Personal Data Protection Policy

> **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. Context

Objectives

This policy (hereinafter the "**Policy**" or "**PPD**" — *Politique de Protection des Données*) sets out the commitments of **LAYAN SAS** regarding the protection of personal data, in compliance with Regulation (EU) 2016/679 of 27 April 2016 ("**GDPR**") and French law no. 78-17 of 6 January 1978 as amended ("**Informatique et Libertés**").

It aims to:

- Establish Layan's overall approach to data protection;
- Document the principles, roles and internal procedures;
- Ensure compliance with the rights of data subjects;
- Demonstrate Layan's compliance (accountability principle — Article 24 GDPR);
- Complement, on the data protection side, the **Information Systems Security Policy** of internal reference **P1 - PSI**, to which it refers for everything related to technical security measures.

Articulation with the PSSI (P1)

This PPD and the PSSI (P1) together constitute the documentary foundation of Layan's compliance:

- **P1 - PSI** covers technical and organisational information security (access control, hosting, testing, incident management, physical security, human resources).
- **P2 - PPD** covers GDPR governance: principles, data subject rights, retention, sub-processing, transfers outside the EU, DPO role.

They are complementary. Any change to one triggers a review of the other.

2. Definitions

- **Personal Data ("Data")**: any information relating to an identified or identifiable natural person (Article 4 (1) GDPR).
- **Processing**: any operation or set of operations performed on Data (Article 4 (2) GDPR).

- **Controller**: the legal entity that determines the purposes and means of the Processing (Article 4 (7) GDPR).
- **Processor**: the legal entity that processes Data on behalf of the Controller (Article 4 (8) GDPR).
- **Data Subject**: the natural person to whom the Data relates.
- **Personal Data Breach**: a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Data (Article 4 (12) GDPR).
- **DPO (Data Protection Officer)**: person designated by Layan to oversee GDPR compliance (Articles 37 to 39 GDPR).
- **DPIA (Data Protection Impact Assessment)**: formalised analysis of the risks of a high-risk processing (Article 35 GDPR).
- **EEA**: European Economic Area.

For other definitions (employees, contractors, company, key assets), please refer to the PSSI (P1, § 1).

3. Scope

This Policy applies to:

- all **employees and staff** of Layan SAS (employees, work-study students, interns, executives, contractors);
- all **contractors and suppliers** of Layan having access, even occasionally, to Data processed by Layan;
- the **clients** of Layan in the context of their use of the ATS (Applicant Tracking System) platform published by Layan;
- all **Data Processing** carried out by Layan, whether acting as **Controller** (e.g. data of its own employees, prospects and clients) or as **Processor** (e.g. candidate data processed on behalf of clients).

4. Management commitment

The management of Layan SAS, represented by its President, **BZM** (Nanterre Trade and Companies Register 989 314 067), itself represented by **Benjamin Zerdoun**, and its Chief Executive Officer, **NCC** (Paris Trade and Companies Register 989 385 901), itself represented by **Nicolas Chevalier Cohen**, jointly with the Data Protection Officer, **Aymen Ezzayer**, undertakes to:

- place data protection at the heart of the company's governance;
- provide the Data Protection Officer with the means necessary for the exercise of his missions;
- integrate data protection from the design of products and processes (*privacy by design*) and by default (*privacy by default*);
- fully cooperate with the *Commission Nationale de l'Informatique et des Libertés* ("**CNIL**") and any other competent supervisory authority;

- review this Policy and the PSSI (P1) annually.

This procedure was reviewed and approved by Management in September 2026.

5. Governance and responsibilities

Role	Person	Responsibilities
President	**BZM** SAS (Nanterre Trade and Companies Register 989 314 067), represented by Benjamin Zerdoun	Legal representative of Layan SAS; signatory of the company's commitments and contracts.
Chief Executive Officer (CEO)	**NCC** SAS (Paris Trade and Companies Register 989 385 901), represented by Nicolas Chevalier Cohen	Guarantor of the proper application of this Policy; line manager of the Technical Lead and the DPO; approves structuring decisions (sub-processor changes, DPIAs, breach notifications); signs the annual compliance report.
Data Protection Officer (DPO)	Aymen Ezzayer — `aymen@layan.eu`	Operational lead for GDPR compliance: record of processing activities (Art. 30), DPIA (Art. 35), staff training, handling of data subject requests, point of contact for the CNIL and data subjects. Reports to the CEO, with functional independence in the performance of his duties (Art. 38).
Technical Lead	Andy Le Roy	Operational implementation of security measures (see PSSI § 2); escalation of incidents to the DPO and Management; technical awareness of the teams. Reports to the CEO.
All employees and staff	All	Compliance with this Policy and the PSSI; reporting of incidents; participation in annual awareness sessions.

The DPO is designated pursuant to Article 37 GDPR. Although Aymen Ezzayer also holds the title of **Chief Information Officer (CIO)**, he has no operational responsibility for the determination of processing means (which fall under the Technical Lead, under the authority of the CEO). His DPO role is exercised independently, in compliance with Article 38 (3) GDPR.

For routine inquiries from data subjects and clients, the preferred contact channel is `support@layan.eu`. For matters requiring direct interaction with the DPO, the address is `aymen@layan.eu`.

6. Principles applied (Article 5 GDPR)

Layan applies the following principles to all of its processing activities:

Principle	Application at Layan
Lawfulness, fairness, transparency	Each processing relies on an identified legal basis (see § 7). Data subjects are informed prior to any collection (accessible privacy policy, notices on forms).

Principle	Application at Layan
Purpose limitation	Data is collected for specified, explicit and legitimate purposes, and is not reused in an incompatible manner.
Minimisation	Only Data strictly necessary for the purposes is collected. Forms are regularly reviewed to remove superfluous fields.
Accuracy	Data subjects can rectify their Data at any time via the platform or by request to the DPO.
Storage limitation	Retention periods are defined per purpose (see § 10). Upon expiry, Data is deleted or anonymised.
Integrity and confidentiality	Implementation of the technical and organisational measures described in the PSSI (P1 § 6, § 7 and § 8).
Accountability	Maintenance of a record of processing activities (Art. 30), DPIAs where required (Art. 35), staff training, internal and external audits.

7. Legal bases (Article 6 GDPR)

Depending on the nature of the processing, Layan relies on one of the following legal bases:

Processing	Legal basis	Justification
Provision of the platform to clients	Performance of contract	Article 6 (1) (b) — performance of the General Terms of Use.
Processing of candidate Data on behalf of clients (Sub-processing)	Sub-processing	Article 28 — Layan acts as Processor; the legal basis is that invoked by the client Controller. Details are set out in the Data Processing Agreement (DPA) signed with each client.
Administrative management of Layan staff	Performance of employment contract / Legal obligations	Article 6 (1) (b) and (c) — contracts, payroll, social declarations.
B2B commercial prospecting	Legitimate interest	Article 6 (1) (f) — outreach to legal entities on their professional capacity, with right to object guaranteed.
Newsletter and marketing communications to B2C contacts or candidates	Consent	Article 6 (1) (a) — explicit opt-in, withdrawal possible at any time.
Cookies on the corporate website and the platform	Consent (non-essential cookies) / Legitimate interest (strictly necessary cookies)	Articles 6 (1) (a) and (f), and Article 82 of the *Informatique et Libertés* Act.

The record of processing activities (Art. 30, see § 14) specifies the legal basis retained for each processing.

8. Categories of Data and data subjects

Layan processes the following categories of Data:

8.1 Data processed as Processor (on behalf of clients)

- **Data subjects**: candidates for job offers, internal users of clients (recruiters, managers, administrators), visitors to career sites edited via the platform, and referees nominated by a candidate where the client uses reference checking.
- **Categories of Data**: identification (title, gender — a required field on the public application form —, surname, first name), contact (email, phone, address), professional background (CV, education, experience, skills, salary expectations), application (cover letter, answers, status, recruiter comments, optional predictive-assessment results), connection (user identifier, IP, timestamps, activity log), authentication (hashed passwords, SSO tokens), communications (emails and SMS exchanged via the platform).
- **Special categories (Art. 9)**: none required; the platform discourages their entry. If a client collects such Data under its own responsibility, it informs Layan beforehand and ensures the existence of an appropriate legal basis.
- **Data relating to criminal convictions (Art. 10)**: none.

8.2 Data processed as Controller (for Layan's own purposes)

- **Layan staff**: Data necessary for the performance of the employment contract and social obligations;
- **Prospects and clients (B2B)**: professional contact Data of representatives (name, role, professional email, history of interactions);
- **Visitors to the `layan.eu` website**: connection Data, visit statistics, trackers after consent where applicable.

9. Data subject rights (Articles 12 to 23 GDPR)

Every data subject has the following rights:

- **Information** (Art. 13-14): notices at the time of collection;
- **Access** (Art. 15): obtain confirmation that their Data is processed and a copy thereof;
- **Rectification** (Art. 16): correct inaccurate Data;
- **Erasure / right to be forgotten** (Art. 17): delete their Data under the conditions set out in the GDPR;
- **Restriction** (Art. 18);
- **Portability** (Art. 20): retrieve their Data in a structured format;
- **Objection** (Art. 21), in particular to prospecting;

- **Automated individual decision-making** (Art. 22): Layan does not perform automatic scoring producing legal effects; the platform's recommendations assist the recruiter without replacing them;
- **Lodge a complaint with the CNIL** (Art. 77): via www.cnil.fr.

Procedure for exercising rights

Step	Deadline	Owner
Receipt of the request	—	Client channel: `support@layan.eu`; DPO channel: `aymen@layan.eu`
Acknowledgement of receipt	Within 5 working days	DPO
Verification of the requester's identity	Within 5 working days	DPO
If the request concerns Data processed as Processor: forwarding to the client Controller	Within 5 working days from verification	DPO
If the request concerns Data processed as Controller: response	Within 1 month (extendable to 3 months in case of complexity, with information to the data subject) — Art. 12 (3) GDPR	DPO
Tracking and logging of the request	—	DPO (rights requests register)

10. Retention period

Retention periods are defined per purpose, in compliance with the recommendations of the CNIL applicable to the recruitment sector:

Category of Data	Retention period
Candidate Data (as Processor for clients)	Defined by each client Controller and specified in their DPA. Configurable in years (1 year or 2 years); **default duration: 2 years** from the application date, reset by renewed consent (CNIL recommendation).
Accounts and activity of clients' internal users	For the duration of the client contract, deleted or anonymised within 30 days of contract termination.
Career-site visit-tracking data (IP, city, postcode)	48 hours, then irreversible daily anonymisation.
Technical logs (application logs, access logs)	12 months (CNIL recommendation for connection logs). Certain internal application logs are not yet purged automatically; the gap is recorded in the record of processing activities.

Category of Data	Retention period
Layan staff Data	According to legal obligations: 5 years after end of employment for payslips (French Labour Code), 10 years for accounting (French Commercial Code).
B2B commercial prospecting	3 years from last contact, unless prior objection.
Cookies	Maximum duration 13 months (CNIL recommendation).

Upon expiry of these durations, Data is irreversibly deleted or anonymised. Backups are encrypted and purged within the rotation cycle described in PSSI § 4.

Erasure on request. Where a client exercises, on behalf of a data subject, an erasure request from the platform's GDPR interface, the application is immediately marked as deleted and withdrawn from offers and talent pools; physical deletion of the records and associated files is carried out by a scheduled task three (3) months after that marking.

11. Sub-processors

Layan engages sub-processors to carry out part of its processing activities, in particular hosting, email delivery, CV analysis, application monitoring, SSO authentication and job offer distribution.

- The **up-to-date list** of named and categorised sub-processors is set out in **Annex 3 of the DPA** signed with each client.
- Each sub-processor is bound by a written contract providing for obligations equivalent to those imposed on Layan regarding the protection of Data.
- Any change to this list is notified to clients having signed a DPA, with at least 30 days' prior notice and a right of reasoned objection (see DPA Art. 6.3).

The platform is hosted by **Scaleway**, in the **France — `fr-par` (Paris)** region. A previous hosting arrangement with Amazon Web Services remains **read-only**, with no new writes, in the European regions France (Paris) and Ireland, until its final deletion scheduled no later than **31 October 2026**.

12. Transfers of Data outside the EEA

Layan processes and stores Data within the European Union (France region — `fr-par`, Paris), subject to the read-only historical residue mentioned in § 11.

However, certain sub-processors may be established in third countries or may access Data therefrom. In such cases, Layan ensures that the transfer is governed by one of the mechanisms provided for in Articles 44 to 49 GDPR:

- An adequacy decision of the European Commission (e.g. the United Kingdom);
- Standard Contractual Clauses (Decision (EU) 2021/914 of 4 June 2021);
- *EU-US Data Privacy Framework* for sub-processors established in the United States that are certified.

No transfer outside the EEA is carried out without one of these mechanisms.

13. Technical and organisational measures

The security measures implemented by Layan are described in detail in the **Information Systems Security Policy (P1 - PSI)**, to which this Policy expressly refers.

The following are notably covered:

Domain	PSSI reference
Access control, authentication, monitoring, secure development, error tracking	PSSI § 6
Risk and incident management	PSSI § 7
Physical security of premises and equipment	PSSI § 8
Human resources security (before, during, end of contract)	PSSI § 9
Hosting (Scaleway, France `fr-par` region)	PSSI § 10
Business Continuity Plan (BCP)	PSSI § 4
Penetration and vulnerability testing	PSSI § 5
Levels of control (operational, permanent, periodic)	PSSI § 3

For the *data protection* aspect specifically, Layan also applies:

- pseudonymisation and minimisation by default in forms and exports;
- deletion and anonymisation mechanisms upon expiry of retention periods;
- structured exports in machine-readable format for the right to portability;
- contractual confidentiality undertakings with each sub-processor handling Data.

14. Record of processing activities (Article 30 GDPR)

Layan maintains a **record of processing activities** maintained by the DPO. This record includes:

- the name of each processing and its purpose;
- the categories of data subjects and Data;
- the recipients (internal and sub-processors);
- any transfers outside the EEA and their framework;
- the retention periods;
- a general description of the technical and organisational measures;
- the capacity in which Layan acts (Controller / Processor).

The record is reviewed at least once a year and made available to the CNIL upon request.

15. Data Protection Impact Assessments (DPIA — Article 35 GDPR)

A DPIA is carried out by the DPO, in consultation with the Technical Lead and Management, when a processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular in the event of:

- the implementation of a new large-scale processing of candidate or staff Data;
- the introduction of a profiling or automated decision-making feature;
- the use of special categories of Data (Art. 9) on a large scale.

DPIAs are archived and made available to the CNIL.

16. Personal Data Breach management (Articles 33-34 GDPR)

In the event of a Personal Data Breach, Layan applies the following procedure:

1. **Detection** by any employee or monitoring tool (see PSSI § 6 and § 7);
2. **Immediate escalation** to the Technical Lead and the DPO;
3. **Assessment** of the nature, volume and risk to data subjects — DPO + Technical Lead + CEO cell;
4. **Containment** (technical) and evidence collection (see PSSI § 7);
5. **Notification to the client** (where Layan acts as Processor), within 72 hours, using the template in **Annex 4 of the DPA**;
6. **Notification to the CNIL** (where Layan acts as Controller and a risk to data subjects exists), within 72 hours, by the DPO via notifications.cnil.fr;
7. **Information of data subjects** (Art. 34) if the risk is high;
8. **Post-mortem** within 30 days following closure, including root cause analysis, corrective measures and procedure updates;
9. **Maintenance of a breach register** by the DPO.

17. Awareness and training

- **Annual awareness session** for all staff, organised jointly by the Technical Lead (security aspect — see PSSI § 7 and § 9) and the DPO (data protection aspect).
- **Onboarding training**: every new staff member receives, within 30 days of arrival, an initial training covering the PSSI and the PPD.
- **Confidentiality undertaking** signed by every employee, contractor or third party with access to Data.

- **Ad hoc communications** in the event of regulatory developments or significant incidents.

18. Control, audit and continuous improvement

The control of this Policy relies on the **three levels of control described in PSSI § 3**:

- **Operational**: continuous, by all staff, on day-to-day compliance with confidentiality;
- **Permanent**: annual, by Management and the DPO, conducting tests, training, compliance with regulatory developments;
- **Periodic**: every 2 to 3 years, independent external audit.

The DPO produces an **annual compliance report** presented to Management. This report includes:

- the state of the record of processing activities (Art. 30);
- the list of DPIAs carried out or in progress;
- rights requests received and their handling;
- any breaches and their consequences;
- the list of sub-processor changes and associated notifications;
- awareness actions carried out;
- improvement recommendations.

19. Approval, communication and update

- This Policy is **approved** by Management (CEO and DPO).
- It is **communicated** to all staff (intranet / shared space) and **made available** to clients and prospects upon request, as well as to any supervisory authority.
- It is **reviewed at least once a year** by the DPO. Any major regulatory development (e.g. new CNIL framework applicable to the recruitment sector) triggers an interim review.
- Version history is kept as an annex to the master document.

For any question relating to this Policy, please contact:

- the **Data Protection Officer**: Aymen Ezzayer — `aymen@layan.eu`
- the **client / data subject channel**: `support@layan.eu`