

Record of Processing Activities, Processor

Language. This English version is provided for information. The French version is the binding one under French law; in the event of any discrepancy between the two, the French version prevails.

1. Purpose and status of the register

This document is the **record of processing activities maintained by Layan SAS acting as a processor**, pursuant to **Article 30(2) of Regulation (EU) 2016/679 (the "GDPR")** and French Law No. 78-17 of 6 January 1978 as amended.

It records the processing of personal data that Layan carries out **on behalf of its clients**, who act as **controllers**, in the context of the provision of its recruitment management software platform (ATS — *Applicant Tracking System*).

This register:

- **complements** the Data Protection Policy (P2 - PPD) § 14, which sets out its principle;
- is an **internal accountability document** (Article 24 GDPR), **not published** to clients;
- is **held at the disposal of the CNIL** and provided on request (Article 30(4) GDPR);
- covers **only the processor side (Article 30(2))**. Processing for which Layan acts as a **controller** (its staff, B2B prospects, `layan.eu` visitors) belongs to a separate **controller register (Article 30(1))**, outside this document.

The **master list of sub-processors** is held in **DPA Annex 3**; this register reproduces it (§ 7) and must be kept consistent with it.

2. Identity and contact details of the processor

Item	Information
Processor	Layan SAS, simplified joint-stock company (<i>société par actions simplifiée</i>)
Registration	RCS Nanterre 891 123 432
Registered office	198 avenue de France, 75013 Paris (France)
Legal representative	BZM , a société par actions simplifiée (Nanterre Trade and Companies Register 989 314 067), President, itself represented by Benjamin Zerdoun
Executive management	NCC , a société par actions simplifiée (Paris Trade and Companies Register 989 385 901), Chief Executive Officer, itself represented by Nicolas Chevalier Cohen
Data Protection Officer (DPO)	Aymen Ezzayer — <code>aymen@layan.eu</code>

Item	Information
Client / data-subject channel	support@layan.eu

The DPO is appointed pursuant to Article 37 GDPR and performs the role with functional independence (Article 38 GDPR). The register is maintained and updated under the DPO's responsibility.

3. Controllers on behalf of which Layan acts

Layan acts as a processor on behalf of **all of its clients** that have subscribed to the Main Agreement (General Terms of Use and applicable specific conditions) and, where applicable, signed a Data Processing Agreement (DPA, Article 28 GDPR).

Given the multi-client SaaS model, the **named list of controllers** (with their contact details and, where applicable, those of their representative and DPO) is not reproduced here: it is held in **Layan's contractual repository / CRM** and provided to the CNIL on request. Each **signed DPA names** the relevant controller.

4. Categories of processing carried out on behalf of controllers

The processing consists in providing an ATS platform enabling the controller to manage its recruitment operations. It covers the following categories of operations (see DPA, Annex 1 § 1):

Processing activity	Description
Publication and distribution of offers	Creation, publication and distribution of job offers, including to third-party distribution platforms.
Collection and management of applications	Receipt, organisation, qualification and evaluation of applications; status and talent-pool management.
Communication with candidates	Exchanges by email and SMS via the platform.
Campaigns and talent pools	Management of recruitment campaigns and talent pools.
Career site	Editing and publishing a career site on a controller-specific subdomain.
Exports and return of data	Export and return of processed data in a structured, machine-readable format.
Options enabled by the controller	Structured CV parsing, enterprise SSO authentication, calendar synchronisation for interview scheduling, content-writing assistance.

General purpose: to enable the controller to conduct its recruitment processes. Layan **does not process** this data for its own purposes, save for strictly technical data necessary for security, billing and service provision, which is subject to separate processing for which Layan is the controller (see Art. 30(1))

register, out of scope).

5. Categories of data subjects and data

5.1 Data subjects

- **Candidates:** persons who have applied to a controller's offer or created a profile on its career site;
- **Internal users of the controller:** recruiters, managers and administrators of the client organisation;
- **Visitors to the career site** edited by the controller (technical connection data / visit statistics);
- **Referees** nominated by a candidate where the controller uses reference checking: their contact details and appraisal are processed although they have not applied.

5.2 Categories of data processed

Category	Examples
Identification	Title, gender (a required field on the public application form), surname, first name
Contact	Postal address, email, telephone number
Professional data	CV (text and file), career history, education, experience, skills, languages, salary expectations
Application	Cover letter, answers to pre-qualification questions, status, recruiter comments and evaluations, interview reports, predictive-assessment results where the controller enables that option
Connection	User identifier, IP address, timestamp, session metadata, activity log
Authentication	Passwords (hashed form only), SSO authentication tokens where applicable
Communication	History of emails and SMS exchanged via the platform

Special categories (Article 9 GDPR): none required by the platform and no field is dedicated to it. The free-text fields and questionnaires configured by the controller (pre-qualification answers, interview answers, recruiter comments and notes) are nevertheless free-form and their content is neither restricted nor screened by Layan: a controller may therefore enter Article 9 data there under its own responsibility. The content of those fields may be transmitted to the CV-analysis and content-generation sub-processors (see § 7.1). If a controller collects such data under its own responsibility, it informs Layan beforehand and ensures an appropriate legal basis exists.

Data relating to criminal convictions (Article 10 GDPR): none.

6. Retention periods

The retention period is **set by each controller** and configured in the platform, in compliance with the CNIL recommendations applicable to the recruitment sector (see PPD § 10 and DPA, Annex 1 § 4):

Data	Period
Candidate data	Configured by the controller, expressed in years (1 year or 2 years offered in the interface); default value: 2 years from the application date, the counter being reset by renewed consent. Absent any configuration, the fallback value applied is 1 year .
Controller's internal-user accounts and activity	Duration of the client contract; deletion or anonymisation within 30 days of contract end.
Career-site visit-tracking data (IP address, city, postcode)	48 hours , then irreversible anonymisation by a daily scheduled task.
Technical and connection logs	12 months targeted (CNIL recommendation). See § 11 for the gap observed on certain internal application logs.

How erasure actually operates. An erasure request handled from the GDPR interface places a deletion marker on the application and detaches it from offers and talent pools. Physical deletion of the records and associated files (CV, attachments, photo) is carried out by a scheduled task **three (3) months** after that marking. No anonymisation step is applied to candidate records: they are deleted, not anonymised.

Periodic reminder. The reminder sent to controllers holding candidates past the retention period is **inoperative at present** (see § 11); purging therefore depends on a manual action by the controller from the GDPR interface.

On expiry, data is irreversibly deleted; backups are purged within their rotation cycle (see DPA, Annex 2 § 6).

7. Recipients and sub-processors

Data is accessible, on a need-to-know basis, to:

- the controller's **authorised users** (recruiters, managers, administrators);
- Layan's **authorised personnel** bound by confidentiality (support, operations);
- the **sub-processors** below, governed by contract (Article 28(4) GDPR).

Single source of truth: the list below reproduces **DPA Annex 3**, which is the master version. Any change is made first in Annex 3 (with a version bump), then mirrored here. Any change is notified to controllers with **30 days'** prior notice and a right of reasoned objection (DPA, Article 6.3).

7.1 Sub-processors specifically named

Name	Role	Country / Region	Categories of data concerned	Transfer outside EEA
Scaleway SAS	Hosting, managed database, object storage, content delivery, secrets management	France — region fr-par (Paris)	All categories (core service)	N/A (EU)
Cloudflare, Inc.	DNS, content delivery, web application firewall and DDoS protection, anti-bot protection (<i>Turnstile</i>)	United States — global network, EU points of presence	IP address and request metadata of every visitor, including candidates	EU-US Data Privacy Framework and Standard Contractual Clauses
Amazon Web Services EMEA SARL	Previous hosting retained read-only , with no new writes, until final deletion scheduled no later than 31 October 2026	European Union — France (Paris) and Ireland regions	Files and attachments predating the migration	N/A (EU)
Brevo SAS (formerly Sendinblue)	Routing of transactional emails and SMS	France	Identification, contact, phone number, communication content	N/A (EU)
OpenAI Ireland Limited	Structured CV parsing and content generation — active by default when a CV is uploaded	Ireland / United States	Full CV text, identification, postal address, email, phone number	EU-US Data Privacy Framework and / or Standard Contractual Clauses
HRflow.ai (Riminder SAS)	Structured CV parsing, as a fallback where local extraction fails	France	CV file and its content	N/A (EU)
Crypтр SAS	Enterprise SSO authentication (option)	France	Identification, email, authentication tokens	N/A (EU)
Google Ireland Limited	Google SSO (option), reCAPTCHA, address autocomplete and map tiles on the application form, tag manager	Ireland / United States	Identification, email, IP address, partial address input	EU-US Data Privacy Framework
Microsoft Ireland Operations Limited	Microsoft / Azure AD / Entra ID SSO (option)	Ireland / United States	Identification, email, authentication tokens	EU-US Data Privacy Framework

Name	Role	Country / Region	Categories of data concerned	Transfer outside EEA
Cronofy Limited	Calendar synchronisation for interview scheduling (option)	United Kingdom	Calendar events, participants' emails	UK adequacy decision
Sentry (Functional Software, Inc.)	Application monitoring and error tracking	United States	User identifier, email, IP address, HTTP request metadata	Standard Contractual Clauses and EU-US Data Privacy Framework
PostHog, Inc.	Product analytics for the recruiter back-office (<i>PostHog Cloud EU</i>)	European Union — Frankfurt	Pseudonymous identifier, IP address, usage events of internal users	N/A (EU)
Content Square SAS	Audience measurement and session replay of the recruiter back-office	France	IP address, interface events and screen recordings of internal users, which may reveal candidate data displayed on screen	N/A (EU)
ip-api.com	Geolocation of career-site visitors' IP addresses (visit statistics)	Australia	Visitor's IP address	Standard Contractual Clauses
Jawg SAS	Career-site map tiles (version 1)	France	Visitor's IP address	N/A (EU)
OpenStreetMap Foundation	Career-site map tiles (version 2, default)	United Kingdom	Visitor's IP address	UK adequacy decision
AssessFirst SAS	Predictive and psychometric assessment of candidates (option)	France	Identification, email, assessment results retained on the candidate record	N/A (EU)
HubSpot Ireland Limited	CRM synchronisation (option)	Ireland / United States	Identification, email, phone number, professional situation	EU-US Data Privacy Framework
Lucca SAS	HRIS synchronisation (option)	France	Identification, email	N/A (EU)
Eurécia SAS	HRIS synchronisation (option)	France	Surname, email, phone numbers	N/A (EU)
Skello SAS	HRIS synchronisation — integration present but not currently selectable in the connection interface	France	Surname, email, contract data	N/A (EU)

Name	Role	Country / Region	Categories of data concerned	Transfer outside EEA
Intercom R&D Unlimited Company	User support (embedded messaging and email), ticket handling	Ireland / United States	Identification and email of the controller's internal users, content of support exchanges	EU-US Data Privacy Framework
Slack Technologies Limited	Internal operational notifications of the processor	Ireland / United States	Technical metadata and, for certain alerts, the name and email of an internal user	EU-US Data Privacy Framework

7.2 Categorised sub-processors

Category	Description	Data concerned
Job board distribution platforms	Reception and publication of offers disseminated by the controller from the platform. No candidate data is transmitted, except: (i) an "easy apply" flow explicitly enabled by the controller; (ii) return of the application status to the originating platform where it provides for this — currently Indeed , to which a pseudonymous identifier and the hiring outcome are transmitted.	Published offer data; where applicable, candidate data in case of "easy apply"; pseudonymous identifier and hiring outcome
Inbound mail provider (IMAP)	Retrieval of candidate emails from the mailbox configured by the controller.	Data of the mailbox configured by the controller

8. Transfers of data outside the EEA

Primary processing and storage take place **within the European Union — France region, zone `fr-par` (Paris)**. A previous hosting arrangement remains **read-only** in the European regions **France (Paris)** and **Ireland**, until its final deletion scheduled no later than **31 October 2026**.

Certain sub-processors (see § 7) are established outside the EEA or access data from there: the United States (edge delivery and web application firewall, application monitoring, optional CRM), the United Kingdom (calendar synchronisation, map tiles) and Australia (IP-address geolocation). In such cases, the transfer is governed by one of the mechanisms of Articles 44 to 49 GDPR (see DPA, Article 7 and PPD § 12):

- a Commission **adequacy decision** (e.g. the United Kingdom — Article 45);
- **Standard Contractual Clauses** (Implementing Decision (EU) 2021/914 of 4 June 2021 — Article 46);
- for the United States: the **EU-US Data Privacy Framework** where the sub-processor is certified, otherwise Standard Contractual Clauses.

No transfer outside the EEA takes place without one of these safeguards.

9. General description of technical and organisational measures (Article 32 GDPR)

Security measures are described in detail in **DPA Annex 2** and in the **PSSI (P1 - PSI)**. In summary:

- **Encryption:** in transit (TLS 1.2 minimum, TLS 1.3 preferred); at rest, object storage encrypted at bucket level with **AES-256** and provider-managed keys, databases and backups on a managed service encrypting volumes at rest; secrets in an encrypted vault, never in clear text in the code.
- **Access control:** individual authentication, least privilege, periodic review, **strict data segregation per client organisation**. MFA: deployment **planned** for privileged accounts.
- **Network:** segregated private network, web application firewall (WAF) and DDoS protection **deployed** at the edge delivery network, default-deny network policies, no direct SSH access from the Internet.
- **Logging and monitoring:** activity log (who accessed what, when), anomaly detection.
- **Backups and continuity:** daily encrypted backups, 7-day retention (extended production retention being rolled out), restore testing, BCP/DRP (RPO $\leq$ 24 h, RTO $\leq$ 4 h).
- **Breach management:** notification to the controller within **72 hours** (DPA, Article 8).
- **Personnel:** confidentiality undertaking, annual awareness training, access revocation on departure.

10. Maintenance and review of the register

Item	Value
Version	1.2
Update date	September 2026
Maintained by	Aymen Ezzayer (DPO) — aymen@layan.eu
Review frequency	At least annually; triggered review on any addition/removal of a sub-processor, change to categories of processing, retention periods or transfer mechanisms.
Availability	Held at the disposal of the CNIL and provided on request (Article 30(4) GDPR).

11. Identified residual risks

The following gaps between the measure as described and the measure as actually applied are recorded here for accountability purposes (Article 24 GDPR). They are tracked in the compliance backlog and reviewed at each revision of this register.

11.1 Candidate documents publicly accessible

The object-storage prefixes holding **CVs, cover letters, attachments, photographs and interview videos** are served on anonymous read, with long-lived caching. The only access control is the unpredictability of the object key, which is derived from an identifier based on the microsecond timestamp of the upload: the real entropy is therefore close to that of the moment of upload, not that of a random key. A third party who knows the application date has a tractable search space, and needs no oracle, since a correct key returns the document directly.

Recruiter export files embed these addresses as direct links, which constitutes an unauthenticated access capability circulating by email.

Moving these prefixes to private access is planned and conditional on rewriting the application read path. **Current compensating measures:** bucket listing denied, full per-tenant exports excluded from any anonymous access, and automatic expiry of those exports at **30 days**.

11.2 Internal application logs without purge

The **12-month** period targeted in § 6 applies to technical and connection logs. By contrast, the product activity log, the log of calls to distribution platforms and the email and SMS dispatch logs are **subject to no purge task at present** and grow without limit. The log of calls to distribution platforms retains the full body of requests and responses.

11.3 Delay and scope of erasure

As stated in § 6, physical erasure occurs **three (3) months** after the request. In addition, when an application is deleted, the **candidate's name persists in the textual label** of the activity-log lines that mentioned it, those labels being built by interpolation at the time of the event. This is residual personal data after erasure.

11.4 Retention reminder inoperative

The periodic reminder intended for controllers holding candidates past the retention period does not run, owing to an inconsistency between the expected value and the stored value for the retention mode. As a result, **no automatic purge mode is active** and purging depends on a manual action by the controller.

11.5 Delegated access not logged

Authorised Layan staff can open a session under the identity of a client user for support purposes. **This operation produces no entry in the activity log**, which limits the scope of the "who accessed what, when" traceability described in § 9 and in Annex 2 § 5 of the DPA.

11.6 Free-text fields and special categories

As stated in § 5.2, the free-text fields and questionnaires configured by the controller may receive Article 9 data without Layan restricting their content, and that content may be transmitted to the CV-analysis and content-generation sub-processors.

11.7 Technical transmissions to monitor

- Geolocation of career-site visitors' IP addresses is called **in clear text (HTTP)**; moving to HTTPS and concluding a processing agreement are to be undertaken.
- Recruiter back-office analytics is **not yet subject to consent collection**; the corresponding banner is planned.
- Operational telemetry retains request lines for **90 days** and error traces for **one year**, carrying a pseudonymous user identifier and the client organisation identifier.

End of register — Processor (Art. 30(2)).

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