Security Assurance Plan

> **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 this document

This **Security Assurance Plan** (hereinafter the "**SAP**" or "**PAS**" — *Plan d'Assurance Sécurité*) describes the technical, organisational and contractual measures implemented by **LAYAN SAS** (hereinafter "**Layan**") to ensure the security, confidentiality, integrity and availability of data processed in connection with the operation of its recruitment management software platform (ATS — *Applicant Tracking System*, hereinafter the "**Platform**").

Its purpose is:

- to address the requirements of the IT departments (CIO / DSI) of Layan's clients and prospects regarding transparency on security measures;
- to constitute a **unilateral, public-ready** document usable during tender, audit, vendor due diligence and annual review processes;
- to complement the **Data Processing Agreement (DPA)** signed between Layan and each client by detailing the technical architecture, service commitments and operational processes underlying the Technical and Organisational Measures (TOMs) set out in Annex 2 of the DPA.

The SAP **does not replace**:

- the **Information Systems Security Policy** (internal reference **P1 - PSI**, hereinafter the "**ISSP**" or "**PSSI**"), an internal governance document;
- the **Personal Data Protection Policy** (internal reference **P2 - PPD**), Layan's GDPR governance document;
- the **DPA**, the bilateral agreement signed by each client.

2. Document framework

Layan's security and data protection documentation rests on four complementary documents:

Reference	Document	Nature	Audience
P1 - PSI	Information Systems Security Policy (ISSP / PSSI)	Internal policy, security governance	Layan staff; shared with clients on request
P2 - PPD	Personal Data Protection Policy	Unilateral GDPR policy	Clients, prospects, data subjects, authorities

Reference	Document	Nature	Audience
P3 - PAS	Security Assurance Plan (this document)	Operational description of measures and commitments	Clients, prospects, CIO / DSI
DPA	Data Processing Agreement (GDPR Article 28)	Bilateral contract	Signed with each Client / Controller

In the event of any contradiction between the SAP and the DPA signed with a client, **the DPA prevails**. Any update to one of these four documents triggers a consistency review of the others.

3. Layan corporate profile

Item	Information
Legal name	LAYAN SAS
Legal form	French *société par actions simplifiée*
Registered office	198 avenue de France, 75013 Paris (France)
Company registration	Nanterre Trade and Companies Register no. 891 123 432
Activity	Publishing and operation of an ATS software platform
Corporate website	layan.eu
Year of incorporation	2020
Headcount	20 to 49 employees band; up-to-date Kbis statement available on request

4. Governance and responsibilities

4.1 Internal organisation

Role	Responsibilities	Contact
President — **BZM** SAS (Nanterre Trade and Companies Register 989 314 067), represented by Benjamin Zerdoun	Legal representative of Layan SAS; signs corporate engagements and contracts	Via `support@layan.eu`
CEO (*Directeur Général*) — **NCC** SAS (Paris Trade and Companies Register 989 385 901), represented by Nicolas Chevalier Cohen	Accountable for security and compliance; oversees the reporting line of the Technical Lead and the DPO; approves structural decisions (sub-processor changes, incident notifications, DPIAs)	Via `support@layan.eu`
Data Protection Officer (DPO) — Aymen Ezzayer	Operational lead for GDPR compliance; point of contact for the CNIL and data subjects; functional independence (GDPR Article 38)	`aymen@layan.eu`

Role	Responsibilities	Contact
Technical Lead — Andy Le Roy	Operational implementation of security measures; oversight of technical incidents; access reviews	Via `support@layan.eu`
Client / support channel	Single entry point for all operational requests, support, and exercise of rights	`support@layan.eu`

4.2 Escalation chain in case of incident

1. **Detection** — Layan staff, monitoring tools, client report.
2. **Level 1** — Technical team / Technical Lead.
3. **Level 2** — CEO and DPO (GDPR notifications, client communications).
4. **Level 3** — President (legal commitments, regulatory complaints), represented by BZM.

5. Service scope

5.1 Service covered

This SAP covers the operation of the **Layan ATS Platform**, accessible via subdomains `app.*.layan.eu` (recruiter back-office), `jobs.*.layan.eu` (public career site), `api.*.layan.eu` (REST API) and `admin.layan.eu` (Layan back-office).

Main features covered:

- Publishing and distributing job offers (including automated multiposting to 50+ job boards);
- Collecting, organising and assessing applications;
- Communication with candidates via email and SMS;
- Talent pool and recruitment campaign management;
- Editing and publishing a careers site on a custom subdomain;
- Calendar synchronisation for interview scheduling;
- AI-assisted content generation and candidate / offer matching (optional features);
- REST API and webhooks for integration with the client's HR and HRIS tools;
- Data export and retrieval.

5.2 Out of scope

The following are expressly excluded from this SAP:

- the client's own information systems (workstations, networks, corporate directories);
- the client's end-user devices;
- third-party integrations not published by Layan, unless expressly listed in Annex 3 of the DPA;

- bespoke developments which are subject to a separate specification and contractual addendum.

6. Service-level commitments (SLA)

6.1 Availability

Layan commits to an **annual availability target of 99.9%** on the production scope of the Platform, calculated over the calendar year and excluding scheduled maintenance windows.

Scheduled maintenance is announced by written notification (via the Platform and / or by email to the client administrator) at least **seventy-two (72) hours in advance**, and preferably on low-traffic time slots.

Emergency maintenance required by a critical security patch may be triggered without prior notice; the client is informed as soon as practicable.

6.2 Support and response commitments

User support is provided via **Intercom** (in-app chat and email), with ticket tracking, history and notifications, in addition to the `support@layan.eu` channel.

Support hours:

- **Monday to Friday**
- **9:00 — 12:30** and **14:00 — 17:30** (Paris time, CET / CEST)
- Excluding French public holidays

Response commitments by severity (in business hours within the support window above):

Severity	Definition	Response	Target resolution
Critical	Service entirely unavailable or unreachable for all users	≤ 1 business hour	Best effort 24/7 until restoration
Major	Key function degraded affecting normal usage	≤ 4 business hours	≤ 2 business days
Minor	Anomaly without significant workaround, limited impact	≤ 1 business day	Scheduled in a release
Enhancement request / question	Functional question or suggestion	≤ 2 business days	Reviewed case-by-case

6.3 Incident communication

Any incident affecting Platform availability is communicated through:

- an **initial communication** in the originating ticket or by proactive notification to impacted client administrators;
- a **status update** at least every two (2) hours for incidents of critical severity;
- a **Reason For Outage (RFO) report** delivered within **ten (10) business days** following the closure of a critical incident, including timeline, root cause, immediate corrective measures and prevention plan.

7. Hosting and infrastructure

7.1 Location

The Platform is hosted with **Scaleway SAS** in the **France** region — code `fr-par` (Paris).

All production data (databases, object storage, application logs) remains within the European Union. Backups do not leave the EEA.

Edge delivery, DNS resolution, the web application firewall and DDoS protection are provided by **Cloudflare**; traffic transits its points of presence, including those located in the European Union.

Previous hosting. Until 1 August 2026 the Platform was hosted with **Amazon Web Services EMEA SARL** (regions `eu-west-3` Paris and, for one historical bucket, `eu-west-1` Ireland). Those buckets are now **read-only**, with no new writes, and their final deletion is scheduled no later than **31 October 2026**.

7.2 Hosting provider certifications

The hosting provider publishes the certifications and attestations it holds at the level of its data centres and the services used, foremost among them **ISO/IEC 27001** (information security management).

The up-to-date list and the exact scope of those certifications are published by the hosting provider on its compliance portal, which prevails over any reproduction in this document. On the client's reasoned request, Layan shares the attestations it holds from its own sub-processors, within the disclosure conditions imposed by them.

7.3 High-availability architecture

The production architecture implements:

- a **managed container orchestrator** (Kubernetes) hosting the application components, with automatic restart and horizontal scaling of the exposed services;
- a **managed database** (MySQL 8) deployed as a **high-availability cluster**, with automatic failover and access restricted to the private network;
- **redundant object storage** for attachments and CVs, in a multi-availability-zone class;
- **content delivery** via an edge delivery network for public static assets.

7.4 Layan compliance posture

As of the date of this SAP, Layan is **not itself certified** to ISO/IEC 27001. Layan is engaged in an **alignment programme with the ISO/IEC 27001:2022 standard and its 2024 amendment**, already evidenced by:

- the drafting of an ISSP (P1) approved by management;
- the drafting of a PPD (P2) approved by management and the DPO;
- the maintenance of a record of processing activities (GDPR Article 30);
- the formalisation of TOMs in Annex 2 of the DPA;
- the implementation of the technical controls described in § 8 below.

This alignment programme does not commit Layan to certification within a specific timeframe; any change to this position will be communicated to clients.

8. Technical security

In line with Annex 2 of the DPA and the ISSP, Layan implements the following technical measures.

8.1 Authentication and access control

- **Individual authentication** is mandatory for all Platform access; no shared accounts.
- **Passwords** are stored hashed using an adaptive password-hashing algorithm resistant to brute-force attacks (Argon2id or bcrypt depending on the environment).
- **Multi-factor authentication (MFA)**: deployment **planned** for privileged accounts and client administrators. In the meantime, access to the infrastructure control plane is restricted by private network and strong authentication, and enterprise SSO allows the client to apply its own multi-factor policy.
- **Enterprise Single Sign-On (SSO)** via OAuth2 / OpenID Connect: native support for Google Workspace, Microsoft 365 / Azure AD / Entra ID, and a multi-IdP gateway (Cryptr) supporting SAML 2.0.
- **Strict tenant isolation** of data between clients by organisation identifier, enforced at every request by the application layer.
- **Time-bound sessions**; session cookies flagged `Secure`, `HttpOnly`, `SameSite`.
- **Annual review** of user accounts and entitlements.

8.2 Encryption

- **In transit**: all inbound and outbound Internet traffic is encrypted using TLS 1.2 minimum, with preference for TLS 1.3. Certificates are managed with automated rotation.

- **At rest**: object storage is encrypted at bucket level using **AES-256**, with keys managed by the hosting provider; databases and backups run on a managed service providing encryption of volumes at rest.
- **Secrets and technical credentials**: stored in the hosting provider's **secret manager** and projected into the runtime environments by an operator holding read-only access, never in plain text in source code or container images.
- **Periodic rotation** of sensitive secrets and technical API keys.

8.3 Network and infrastructure security

- **Segmented private network**; databases and internal systems are not directly reachable from the Internet.
- **Strict segmentation** between public exposure (the load balancer only) and private subnets (applications, databases).
- **Default-deny network policies** at container level, with an explicit allow-list of outbound traffic (database, cache, SMTP, IMAP, distribution partners).
- **Web Application Firewall (WAF) deployed in production** at the edge delivery network, for protection against common attacks (OWASP Top 10) and rate limiting.
- **DDoS protection** provided at the edge delivery network.
- **Origin filtering**: the production load balancer accepts traffic only from the edge delivery network's address ranges, so the origin cannot be reached directly.
- **Anti-bot protection** (*Turnstile*) on public application forms.
- **Administrative access** to the control plane is via private network with strong authentication; no direct SSH access from the Internet.

8.4 Application security

- **Secure development lifecycle**: mandatory code reviews, static analysis, software composition analysis (SCA) of dependencies, quality gates (PHPStan level 9+, ESLint).
- **Input validation** at system boundaries (forms, API); parameterised queries exclusively (no SQL string interpolation).
- **Protection** against the OWASP Top 10 (injection, XSS, CSRF, SSRF, deserialisation, etc.).
- **HTTP security headers**: `Strict-Transport-Security` is applied across the whole domain at the edge delivery network (two-year max-age, subdomains included, with preload). Deployment of the complementary headers (`Content-Security-Policy`, `X-Frame-Options`, `X-Content-Type-Options`, `Referrer-Policy`) is **in progress**.

8.5 Logging and monitoring

- **Logging** of access to data and sensitive actions (who accessed what, when), retained for the period required by legal and operational obligations (see PPD § 10).
- **Centralisation** of application and system logs.
- **Real-time application monitoring** with automated alerts on incidents (errors, abnormal latency, traffic spikes).
- **Access anomaly detection** (repeated failed logins, off-hours access, sensitive configuration changes).
- **Error tracking** via an application monitoring tool (Sentry).

8.6 Backups

- **Automated daily backups** of databases via the hosting provider's managed service, in a nightly window.
- **Retention**: a minimum of seven (7) days for managed-database backups, across all environments. Extending this retention in production, together with the retention of manual snapshots beyond the rotation window, is currently being rolled out.
- **Encryption** of backups at rest with the same guarantees as production databases.
- **Periodic restoration tests**, documented.
- **Object storage** redundant in a multi-availability-zone class for candidate files.

9. Organisational and HR security

9.1 Pre-employment

- Reference checks to the extent permitted by applicable law.
- Contractual confidentiality undertaking (clauses in employment and service contracts).
- Awareness briefing prior to granting access to sensitive data.

9.2 During employment

- **Mandatory annual awareness training** on information security and data protection for all staff.
- **Onboarding training** within thirty (30) days of arrival, covering the ISSP and the PPD.
- **Confidentiality undertaking** signed by every employee, contractor or intervener accessing data.
- **Ad hoc communications** on regulatory updates or significant incidents.
- **Least-privilege application**: entitlements are granted on a need-to-know basis and reviewed periodically.

9.3 End of employment

- **Formal off-boarding procedure**: immediate revocation of access, return of equipment, reminder of residual confidentiality obligations.
- **Inventory** of accounts and access to close (internal, sub-processors, partners).

10. Business continuity (BCP / DRP)

10.1 Architecture

- **Multi-AZ** deployment of critical production components (see § 7.3).
- **Automatic database failover** between availability zones in case of zone failure.
- **Geographic distribution** of backups within the European region for resilience.

10.2 Production targets

Indicator	Definition	Target
RPO (*Recovery Point Objective*)	Maximum tolerable data loss	≤ 24 hours
RTO (*Recovery Time Objective*)	Maximum time to restore service after a major incident	≤ 4 hours

10.3 Tests

- Periodic restoration and failover tests, documented and traceable.
- Annual review of the BCP / DRP and update against architectural evolutions.

11. Security incident management

11.1 Detection

- **Automated tools**: application monitoring, error tracking, network and access anomaly detection, vulnerability scanners.
- **Human reporting**: staff, clients, security researchers, third parties.

11.2 Response

Procedure aligned with the ISSP (§ 7) and the DPA (Article 8):

1. **Detection** and initial qualification by the technical team;
2. **Immediate escalation** to the Technical Lead and the DPO;

3. **Crisis team** activated based on severity (Technical Lead + DPO + CEO);
4. **Technical containment** and collection of forensic evidence (logs, network traces);
5. **Client notification** within **seventy-two (72) hours** at the latest from awareness, in the event of a breach of data processed on the client's behalf (Annex 4 of the DPA — notification template);
6. **CNIL notification** by the DPO if Layan acts as Controller and a risk to data subjects exists, within seventy-two (72) hours;
7. **Information of data subjects** if the risk is high (GDPR Article 34);
8. **Post-mortem** within thirty (30) days of closure, including root cause analysis, corrective measures and procedure updates;
9. **Maintenance of a breach register** by the DPO.

11.3 Insurance coverage

Layan holds a **cyber insurance policy** covering incidents affecting its information system; the policy certificate is available on the client's reasoned request.

12. Vulnerability management and security testing

12.1 Watch and patching

- **Active monitoring** of CVE vulnerabilities affecting software components and infrastructure.
- **Automated dependency tracking** (software composition analysis) with alerts on vulnerability disclosures.
- **Application of critical security patches** without undue delay following qualification (target: ≤ 7 days for critical CVEs on externally exposed components, save for documented operational constraints).

12.2 Security testing

- **Static Application Security Testing (SAST)** integrated into the development pipelines.
- **Software Composition Analysis (SCA)** on open-source dependencies.
- **Periodic vulnerability scans** of the exposed infrastructure.
- **Penetration testing** performed at the client's request as part of its audit right (see § 14), or periodically by independent providers at Layan's initiative. The operational conditions (window, scope, intensity) are agreed in writing beforehand so as not to disrupt the service.

12.3 Environment isolation

- **Development, test and production environments** are strictly isolated (separate cloud projects, private networks and credentials).

- **Production data is not used in development environments** without prior anonymisation or pseudonymisation.
- **Separation of duties** between environment administrators.

13. Sub-processing

13.1 Principles

Layan relies on sub-processors (as defined in GDPR Article 28 §2) to perform parts of its processing activities, including hosting, email and SMS routing, CV parsing, application monitoring, SSO authentication and job offer distribution.

Each sub-processor is:

- **bound contractually** by an agreement imposing data protection obligations equivalent to those imposed on Layan;
- **selected** based on security and compliance criteria, with periodic review of the relationship;
- **listed** in **Annex 3 of the DPA**, updated under the terms of Article 6.3 of the DPA (written notification with at least thirty (30) days' notice and the client's right to object on reasoned grounds).

13.2 Current list

The up-to-date list of nominally designated sub-processors, with their role, country of establishment and (where applicable) the mechanism framing transfers outside the EEA, is set out in **Annex 3 of the DPA** signed with each client. As of the date of this SAP, it notably includes:

- **Scaleway SAS** — hosting, managed database, object storage, content delivery (France, `fr-par`);
- **Cloudflare, Inc.** — DNS, edge delivery, web application firewall and DDoS protection, anti-bot protection (United States, DPF + SCCs);
- **Amazon Web Services EMEA SARL** — previous hosting, read-only until 31 October 2026 (EU: France and Ireland);
- **Brevo SAS** — email and SMS routing (France);
- **OpenAI Ireland Limited** — CV parsing and content generation, active by default (Ireland / United States, DPF + SCCs);
- **HRflow.ai (Riminder SAS)** — CV parsing as a fallback (France);
- **Cryptr SAS** — optional SSO (France);
- **Google Ireland Limited** — Google SSO, reCAPTCHA, address autocomplete and map tiles, tag manager (Ireland / United States, DPF);
- **Microsoft Ireland Operations Limited** — Microsoft / Azure AD / Entra ID SSO (Ireland / United States, DPF);
- **Cronofy Limited** — optional calendar synchronisation (United Kingdom, adequacy decision);

- **Sentry (Functional Software, Inc.)** — application monitoring (United States, SCCs + DPF);
- **PostHog, Inc.** — recruiter back-office analytics, *PostHog Cloud EU* (European Union, Frankfurt);
- **Content Square SAS** — audience measurement and session replay of the recruiter back-office (France);
- **ip-api.com** — IP-address geolocation of career-site visitors (Australia, SCCs);
- **Jawg SAS** — career-site map tiles (France);
- **OpenStreetMap Foundation** — career-site map tiles (United Kingdom, adequacy decision);
- **AssessFirst SAS** — optional predictive assessment (France);
- **HubSpot Ireland Limited** — optional CRM synchronisation (Ireland / United States, DPF);
- **Lucca SAS**, **Eurécia SAS**, **Skello SAS** — optional HRIS synchronisations (France);
- **Intercom R&D Unlimited Company** — user support and ticket handling (Ireland / United States, DPF);
- **Slack Technologies Limited** — internal operational notifications (Ireland / United States, DPF).

13.3 Transfers outside the EEA

Data is processed and stored within the European Union. Where a sub-processor is established outside the EEA or accesses data from a third country, the transfer is framed by one of the mechanisms provided in GDPR Articles 44 to 49 (adequacy decision, Standard Contractual Clauses 2021/914, EU-US Data Privacy Framework). Details are set out in Annex 3 of the DPA.

14. Audit rights

In accordance with **Article 5.8 of the DPA**, the client may carry out an audit, by itself or through an independent third party bound by confidentiality, under the following conditions:

- written reasonable notice, generally thirty (30) days;
- audit performed during business hours, without disrupting Layan's activity;
- audit scope limited to the data and systems of the requesting client (no information on other Layan clients);
- audit cost borne by the requesting client, unless the audit reveals a material breach by Layan, in which case Layan bears the cost;
- frequency limited to one (1) audit per calendar year, save in case of a proven security incident or a reasoned request from a supervisory authority.

Following the audit, Layan implements, at its own expense and within a reasonable timeframe, any corrective measure necessary to remedy the non-conformities identified.

In addition, Layan makes available to the client, on reasoned request:

- documentation regarding the TOMs (Annex 2 of the DPA and this SAP);

- the up-to-date sub-processor list (Annex 3 of the DPA);
- audit reports and compliance attestations of its own sub-processors where available, within the disclosure conditions imposed by them;
- the current cyber insurance certificate.

15. Reversibility and data restitution

15.1 During the contract

Through the Platform administration interface, the client has access at any time to the following export features:

- **Candidate export** in **CSV** format;
- **Job offer export** with associated data;
- **Document and CV download** (per candidate).

For specific needs (bulk exports, alternative format), the client may contact support at `support@layan.eu`.

15.2 At the end of the contract

In accordance with **Article 5.7 of the DPA**, upon expiry or termination of the main contract, Layan shall, at the client's written choice expressed within **thirty (30) days** of the end of the contract:

- **return** the data in a structured, commonly used and machine-readable format (downloadable export from the Platform: CSV for structured data, archive of documents and CVs for object storage, SQL *dump* of the database for a full export of the client organisation); and / or
- **definitively delete** the data and all existing copies.

In the absence of instructions from the client within the thirty (30)-day period, Layan proceeds with **definitive deletion** thirty (30) days after that deadline, unless a legal retention obligation applies.

15.3 Cost

Data restitution in the standard formats listed above is **free of charge**. Specific requests requiring custom development may be the subject of a quote.

15.4 Residual backups

Backups containing the client's data are deleted as part of the natural backup rotation cycle, within a maximum timeframe corresponding to the backup retention duration (see § 8.6). During this residual period, backups remain isolated, encrypted and inaccessible for any use other than restoration in case of

incident.

15.5 Attestation

A **deletion certificate** may be issued to the client on written request to `support@layan.eu`.

16. Regulatory and standards compliance

16.1 Regulatory framework

- **Regulation (EU) 2016/679 (GDPR)**;
- French **Act No. 78-17 of 6 January 1978 "Informatique et Libertés"**, as amended;
- **CNIL recommendations** applicable to the recruitment sector;
- **ePrivacy Directive** (2002/58/EC, as amended) and Article 82 of the French Data Protection Act (cookies and trackers).

16.2 Alignment frameworks

The technical and organisational measures described in this SAP are aligned with:

- the principles of **ISO/IEC 27001:2022** and its 2024 amendment (Annex A);
- the controls of **ISO/IEC 27002:2022** for their detailed implementation;
- the recommendations of the French **ANSSI** (in particular guides on IT hygiene and cloud best practice);
- **OWASP** best practices for application security;
- CNIL recommendations specific to recruitment (retention periods, candidate rights).

16.3 Certifications

As of the date of this document:

- **Layan** does not hold an ISO 27001 certification in its own name; an alignment programme is in progress (see § 7.4).
- The **hosting provider** is certified ISO/IEC 27001; the exact scope and up-to-date list of its certifications are published by it (see § 7.2).
- The certifications of the other sub-processors are those they themselves publish; on reasoned request Layan shares the attestations it holds.

Any change to these elements is communicated to clients as part of the annual review of this SAP.

17. Approval, communication and maintenance

- This SAP is **approved** by Layan's management (CEO and DPO).
- It is **communicated** to clients and prospects on request, and made available to supervisory authorities.
- It is **reviewed at least once a year** by the Technical Lead and the DPO, and systematically in case of:
  - substantial architectural change;
  - major regulatory evolution;
  - significant security incident leading to lasting corrective measures;
  - update of the ISSP (P1) or the PPD (P2).
- The version history is kept internally and available on request.

For any question regarding this Security Assurance Plan, the preferred contacts are:

- **Client / support channel**: `support@layan.eu`
- **Data Protection Officer (DPO)**: Aymen Ezzayer — `aymen@layan.eu`