

Privacy Notice



Policy last reviewed: June 2026

Next review due: June 2027

Table of Amendments	
1st January 2025	General wording and grammar update
1st June 2026	reviewed and updated to improve clarity, transparency and compliance with UK data protection requirements. Amendments include updated data protection contact details, clearer explanations of the types of personal data processed.

1. Introduction

VIP Security (Essex) Ltd respects your privacy and is committed to protecting personal data.

This website privacy notice explains how we collect, use, store, share and protect personal data when you visit our website, contact us, make an enquiry, request information about our services, submit a career enquiry, communicate with us using the contact details shown on our website or engage with us as a customer, prospective customer, client, prospective client or supplier.

This website is not intended for children, and we do not knowingly collect personal data relating to children through this website.

This notice is intended to be clear and proportionate for website use. Where we collect personal data for other purposes, such as recruitment, employment, vetting, screening, SIA compliance, security services, CCTV, body-worn video, incident management or client-site records, we may provide separate or additional privacy information at the time the data is collected.

2. Who we are

VIP Security (Essex) Ltd is the data controller for personal data collected through this website and for personal data processed for our own business purposes.

Company registration number: 07940645

Registered office: Create Business Hub, Ground Floor, 5 Rayleigh Road, Hutton, Brentwood, Essex, England, CM13 1AB

Principal place of business: Security House, 4 Station Court, Wickford, Essex, SS11 7AT

Website: www.vipsecurityservices.co.uk

You can contact us by post at our principal place of business, through our website contact form, by telephone on 01268 526212 or by email at info@vipsec.at.

Data protection contact: VIP Security (Essex) Ltd, info@vipsec.at

3. Website providers and third-party links

Our website is managed and supported by Universal Web Design. We may also use third-party website, IT, hosting, form, analytics or security providers. These providers may process limited personal data where this is necessary to operate, secure, maintain or improve the website.

If our website providers change, this notice will be reviewed and updated where necessary.

Our website may include links to third-party websites, plug-ins or applications. We do not control third-party websites and are not responsible for their privacy notices. When you leave our website, you should read the privacy notice of the website you visit.

4. Personal data we collect through the website

Personal data means information relating to an identified or identifiable individual.

We may collect the following personal data through the website or through contact details published on the website:

- **Identity and contact data:** name, organisation or business name where relevant, job title, email address, telephone number, address and other contact details provided by you.
- **Enquiry and communication data:** messages, service requests, career enquiries, contact form submissions, email correspondence, telephone notes and related communications.

- **Recruitment or career enquiry data:** CVs, work history, role interests, availability and any information you choose to provide when making a career enquiry or applying through a website link.
- **Client, customer and business relationship data:** information about customers, clients, prospective customers or clients, suppliers, business contacts and service requirements.
- **Credit, identity and affordability data:** information used to assess customers, prospective customers, clients, suppliers, payment terms, creditworthiness, affordability, fraud risk, account management or debt recovery. Where this includes personal data, this may include details relating to individuals, sole traders, partners, directors, beneficial owners or relevant business contacts.
- **Technical and usage data:** IP address, device information, browser type, operating system, pages visited, referral source, time spent on the website and similar technical information.
- **Cookie and analytics data:** information collected through cookies or similar technologies where used.
- **Call data:** where you contact us by telephone, calls may be monitored or recorded for training, customer service, quality, dispute resolution or security purposes.
- **Marketing preference data:** your preferences about receiving marketing communications from us.

We do not intend to collect special category data or criminal offence data through the general website contact form. You should not provide this type of information unless it is necessary for your enquiry or you are asked to provide it through an appropriate process. If you voluntarily provide such information, we will only use it where lawful, necessary and proportionate.

5. How we collect personal data

We may collect personal data:

- directly from you when you complete a contact form, send an email, telephone us, request information, submit a career enquiry or otherwise communicate with us;
- automatically when you use our website, including through cookies and similar technologies where used;
- from third-party website, IT, analytics, hosting, security, form or communications providers who support our website and systems;
- from customers, prospective customers, clients, suppliers, business contacts, referees or other third parties where this is relevant to your enquiry or our services.
- from credit reference agencies, business information providers, fraud prevention providers or public sources where relevant to credit, identity, affordability, payment or fraud prevention checks.

6. How we use personal data and lawful basis

We will only use personal data where the law allows us to do so. The lawful bases we may rely on include:

- **Performance of a contract:** where processing is necessary to perform a contract with you or take steps at your request before entering into a contract.

- **Legal obligation:** where processing is necessary to comply with the law.
- **Legitimate interests:** where processing is necessary for our legitimate business interests, provided your rights and freedoms do not override those interests.
- **Consent:** where we rely on your consent, for example for certain marketing communications or non-essential cookies.

PURPOSE	PERSONAL DATA USED	LAWFUL BASIS
Responding to enquiries and contact form submissions	Identity and contact data; enquiry and communication data	Legitimate interests; performance of a contract where the enquiry relates to services or a contract
Providing information about our services and managing customer or supplier relationships	Identity and contact data; business relationship data; communication data	Performance of a contract; legitimate interests; legal obligation where applicable
Managing career enquiries submitted through the website	Identity and contact data; recruitment or career enquiry data; communication data	Taking steps before entering into a contract; legitimate interests; legal obligation where applicable
Operating, maintaining and securing the website and IT systems	Technical and usage data; security logs; enquiry data where relevant	Legitimate interests; legal obligation where applicable
Using analytics to understand and improve website performance	Technical, usage, cookie and analytics data	Consent where required for non-essential cookies; legitimate interests for necessary, aggregated or security-related analysis where applicable
Sending marketing communications where lawful	Identity and contact data; marketing preference data; communication data	Consent and/or legitimate interests, depending on the circumstances
Monitoring or recording calls where telephone contact is used	Call data; identity and contact data; communication data	Legitimate interests; legal obligation where applicable
Managing complaints, disputes, legal claims or regulatory matters	Relevant contact, enquiry, communication, business relationship, call and technical data	Legitimate interests; legal obligation; establishment, exercise or defence of legal claims
Carrying out business credit, identity, affordability, payment terms, fraud prevention or debt recovery checks where relevant	Identity and contact data; business relationship data; business credit, identity and affordability data; financial and transaction data where relevant	Legitimate interests; performance of a contract; legal obligation where applicable

7. Credit, identity and affordability checks

Where you contact us as, or on behalf of, a customer, prospective customer, client, prospective client, supplier or organisation, we may carry out credit, identity, affordability, payment or fraud prevention checks where relevant. These checks may be used to assess creditworthiness, affordability, identity, fraud risk, payment terms, account management, debt recovery or whether to enter into or continue a customer, client or supplier relationship.

These checks may involve information from credit reference agencies, business information providers or fraud prevention providers, including Creditsafe and, where applicable, their data partners. They are used only where relevant, lawful and proportionate to the relationship or proposed relationship.

These checks are not carried out simply because someone browses our website. They are separate from recruitment, employment, vetting or SIA screening checks, which are covered through separate privacy information where relevant.

8. Applicants and recruitment

Recruitment, vetting and screening information is not processed simply because you browse our website. Further information about how we use applicant, worker and employee personal data will be provided through our applicant, recruitment, vetting or onboarding privacy information.

Where relevant to the role or contract, this may also include vetting or screening information required for SIA, BS 7858, client, insurance or accreditation purposes.

This may include information provided in your application, CV, interview records, right to work information, SIA licence information, employment history, references, address history, training information, criminal record information where lawful and relevant, and credit reference or public record information where required for the role or contract.

Where you apply for a role with us, submit a career enquiry or provide recruitment information through our website or a linked recruitment form, we will process personal data as part of our recruitment, vetting, screening and onboarding process.

9. Marketing

We may send information about our services where we are allowed to do so by law. We will not send marketing communications where consent is required unless you have given that consent.

You can ask us to stop sending marketing communications at any time by contacting info@vipsec.at or by using any unsubscribe option provided in the communication.

Where marketing is based on consent, you may withdraw your consent at any time.

10. Cookies and analytics

Our website uses cookies and similar technologies to make the website work, improve security, understand how visitors use the website and improve the user experience.

Some cookies are necessary for the website to function properly. These cookies may be used without consent where they are strictly necessary.

Where the website uses analytics, marketing, advertising or other non-essential cookies, these will only be used where required consent has been obtained through the website cookie banner or cookie settings tool.

The website is managed and supported by Universal Web Design. Universal Web Design may support the operation, maintenance and technical management of the website on our behalf.

You can manage your cookie preferences through the website cookie banner or your browser settings. Please note that disabling some cookies may affect how the website works.

We may update this notice when our website provider confirms further details about the specific cookies used, including cookie names, providers, purposes, categories and retention periods.

11. Call monitoring and recording

If you telephone us using a number published on our website, calls may be monitored or recorded for training, customer service, quality, dispute resolution or security purposes.

Call recordings, where used, are kept only for as long as necessary for the purpose for which they were recorded, unless a longer period is needed for a complaint, investigation, legal claim, insurance matter, regulatory matter, safeguarding concern or security incident.

12. Who we share personal data with

We may share personal data with:

- website, hosting, IT, email, form, analytics, security and communications providers;
- customers, prospective customers, clients, suppliers, business partners or site contacts where this is necessary to respond to an enquiry or provide services;
- professional advisers, including lawyers, accountants, auditors, consultants and insurers;
- payment providers, banks or debt recovery organisations where relevant;
- credit reference agencies, business information providers or fraud prevention providers where relevant to credit, affordability, identity, payment terms or fraud prevention checks;
- regulators, public authorities, law enforcement agencies, courts or tribunals where required or permitted by law;
- prospective buyers, sellers or merged entities where we sell, transfer or merge part of our business or assets.

We require third parties to respect the security of personal data and to process it in accordance with the law. Third-party service providers must only use personal data for specified purposes and in accordance with our instructions, unless they act as independent controllers.

13. International transfers

We do not routinely transfer personal data outside the UK.

However, some website, IT, hosting, analytics or communications providers may process data outside the UK. Where personal data is transferred outside the UK, we will ensure appropriate safeguards are in place in accordance with applicable data protection laws. These may include

adequacy regulations, international data transfer agreements, standard contractual clauses, transfer risk assessments or other lawful safeguards.

14. Data security

We use appropriate security measures to help prevent personal data from being accidentally lost, used, accessed, altered or disclosed without authorisation.

We limit access to personal data to employees, workers, contractors, agents and service providers who have a business need to know. Those who process personal data on our behalf are subject to appropriate confidentiality and data protection obligations.

We have procedures to deal with suspected personal data breaches and will notify affected individuals and any applicable regulator where legally required.

15. Data retention

We will only keep personal data for as long as necessary for the purpose for which it was collected, including legal, accounting, tax, reporting, regulatory, contract, insurance, security and compliance purposes.

To decide how long to keep personal data, we consider the nature and sensitivity of the data, the purpose for which it is used, the risk of harm from unauthorised use or disclosure, legal and contractual requirements, and whether the data is needed for a complaint, dispute, audit, investigation or legal claim.

Examples include:

- website enquiries and general correspondence are normally kept for no longer than necessary to respond and manage the enquiry, unless an ongoing relationship, complaint, dispute or legal reason requires longer retention;
- customer, client, supplier, finance, transaction, credit and affordability check records are usually kept for six years after the end of the relevant relationship or transaction, unless a different period is required or justified;
- marketing preference records are kept while you receive marketing from us and suppression records may be kept, to ensure we respect opt-out requests;
- technical, cookie and analytics data are kept in line with the settings and retention periods of the relevant website, analytics or IT provider;
- career enquiry or applicant data submitted through the website is managed in line with our applicant privacy information and recruitment retention procedures;
- call recordings, where used, are kept only for as long as necessary unless needed for a complaint, investigation, legal claim, insurance matter, regulatory matter or security incident.

In some circumstances, we may anonymise personal data so that it can no longer identify you. We may use anonymised information indefinitely without further notice.

16. Provision of personal data

You do not have to provide personal data when browsing our website. However, if you choose not to provide information requested through a contact form or enquiry process, we may be unable to respond to your enquiry, provide requested information, consider a career enquiry or provide services.

Where personal data is requested for optional purposes, such as certain marketing communications or non-essential cookies, providing it is not mandatory and you may withdraw consent at any time.

17. Automated decision-making

We do not make decisions through this website that have a legal or similarly significant effect on individuals based solely on automated processing.

Website security, spam prevention, form management, analytics or similar tools may use automated processes to help operate and protect the website. These tools do not result in automatic rejection or adverse decisions without human involvement.

18. Your legal rights

Subject to certain exemptions, you have rights in relation to your personal data. These may include:

- **Right of access:** to request a copy of the personal data we hold about you and information about how it is used.
- **Right to rectification:** to ask us to correct inaccurate or incomplete personal data.
- **Right to erasure:** to ask us to delete personal data where there is no lawful reason for us to continue processing it.
- **Right to restrict processing:** to ask us to limit how we use personal data in certain circumstances.
- **Right to data portability:** to receive certain personal data in a structured, commonly used and machine-readable format, where this right applies.
- **Right to withdraw consent:** to withdraw consent at any time where we rely on consent.
- **Rights relating to automated decision-making:** where applicable, to request human intervention, express your point of view and challenge a decision made solely by automated means.

Right to object: You have the right to object to processing where we rely on legitimate interests. You also have the right to object to direct marketing at any time.

To exercise your rights, please contact info@vipsec.at.

19. Fees and time limits

You will not usually have to pay a fee to access your personal data or exercise your rights.

We may charge a reasonable fee or refuse to comply with a request if it is manifestly unfounded or excessive. We may also refuse to comply where an exemption or restriction applies.

We usually respond to legitimate requests within one month. If a request is complex or you have made a number of requests, we may take longer. If this happens, we will tell you and keep you updated.

We may need to request specific information from you to confirm your identity before responding. This helps ensure personal data is not disclosed to someone who has no right to receive it.

20. Complaints

If you have any questions, requests or complaints about this privacy notice or how we use personal data, please contact us first using the details below:

Email: info@vipsec.at

Telephone: 01268 526212

You also have the right to complain to the UK Information Commissioner's Office if you are dissatisfied with how we handle your personal data.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113

Website: www.ico.org.uk

21. Changes to this notice

This notice was last updated in June 2026.

Historic versions can be obtained by contacting us.

Please keep us informed if your personal data changes during your relationship with us. It is important that the personal data we hold is accurate and current.