Client, Applicant, Worker and Employee Privacy Notice

VIP SECURITY SERVICES

Reviewed on: June 2026

Next review due: June 2027

Document control

Field	Details
Document owner	VIP Security (Essex) Ltd
Data protection contact	VIP Security (Essex) Ltd – info@vipsec.at
Applies to	Clients, prospective clients, client contacts, applicants, candidates, employees, workers, contractors, self-employed individuals engaged by the Company, former staff, referees, emergency contacts and other individuals whose personal data is processed in connection with recruitment, employment, worker engagement or client services.
Status	Approved for issue

1. About this notice

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

1.2. This privacy notice explains how we collect, use, store, share and protect personal data when we deal with clients and prospective clients, provide security services, consider job applications, carry out recruitment, vetting and screening checks, engage workers or contractors, employ staff, manage our workforce, or process information connected with security services and client sites.

1.3. This notice also explains your legal rights and how data protection law protects you. It should be read alongside any specific privacy information we provide to you when collecting personal data, such as a website privacy notice, recruitment form privacy wording, vetting notice, CCTV notice, client contract, employee handbook or site-specific privacy information.

2. Who we are and how to contact us

2.1. VIP Security (Essex) Ltd is the data controller responsible for personal data collected and processed for its own business purposes.

Field	Details
Company name	VIP Security (Essex) Ltd
Company number	07940645
Registered office	Create Business Hub, Ground Floor, 5 Rayleigh Road, Hutton, Brentwood, Essex, CM13 1AB
Principal place of business	Security House, 4 Station Court, Wickford, Essex, SS11 7AT
Telephone	01268 526212
Email	info@vipsec.at

2.2. Data protection contact: VIP Security (Essex) Ltd is responsible for responding to data protection queries, rights requests and data protection complaints. Data protection matters should be sent to info@vipsec.at or to the principal place of business above. The Company has designated a data protection contact and will keep its Data Protection Officer position under review.

3. Who this notice applies to

3.1. This notice applies to personal data relating to:

- clients, customers and prospective clients, including individual clients, sole traders, partnerships, companies and client representatives;
- client site contacts, landlords, managing agents, occupiers, visitors, witnesses, service users and members of the public where their data is processed in connection with security services;
- applicants, candidates, prospective workers, prospective contractors and anyone applying for work or engagement with us;
- employees, workers, temporary staff, contractors, self-employed individuals engaged by us, former staff and former workers;
- referees, emergency contacts, next of kin, dependants, beneficiaries and other individuals whose data is provided to us as part of recruitment, employment, worker engagement or client service delivery.

4. When we act as controller or processor

4.1. In most cases, VIP Security (Essex) Ltd is the data controller for personal data we collect and use for our own business purposes. This includes client management, customer enquiries, quotations, accounts, debt recovery, recruitment, employment, worker management, vetting, SIA compliance, training, payroll, pensions, health and safety, audit, insurance, legal claims, marketing, website use and business administration.

4.2. In some cases, when providing security services to a client, we may process personal data on behalf of that client. This may include visitor logs, incident reports, CCTV, body-worn video, access control records, patrol records, keyholding records, alarm response records, assignment records or other site security records. In those circumstances, the client may be the data controller, and we may act as a data processor. The client's own privacy notice, site signage or local privacy information may also apply.

4.3. Where we act as a processor, we will process personal data only in accordance with the client's lawful instructions and any applicable contract.

5. Personal data we collect

5.1. Personal data means any information about an individual from which that person can be identified. We may collect, use, store and share the following types of personal data, depending on your relationship with us and the purpose of processing.

5.2. Some information may fall into more than one category depending on the purpose for which it is used. For example, SIA licence information may be used for recruitment, vetting, deployment and ongoing security industry compliance.

Type of personal data	Examples
Identity data	Name, title, date of birth, employee, worker, applicant, customer or supplier reference number, job title, employer or organisation, photographic identification, copies or details of identity documents, and other information used to identify or verify an individual.

Type of personal data	Examples
Contact data	Home, work or site address, email address, telephone number, emergency contact details and other contact details.
Client and customer data	Enquiries, quotations, service requirements, contracts, site information, assignment or service instructions, keyholding and alarm response details, invoicing records, account notes, complaints, feedback and service communications. Where a client, customer or supplier is a company or organisation, we may still process personal data relating to individual contacts, directors, employees, site contacts or other individuals connected with that relationship.
Recruitment and applicant data	Application forms, CVs, covering letters, employment history, qualifications, interview notes, assessment results, recruitment communications, role preferences, availability, references, screening information and suitability information.
Right to work data	Identity documents, Home Office share codes, online right to work check results, immigration status information, visa or permission details where relevant, expiry dates, follow-up check dates and other evidence needed to confirm and evidence the right to work.
Screening and vetting data	Employment history, education history where relevant, address history, identity verification, right to work evidence, gap verification, references, character or employment referee details, qualification checks, professional licence checks, SIA licence information, public record checks, financial probity or credit reference information where required and lawful, criminal record or DBS information where lawful and relevant, sanctions or watchlist checks where required and lawful, publicly available online or social media information where relevant and proportionate, social media usernames or handles where reasonably required to support a proportionate public-source check, and other information needed to carry out screening in line with BS 7858:2019 or any comparable security screening, client, contractual, regulatory or accreditation requirement.
SIA and security industry compliance data	SIA licence number, licence type, status, expiry date, licence conditions, licence checks, training and competency records, deployment records, assignment instructions, site instructions, incident records, patrol records, keyholding records, alarm response records, check call records, welfare or lone working check records, and other records needed to evidence security industry compliance and service delivery.
Employment, worker and HR data	Contracts, start date, role, site allocation, training, attendance, rotas, timesheets, payroll, pension, holiday, performance, disciplinary, grievance, welfare, absence, accident, uniform, equipment and issued-device records, including records relating to company mobile phones, tablets or other work-issued devices.
Financial and transaction data	Bank details, payroll, pension, payment details, billing, invoices, purchase orders, payment history, charges, expenses, deductions, deposits, advances and debt recovery.

Type of personal data	Examples
Credit reference, identity, financial probity and affordability data	Information from credit reference agencies or similar providers, including identity data, address data, credit commitments, payment history, public record information, affordability indicators and fraud prevention information, where relevant and lawful.
Operational security data	Visitor logs, access control records, patrol records, incident reports, witness details, vehicle details, images, CCTV, body-worn video, relevant audio, alarm response records, keyholding records and site security information.
Technical and system data	IP address, browser type and version, login data, location data where enabled, operating system, device type and identifiers, mobile phone and tablet information, system access records, audit logs and technology data relating to our website, systems, company mobile phones, tablets or other devices.
Profile, usage and communications data	Usernames, system profiles, communication preferences, feedback, survey responses, website or system usage and correspondence records.
Marketing data	Marketing preferences, communication preferences, opt-in and opt-out records.

6. Special category data and criminal offence data

6.1. Special category data includes information about race or ethnicity, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic data and biometric data used for identification.

6.2. Criminal offence data includes information relating to criminal convictions, offences, allegations, investigations, proceedings or related security measures.

6.3. We may process special category data or criminal offence data where it is lawful, necessary and proportionate. This may include where processing is required for employment, recruitment, vetting, safeguarding, health and safety, workplace adjustments, legal claims, compliance checks, insurance, client contract requirements or security incident management.

6.4. Examples may include health information needed for workplace adjustments, welfare, absence management or health and safety; criminal record check information where the role, contract or law permits or requires it; incident reports involving alleged criminal conduct; information needed to protect staff, clients, members of the public or property; or biometric data only where used and where a lawful basis and additional condition apply.

6.5. Where required, the Company will identify an Article 6 lawful basis, an Article 9 condition for special category data, and an Article 10 / Data Protection Act 2018 condition for criminal offence data. The Company maintains an Appropriate Policy Document for processing that requires one and keeps it under review alongside this notice, retention arrangements and related data protection procedures.

7. How we collect personal data

7.1. We may collect personal data from the following sources:

- directly from you, including when you complete forms, contact us, apply for a role, work with us, use our services, attend a client site or correspond with us;
- automatically, when you use our website, email, IT systems, rota systems, training systems, telephone systems or other systems, including through cookies and similar technologies where relevant;
- clients, customers, employers, agencies, business partners or site contacts where you apply for a role, are considered for work, provide services, attend a site, are involved in an incident or are connected to services we provide;
- referees, previous employers, education providers, training providers, professional bodies and licensing bodies where relevant and lawful;
- public sources, including professional networking sites, business websites, Companies House, public records, sanctions or watchlists where relevant and lawful, the public SIA register, and publicly available online or social media information where relevant and proportionate for recruitment, screening, employment, security, safeguarding, client assurance, BS 7858:2019 screening or counter-terrorism risk awareness purposes;
- social media usernames or handles provided by applicants, workers or employees where reasonably required to enable a proportionate review of publicly available online information for recruitment, screening, employment, security, safeguarding, client assurance, BS 7858:2019 screening or counter-terrorism risk awareness purposes;
- credit reference agencies and fraud prevention providers, where required for client credit, identity, affordability, financial probity or fraud prevention checks;
- DBS providers, screening providers or other background check providers where relevant and lawful;
- third-party service providers supporting recruitment, screening, compliance, IT, email, website, payroll, pension, finance, insurance, security, training, hosting, telephone systems, call recording and administration;
- clients, site contacts, witnesses, visitors, service users or members of the public in connection with security services, accidents, complaints or incidents;
- regulators, public authorities, law enforcement agencies, courts, tribunals or professional advisers.

7.2. The Company will not ask individuals to provide passwords, require access to private social media accounts, require individuals to connect with the Company on personal social media, or require screenshots or disclosure of private social media content.

8. Lawful basis for processing

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

Lawful basis	Meaning
Performance of a contract	Where processing is necessary to perform a contract with you, or to take steps at your request before entering into a contract.
Legal obligation	Where processing is necessary to comply with a legal obligation.

Lawful basis	Meaning
Legitimate interests	Where processing is necessary for our legitimate business interests, provided your rights and freedoms do not override those interests.
Recognised legitimate interests	Where processing is necessary for a recognised legitimate interest set out in data protection law. We will only rely on this where the relevant statutory condition applies.
Consent	Where we rely on your consent, such as for certain marketing communications or optional processing. You can withdraw consent at any time.
Vital interests	In rare situations, where processing is necessary to protect someone's life or physical safety.

8.1. Our legitimate interests may include operating and managing our business; providing security services; managing client sites and assignments; recruiting, vetting and deploying suitable staff, workers and contractors; checking SIA licence status and suitability for security work; supporting BS 7858:2019 screening and security-sector compliance; ensuring system, site and data security; preventing and detecting fraud, crime, misconduct and security risks; supporting audit, insurance, compliance and accreditation activities; maintaining accurate records; recovering debts owed to us; improving services and customer experience; and protecting our business, staff, workers, contractors, customers, suppliers, clients, service users, visitors and members of the public.

8.2. Where we process special category data or criminal offence data, we will also identify an additional condition under data protection law and the Data Protection Act 2018 where required. This may include employment law obligations, health and safety, safeguarding, substantial public interest, legal claims, regulatory requirements or explicit consent where appropriate.

9. Purposes for which we use personal data

9.1. The table below summarises the main purposes for which we use personal data. The exact data used will depend on the situation.

Purpose	Data used	Lawful basis / additional conditions
To register and manage clients, customers, suppliers and business contacts	Identity, contact, client/customer, financial, transaction and communications data	Performance of a contract, legitimate interests and/or legal obligation
To respond to enquiries, provide quotes and manage prospective client relationships	Identity, contact, client/customer, communications, financial and transaction data where relevant	Legitimate interests and/or steps before entering into a contract
To provide and manage security services	Identity, contact, operational security, SIA/security industry compliance, client/customer and communications data	Performance of a contract, legitimate interests, legal obligation and/or vital interests in emergencies

Purpose	Data used	Lawful basis / additional conditions
To carry out client/customer identity, creditworthiness, affordability or fraud prevention checks where relevant	Identity, contact, financial, transaction, credit reference, identity, affordability and fraud prevention data	Legitimate interests, legal obligation and/or performance of a contract
To process invoices, payments, payroll, pensions, charges, expenses, deposits, advances and debt recovery	Identity, contact, financial, transaction, employment, worker and HR data	Performance of a contract, legal obligation and legitimate interests
To recruit, vet and screen applicants, workers and contractors	Identity, contact, recruitment/applicant, screening/vetting, right to work, SIA/security industry compliance, financial probity and publicly available online/social media data where required and lawful	Steps before entering into a contract, performance of a contract, legal obligation and legitimate interests
To carry out BS 7858:2019 screening, security vetting and related suitability checks	Identity, contact, screening/vetting, employment history, address history, references, SIA/security industry compliance, right to work, financial probity, sanctions/watchlist, publicly available online/social media and criminal offence data where relevant and lawful	Legal obligation where applicable, legitimate interests, performance of a contract where relevant, substantial public interest where applicable, legal claims where applicable, and Article 10 / Data Protection Act 2018 condition where criminal offence data is processed
To carry out right to work checks	Identity, contact, right to work, recruitment/applicant and screening/vetting data	Legal obligation and legitimate interests for related record keeping, audit and deployment administration
To carry out DBS or criminal record checks where eligible and relevant	Identity, contact, recruitment/applicant, screening/vetting, DBS application data, criminal record information and suitability decision records	Legal obligation or legitimate interests where applicable, Article 10 / Data Protection Act 2018 condition, substantial public interest where applicable, legal claims where applicable, and APD where required
To carry out SIA licence checks and security industry compliance checks	Identity, SIA/security industry compliance, screening/vetting and training data	Legitimate interests, legal obligation and/or performance of a contract
To manage employees, workers, contractors and self-employed individuals engaged by us	Identity, contact, employment/worker/HR, payroll, pension, rota, attendance, training, SIA/security industry compliance, issued-device and operational security data	Performance of a contract, legal obligation and legitimate interests
To manage rotas, deployment, check calls, attendance, training and site allocation	Identity, contact, employment/worker/HR, rota, attendance, training, operational security and SIA/security industry compliance data	Performance of a contract, legal obligation and legitimate interests

Purpose	Data used	Lawful basis / additional conditions
To manage company mobile phones, tablets and other work-issued devices	Identity, contact, employment/worker/HR, technical and system data, device identifiers, mobile phone and tablet information, system access records, audit logs, usage records and security records	Legitimate interests, performance of a contract, legal obligation and/or recognised legitimate interests where applicable
To manage health, safety, welfare, workplace adjustments, absence and accidents	Identity, contact, employment/worker/HR, health, accident, welfare and operational security data	Legal obligation and/or legitimate interests. Where health or other special category data is used, Article 9 employment, social security and social protection obligations, health and safety, legal claims or explicit consent where appropriate
To investigate incidents, complaints, accidents, misconduct or security concerns	Identity, contact, operational security, employment/worker/HR, SIA/security industry compliance, special category data or criminal offence data where relevant	Legal obligation, legitimate interests, legal claims and/or recognised legitimate interests where applicable. Where special category or criminal offence data is used, an Article 9 or Article 10 / Data Protection Act 2018 condition will also be identified
To administer and protect our business, website, IT systems, company mobile phones, tablets, work-issued devices, premises and records	Identity, contact, technical, usage, system, device, audit and operational security data	Legitimate interests, legal obligation and/or recognised legitimate interests where applicable

10. Applicants, recruitment, vetting and screening

10.1. Where you apply for a role with us, we will process personal data for recruitment, vetting, screening and onboarding. As a private security company this may include checks needed to meet legal, regulatory, contractual, insurance, accreditation, client, security industry or **BS 7858:2019** requirements.

10.2. Screening may include right to work, SIA licence, identity, address history, employment history, gap verification, references, qualifications, training, financial probity or credit reference checks where required and lawful, sanctions or watchlist checks where relevant and lawful, publicly available online or social media checks where relevant and proportionate, and criminal record or DBS checks where permitted or required.

10.3. We will only carry out checks that are necessary, proportionate and relevant to the role, contract, site, client requirement or service. We may ask for information in stages.

10.4. Where publicly available online or social media information is reviewed, we will not ask for passwords, require access to private accounts or require disclosure of private social media content.

10.5. If you are unsuccessful, we will normally retain general recruitment information for up to six months after the recruitment decision. Where BS 7858 screening applies, preliminary screening records for unsuccessful individuals will normally be retained for at least 12 months after the

screening decision. If you are successful, relevant recruitment and vetting information will become part of your personnel, worker or contractor record.

11. Employees, workers and contractors

11.1. We process personal data to manage employment, worker and contractor relationships, including contracts, personnel records, rotas, deployment, attendance, timesheets, payroll, pensions, holiday, absence, welfare, training, performance, conduct, grievances, health and safety, site allocation, uniform, equipment and work-issued devices.

11.2. We may continue to process certain records after employment or engagement ends where this is necessary for legal, regulatory, tax, pension, payroll, insurance, contractual, audit, accreditation, complaint, investigation or legal claim purposes.

12. Credit reference, identity, financial probity and affordability checks

12.1. Where relevant and lawful, we may obtain information from credit reference agencies or similar providers. We use Creditsafe and its data partner TransUnion for certain credit reference, identity, financial probity, affordability and fraud prevention information.

12.2. For clients, prospective clients, customers, suppliers or other account relationships, checks may be used to assess identity, creditworthiness, affordability, fraud risk, payment risk, account suitability, contractual risk and debt recovery risk.

12.3. For applicants, workers or employees, credit reference, public record or financial probity checks will only be used where required, lawful, proportionate and relevant to the role, contract, security screening requirement, **BS 7858:2019** requirement, client requirement, insurance requirement or other compliance requirement. Affordability checks are not used as a general employee screening assessment.

12.4. The information we receive may include identity, address history, credit commitments, payment history, public record information, affordability indicators and fraud prevention information. This information will be used only for lawful and relevant business, compliance, screening, fraud prevention, account management or legal purposes.

12.5. Further information about how Creditsafe and TransUnion process personal data can be found in their privacy notices:

- Creditsafe Privacy / Transparency Notice: https://www.creditsafe.com/gb/en/legal/transparency-notice-customer-supplier.html
- TransUnion Credit Reference Agency Information Notice: https://www.transunion.co.uk/legal/privacy-centre/pc-credit-reference
- TransUnion Bureau Privacy Notice: https://www.transunion.co.uk/legal/privacy-centre/pc-bureau

13. CCTV, body-worn video and security incident data

13.1. Depending on the service, site and client requirements, personal data may be collected through CCTV, body-worn video, access control systems, visitor records, patrol records, alarm response records, incident reports, check call records or other security systems.

13.2. This information may be used to protect people, property and premises; prevent and detect crime; manage incidents; support health and safety; support insurance, legal, contractual or regulatory matters; assist clients, regulators or law enforcement where appropriate; and manage staff conduct, training and service quality where relevant.

13.3. Where CCTV or body-worn video is used at a client site, the client may be the data controller. Site signage, local procedures and the client's own privacy notice may also apply.

13.4. Recordings and incident records will only be kept for as long as necessary, unless they are required for an investigation, complaint, legal claim, insurance matter, disciplinary matter, client requirement, regulatory matter or law enforcement request.

14. Call recordings and communications

14.1. The Company's telephone system has active call recording and monitoring. Inbound callers receive an automated message informing them that calls will be recorded for compliance, quality and training purposes. Calls to or from the Company may be monitored or recorded for training, customer service, quality assurance, safety, complaint handling, dispute resolution, evidence, operational management and business administration purposes.

14.2. Call recordings and call logs are retained for a maximum of 90 days. A specific recording or log may be extracted and retained separately for longer only where this is necessary and proportionate for a complaint, investigation, legal claim, insurance matter, disciplinary matter, regulatory matter, safeguarding concern, security incident or law enforcement request.

14.3. The Company uses Grandstream/GDMS-related phone system services where applicable for telephone system management, provisioning, monitoring, support, diagnostics, call quality information, RemoteConnect, backups and related operational functions. Phone system data may include device identifiers, device model, firmware and hardware version, network information, account registration status, diagnostic information, call quality statistics where enabled, UCM statistics, call detail records, instant messaging data where used, support access and backup information.

14.4. Provider information supplied to the Company states that GDMS does not collect call audio or video content for call quality statistics and that UCMRC acts as a proxy service without storing transmitted media streams between UCM and terminals.

15. Marketing

15.1. We may use personal data to send information about our services where we are allowed to do so by law. This may include communications with clients, prospective clients and business contacts.

15.2. More detailed information about website enquiries, cookies and online marketing is provided in our website privacy notice.

15.3. You can ask us to stop sending marketing communications at any time by contacting us at info@vipsec.at or by using any unsubscribe or opt-out method provided.

16. Who we share personal data with

16.1. We may share personal data with:

- customers, clients, site contacts, landlords, managing agents, occupiers or business partners where necessary to provide services or fulfil contracts;
- the SIA and other regulatory, licensing or accreditation bodies where required;
- credit reference agencies and fraud prevention providers, including Creditsafe and TransUnion where relevant;
- DBS providers, screening providers and identity verification providers where used for DBS application processing, vetting, screening or related checks. For Enhanced DBS applications,

this may include DBS Umbrella Solution / EmploymentCheck, HR Connect powered by Cantium / Cantium Business Solutions, UK Fast.Net Ltd for system hosting, and relevant identity verification providers where used. The provider privacy notice is available at: https://dbschecks.employmentcheck.org.uk/content/privacy-notice;

- third-party service providers supporting IT, hosting, email, Microsoft 365, website, analytics, recruitment, screening, compliance, rota management, time and attendance, training, HR, payroll, pension, accounting, finance, insurance, security, administration, telephone systems, call recording, device management, cloud services or business operations;
- telephone, call recording and phone system providers, including Grandstream/GDMS-related providers where used for telephone system management, provisioning, support, diagnostics, call quality information, RemoteConnect, backups, call logs or related operational functions;
- regulators, public authorities, law enforcement agencies, courts or tribunals where required or where lawful and necessary;
- professional advisers, including lawyers, accountants, auditors, consultants and insurers;
- payment providers, banks, pension providers, benefits providers and debt recovery organisations where necessary;
- prospective buyers, sellers or merged entities where we sell, transfer or merge part of our business or assets.

16.2. We require third parties to respect the security of personal data and to treat it in accordance with the law. We do not allow third-party service providers to use personal data for their own purposes where they are processing data on our behalf. They may only process personal data for specified purposes and in accordance with our instructions, unless they are acting as an independent controller.

17. International transfers

17.1. We do not routinely transfer personal data outside the UK. However, some service providers, systems, support services, phone system services, cloud services or recipients may be located outside the UK, or may allow support access from outside the UK.

17.2. Where personal data is transferred outside the UK, we will ensure appropriate safeguards are in place in accordance with applicable data protection laws. These safeguards may include adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, transfer risk assessments or other lawful transfer safeguards approved under data protection law.

18. Data security

18.1. We use appropriate technical and organisational security measures to reduce the risk of personal data being accidentally lost, used, accessed, altered or disclosed without authorisation. Measures may include access controls, password controls, role-based permissions, secure storage, supplier checks, encryption or secure transmission where appropriate, audit logs, staff confidentiality obligations, staff training, secure disposal and incident management procedures.

18.2. The Company uses Microsoft 365 for email and related Microsoft services. The Computer Centre provides Microsoft 365 support and administration where required. The Company's Microsoft 365 data-at-rest locations are currently shown as United Kingdom.

18.3. Provider information supplied to the Company states that relevant Grandstream/GDMS communications use TLS v1.2, UCMRC media streams use SRTP with AES encryption, passwords are hashed before storage, and certain backup or device information is encrypted. The Company will keep supplier security information with its supplier due diligence records.

18.4. We limit access to personal data to employees, workers, agents, contractors and third parties who have a business need to know. Those who process personal data on our behalf must only do so on our instructions and are subject to appropriate confidentiality and security obligations.

18.5. We have procedures in place to deal with suspected personal data breaches and will notify affected individuals and the Information Commissioner's Office where legally required.

19. Data retention

19.1. We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including legal, accounting, tax, reporting, regulatory, employment, contract, screening, insurance, security and compliance purposes.

19.2. To decide the appropriate retention period, we consider the amount, nature and sensitivity of the personal data; the risk of harm from unauthorised use or disclosure; the purposes for which we process the data; whether we can achieve those purposes by other means; and legal, regulatory, contractual, insurance, audit and accreditation requirements.

19.3. Where BS 7858 screening applies, screening files are retained in line with the applicable screening standard and Company retention schedule. This includes retaining the screening file during employment or engagement, retaining relevant post-cessation screening records for seven years after employment or engagement ends, and retaining unsuccessful preliminary screening files for a minimum of 12 months unless a longer lawful retention reason applies.

Record type	Typical approach
Client, supplier, finance and transaction records	Usually kept for six years after the end of the relevant relationship or transaction, unless a longer period is required for legal, tax, contractual, insurance, audit or dispute reasons.
Recruitment records for unsuccessful applicants	Usually kept for up to six months after the recruitment process, unless a longer period is required for legal, regulatory, contractual, accreditation, insurance, screening, audit or business reasons. Where a person is unsuccessful at preliminary BS 7858 screening, the screening file is normally retained for a minimum of 12 months and then securely disposed of unless a longer lawful retention reason applies.
Successful applicant records	Relevant records become part of the personnel, worker or contractor file.
Right to work records	Kept for the duration of employment and for two years after employment ends.

Record type	Typical approach
DBS certificate information and DBS risk assessment records	DBS or criminal record checks are only requested where required as part of BS 7858:2019 or comparable security screening, and where lawful, relevant, proportionate and the role is eligible for the level of check requested. DBS certificate information is handled securely and is normally not kept for longer than necessary, usually no longer than six months unless exceptional circumstances apply. We may retain a record that a check was completed, the date, certificate number, level of check and recruitment or suitability decision where lawful and necessary. Where a DBS risk assessment form is completed, it may be retained as part of the employee, worker or contractor file where necessary to evidence the suitability decision, risk assessment, mitigation measures, safeguarding, screening, client assurance, audit, insurance, legal or regulatory compliance. Access will be restricted to authorised persons only.
Employment, worker and contractor records	Kept for as long as necessary for employment, payroll, tax, pension, insurance, legal, contractual, accreditation, screening and compliance purposes. PAYE records must be kept for at least three years from the end of the tax year they relate to. Many wider HR, personnel, contractual and employment records are usually kept for six years after employment or engagement ends, unless a different period applies.
Screening, vetting and SIA compliance records	Kept for as long as required for legal, regulatory, contractual, accreditation, insurance, audit, client assurance and applicable screening standard purposes. Where BS 7858 screening applies, relevant screening records are retained during employment or engagement and relevant post-cessation screening records are normally retained for seven years after employment or engagement ends, unless a different lawful retention reason applies.
Accident and health and safety records	Kept in line with health and safety, insurance and legal claim requirements. Accident and reportable incident records are usually kept for at least three years where applicable, and may be kept longer where needed for insurance, legal claim, regulatory, health and safety or safeguarding reasons.
CCTV, body-worn video and site security recordings	Kept only for as long as necessary, unless required for an investigation, complaint, legal claim, insurance matter, disciplinary matter, client requirement, regulatory matter or law enforcement request.
Call recordings and call logs	Retained for a maximum of 90 days in the telephone system. A specific recording or log may be extracted and retained separately for longer only where necessary and proportionate for a complaint, investigation, legal claim, insurance matter, disciplinary matter, regulatory matter, safeguarding concern, security incident or law enforcement request.

Record type	Typical approach
Credit reference, identity, financial probity and affordability checks	Kept only for as long as required for the relevant purpose and then securely deleted or anonymised, unless we are required or permitted by law to retain it for longer.
Phone system, diagnostic and backup data	Kept only for as long as necessary to operate, secure, troubleshoot, evidence and support the telephone system and related services. Call detail records, instant messaging data where used, diagnostic, device management, support and backup data are reviewed and deleted, overwritten or anonymised when no longer required, unless needed for security, audit, investigation, legal, insurance, regulatory or business continuity purposes.

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

20. Provision of personal data

20.1. Some personal data is required so that we can enter into or perform contracts, provide services, process applications, manage employment or worker relationships, carry out screening and vetting, check right to work, check SIA licence status, manage payments, recover debts and comply with legal, regulatory, accounting, tax, insurance, contractual, accreditation and security industry requirements.

20.2. If you do not provide personal data that we reasonably require, we may be unable to enter into or continue a contract with you, employ or engage you, deploy you to work, provide services, process an application, complete required verification, screening, vetting or compliance checks, or our services may be delayed, restricted or declined.

20.3. Where personal data is requested for optional purposes, such as certain marketing communications, providing it is not mandatory. Where we rely on consent, you may withdraw your consent at any time.

21. Automated decision-making and profiling

21.1. We may use automated systems and tools to support certain business processes, such as fraud prevention, client account checks, identity verification, recruitment screening administration, compliance checks, rota management, system security and record management.

21.2. These systems may help us organise, assess or flag information using predefined criteria or rules. However, we do not make decisions that have a legal or similarly significant effect on individuals based solely on automated processing. Any important decision affecting you will involve meaningful human review.

21.3. You may contact us for further information about any automated processing that affects you.

22. Your legal rights

22.1. Subject to certain exemptions, you have the following rights in relation to your personal data:

Right	What it means
Right of access	You have the right to request a copy of the personal data we hold about you and information about how it is used.

Right	What it means
Right to rectification	You have the right to request that inaccurate or incomplete personal data is corrected.
Right to erasure	You have the right to request that we delete your personal data where there is no lawful reason for us to continue processing it.
Right to restrict processing	You have the right to request that we limit how we use your personal data in certain circumstances.
Right to data portability	In certain circumstances, you have the right to receive personal data you have provided to us in a structured, commonly used and machine-readable format, and to request that we transfer it to another organisation where technically feasible.
Right to object	You have the right to object to the processing of your personal data where we rely on legitimate interests or where data is used for direct marketing.
Right to withdraw consent	Where we rely on consent, you have the right to withdraw that consent at any time.
Rights relating to automated decision-making	Where applicable, you have the right to request human intervention, express your point of view and challenge decisions made solely by automated means.

22.2. To exercise any of these rights, please contact us at info@vipsec.at.

23. Fees, identity checks and response times

23.1. You will not usually have to pay a fee to access your personal data or exercise your other rights. However, we may charge a reasonable fee, or refuse to comply with a request, if the request is manifestly unfounded or excessive, including where the request is repetitive.

23.2. We may need to request specific information from you to confirm your identity and ensure your right to access personal data or exercise your other rights. This is a security measure to ensure personal data is not disclosed to someone who has no right to receive it.

23.3. We will respond to rights requests without undue delay and normally within one month of the relevant time. Where permitted by law, the relevant time may depend on receipt of information reasonably needed to confirm identity, receipt of any reasonable fee requested for a manifestly unfounded or excessive request, or clarification reasonably required to identify the information requested. Where a request is complex or a number of requests have been made, the response period may be extended where permitted by law.

24. Complaints

24.1. If you have any queries, rights requests or complaints in relation to this privacy notice or any other data protection matter, please contact us using the contact details in section 2.

24.2. The Company will provide a way for individuals to make data protection complaints, acknowledge data protection complaints within 30 days, make appropriate enquiries, keep the complainant informed where necessary and respond without undue delay.

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

ICO contact	Details
Information Commissioner's Office	Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Telephone	0303 123 1113
Website	www.ico.org.uk

25. Clarity, accessibility and changes to this notice

25.1. We are committed to being transparent about how we collect, use and protect personal data. This privacy notice is intended to be clear, concise and easy to understand. If any part of this notice is unclear, or if you require further explanation, please contact us using the details in section 2 and we will assist where reasonable.

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

Last reviewed in **June 2026**

Next review due in **June 2027**

25.3. or earlier if there are material changes in data protection law, ICO guidance, Company systems, suppliers, services, processing activities, retention arrangements or operational procedures. Historic versions can be obtained by contacting the Company using the details in section 2.