

Vanguard Frontline Security Solutions Limited - Privacy Notice

Version: 2.0

Effective date: 8 September 2026

This privacy notice explains how Vanguard Frontline Security Solutions Limited (“Vanguard”, “we”, “us”) collects, uses, shares and protects personal information. It covers our public website, client and venue relationships, recruitment and workforce administration, and the Vanguard Ops operational portal.

1. Who we are and how to contact us

Vanguard Frontline Security Solutions Limited is the data controller for the personal information described in this notice unless another organisation is clearly identified as controller for a particular activity.

Company number: 16748303

Registered office: 16 Gascoigns Way, Bristol, BS34 5BY

Privacy and legal contact: legal@vanguard-security.co.uk

If you have a question about this notice, want to exercise a data protection right, or have a concern about how your information has been used, contact us at the email address above.

2. Who this notice applies to

This notice may apply to:

- current, former and prospective clients, venue representatives and business contacts;
- people who contact us through our website or by email;
- job applicants, employees, workers, contractors and SIA-licensed security personnel;
- Vanguard Ops users, including Staff, Head Door personnel, Operations users and Venue/Customer users;
- people involved in, affected by or witnessing security incidents at venues where Vanguard provides services; and
- other individuals whose information is reasonably contained in our operational, contractual, compliance or incident records.

3. Information we collect and use

The information we use depends on your relationship with Vanguard and the reason we need it.

Clients, venues and business contacts

We may use:

- names, job titles and business contact details;
- organisation, venue and address details;
- records of meetings, enquiries, quotations, decisions and communications;
- contract, service, transaction and payment information;
- staffing and additional-cover requests;
- venue operating information and approved venue SOPs; and
- technical or usage information about interaction with our website and services.

Recruitment, staff and workers

We may use:

- name, address, email address, telephone number and date of birth;
- National Insurance number and other payroll/employment information where required;
- employment history, references, right-to-work information and secondary-employment information;
- employee/workforce identifiers;
- SIA licence number, licence status and expiry date;
- operating region, role and account permissions;
- availability and unavailability;
- shift offers, assignments, acceptance/decline status and assignment role;
- venue SOPs made available to you and your acknowledgements;
- live attendance status and shift timesheets;
- approved payable and billable working times, timesheet queries and amendments;
- incident reports, amendments and evidence you submit; and
- operational communications, account-security information and audit history.

Vanguard Ops is not designed to continuously track workers' location. Our current attendance and timesheet model records operational presence and approved working time without routine continuous GPS monitoring.

Venue and customer portal users

We may use:

- name, business email address and telephone number;
- employer/customer organisation;
- account, role and venue/customer access permissions;
- staffing and additional-cover requests;
- venue SOP access;
- venue-facing incident summaries;

- live attendance information relevant to the user's venue(s);
- timesheet review, confirmation or query activity; and
- account-security and audit information.

Security incidents

Incident records may include:

- names or descriptions of people involved;
- date, time, venue and circumstances;
- witness information;
- refusals of entry, removals/ejections and alleged unlawful behaviour;
- police, ambulance or other emergency-service involvement and reference numbers;
- injuries or other health information where relevant;
- photographs, documents and other supporting evidence; and
- amendments, management reviews and venue-facing summaries.

Incident records can contain **special category information**, particularly health information, and **criminal offence information**, including information about alleged offences.

Website, communications and marketing

We may process:

- names and contact details;
- marketing and communication preferences;
- enquiry and communication history;
- basic technical logs and website/app usage information; and
- cookies or similar technologies where used and lawfully permitted.

We aim to keep marketing relevant, proportionate and infrequent. You can opt out of direct marketing at any time.

4. Where we get personal information from

We may obtain information:

- directly from you;
- from Vanguard directors, managers, supervisors and Head Door personnel;
- from venue/customer representatives;
- from witnesses or other people involved in an incident;
- from police, emergency services, regulators or public authorities where lawful;
- from publicly available sources, including the SIA public register where relevant;
- from existing Vanguard employment, compliance, contractual or operational records; and

- automatically from technical/security logs created when our systems are used.

5. Why we use personal information and our lawful bases

UK data protection law requires us to have a lawful basis for processing personal information. The basis depends on the purpose and circumstances.

Purpose	Typical lawful basis/bases
Respond to enquiries and provide security services	Contract; steps before entering a contract; legitimate interests
Manage client and venue relationships	Contract; legitimate interests
Business development and relevant updates	Consent where required; legitimate interests
Recruitment	Steps before entering a contract; legitimate interests; legal obligation where applicable
Manage workers, shifts, availability and assignments	Contract; legal obligation; legitimate interests
Record working time and support payroll/invoicing	Contract; legal obligation; legitimate interests
Maintain SIA and compliance records	Legal obligation where applicable; legitimate interests
Maintain SOPs, acknowledgements and operational instructions	Legitimate interests; legal obligation where applicable
Secure Vanguard Ops, control access and maintain audit trails	Legitimate interests; legal obligation where applicable
Record, investigate and manage security incidents, complaints and claims	Legitimate interests; legal obligation; legal claims; vital interests in emergencies where applicable
Share information with police or public authorities	Legal obligation, legitimate interests or another applicable lawful basis depending on the circumstances

Where we rely on **legitimate interests**, our interests can include operating a safe and effective security service, protecting people and property, managing our workforce and contracts, keeping accurate operational records, preventing misuse, maintaining business relationships, and establishing or defending legal claims. We consider whether processing is necessary and proportionate and whether an individual's rights override those interests.

We do not generally rely on consent for core employment, security, incident-management or contractual processing where another lawful basis is more appropriate.

6. Special category and criminal offence information

Where we process special category information, we identify an additional condition under Article 9 UK GDPR. Depending on the circumstances, this may include processing necessary for employment obligations, vital interests or the establishment, exercise or defence of legal claims.

Where we process criminal offence information, including information about alleged offences, we do so only where Article 10 UK GDPR and the Data Protection Act 2018 permit it. Relevant Schedule 1 conditions may include preventing or detecting unlawful acts and legal claims, depending on the circumstances.

Vanguard maintains an Appropriate Policy Document where required, setting out safeguards, retention and deletion arrangements for relevant special category and criminal offence processing.

7. Who we share information with

We share personal information only where reasonably necessary and lawful. Recipients may include:

- authorised Vanguard directors, managers, Operations personnel, workers and advisers;
- the relevant venue/customer, limited to information needed to provide or manage the service;
- payroll, accounting and professional advisers;
- insurers, solicitors and claims advisers;
- the Security Industry Authority and other regulators where relevant;
- police, emergency services, courts and public authorities where lawful and necessary; and
- technology suppliers that process information on our behalf.

Major technology providers used by Vanguard may include:

- **Google Workspace** for company email, documents and collaboration;
- **Supabase** for Vanguard Ops database, authentication and private file-storage infrastructure;
- **Netlify** for website/portal hosting and server-side functions; and
- **Resend** for transactional and operational email delivery.

Venue/customer users do not receive unrestricted access to Vanguard's internal staff records, commercial information, incident evidence or private contact information merely because Vanguard provides services to their venue or organisation.

8. International transfers

Some suppliers or their support/sub-processors may process or access personal information outside the UK.

Where a transfer is a restricted transfer under UK data protection law, Vanguard will use an applicable UK adequacy regulation or appropriate safeguards, such as the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses, together with any required transfer-risk assessment.

You can ask legal@vanguard-security.co.uk for further information about safeguards used for a particular transfer.

9. How long we keep information

We retain information only for as long as reasonably required for its purpose, legal obligations, dispute resolution and legal claims. Normal retention is subject to review and can be extended where an investigation, safeguarding issue, complaint, legal claim, court order or regulatory requirement remains active.

Record type	Normal retention approach
Marketing/prospective-client contacts	Normally up to 2 years after the last meaningful interaction, unless an ongoing relationship or another lawful reason applies
Unsuccessful recruitment records	Normally up to 12 months after the recruitment process ends
Employee/worker and compliance/SIA records	During engagement and normally up to 6 years afterwards, subject to specific legal requirements
Availability records	Normally 12 months after the relevant period unless required for a dispute
Shift assignments, SOP acknowledgements and approved timesheets	Normally 6 years from the relevant record/shift, or longer where legally required or disputed
Incident reports and evidence	Normally 6 years from the incident; longer where an investigation, safeguarding issue, complaint or claim requires it
Client, venue and contractual records	Duration of the relationship and normally up to 6 years afterwards where required for contract, tax or claims purposes
Security and audit logs	Normally 24 months, unless linked to an investigation, incident, legal claim or other record requiring longer retention

Routine notification/delivery records	Normally up to 12 months unless required for an investigation or dispute
---------------------------------------	--

Archived records remain subject to these retention rules. Archiving removes records from normal operational use; it does not mean they are retained indefinitely.

10. Security

We use technical and organisational measures intended to protect personal information against unauthorised access, alteration, loss or disclosure. Depending on the system and information, measures include:

- individual user accounts and mandatory two-step verification for Vanguard Ops;
- least-privilege role, venue, customer and region-based access controls;
- database-enforced access restrictions;
- private evidence storage;
- immutable or append-only records where evidential integrity matters;
- audit logging of significant activity;
- encrypted network connections;
- controlled server-side privileged operations;
- backups, security testing and access reviews; and
- non-destructive archival of historical operational records.

No system can be guaranteed to be completely secure. Users must protect their credentials and report suspected compromise promptly.

11. Automated decision-making

Vanguard Ops does not currently make solely automated decisions about individuals that produce legal effects or similarly significant effects.

The system may assist authorised managers by filtering or highlighting information such as availability, overlapping assignments, SIA validity or overdue actions. Human users remain responsible for operational decisions and can review appropriate system suggestions.

12. Your data protection rights

Depending on the circumstances and lawful basis, you may have rights to:

- be informed about how we use your information;
- request access to your personal information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information in certain circumstances;

- ask us to restrict processing in certain circumstances;
- object to processing based on legitimate interests or to direct marketing;
- receive certain information in a portable format where applicable; and
- withdraw consent where consent is the lawful basis.

These rights are not absolute. For example, we may need to retain an incident report, audit record, payroll record or contractual record despite an erasure request where the law permits or requires continued retention.

To exercise a right, contact **legal@vanguard-security.co.uk**. We normally respond without undue delay and within one month, subject to the rules and exemptions in data protection law.

13. Complaints

Please contact us first at **legal@vanguard-security.co.uk** if you have concerns about how we use personal information so we can investigate and respond.

You also have the right to complain to the **Information Commissioner's Office (ICO)**:

Information Commissioner's Office
 Wycliffe House
 Water Lane
 Wilmslow
 Cheshire
 SK9 5AF
 Helpline: 0303 123 1113
 Website: ico.org.uk/make-a-complaint

14. Changes to this notice

We review this notice periodically and update it where our processing changes materially. Where appropriate, we will bring significant changes to the attention of affected users.