et questionnaires configurés par le responsable peuvent recevoir des données relevant de l'article 9 sans que Layan en restreigne le contenu, et ce contenu est susceptible d'être transmis aux sous-traitants d'analyse de CV et de génération de contenu.

11.7 Transmissions techniques à surveiller

- La géolocalisation de l'adresse IP des visiteurs du site carrière est appelée **en clair (HTTP)** ; le passage en HTTPS et la conclusion d'un acte de sous-traitance sont à engager.
- L'analytics du back-office recruteur n'est **pas encore soumis à un recueil de consentement** ; le bandeau correspondant est planifié.
- La télémétrie d'exploitation conserve les lignes de requête **90 jours** et les traces d'erreur **un an**, porteuses d'un identifiant utilisateur pseudonyme et de l'identifiant de l'organisation cliente.

Fin du registre — Sous-traitant (Art. 30(2)).

Layan SAS — RCS Nanterre 891 123 432 — 198 avenue de France, 75013 Paris. Contact DPO : Aymen Ezzayer — aymen@layan.eu — canal client : support@layan.eu.