Privacy Policy - updated: 18/12/2025
Version: 5.0

---

1. Introduction

1.1 Hound Security Limited ("we", "us", "our") is committed to protecting your personal data and respecting your privacy.

1.2 This Privacy Policy explains how we collect, use, store, and protect your personal information when you use our services or interact with our website www.houndsecurity.co.uk.

1.3 Hound Security Limited is the Data Controller responsible for your personal data. This means we determine how and why your personal data is processed.

1.4 This policy complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.5 Please read this Privacy Policy carefully to understand how we handle your personal data. If you have any questions, please contact us using the details in Section 15.

---

2. Who We Are

2.1 **Company Name:** Hound Security Limited

2.2 **Registered Address:** 142 High Street, Codicote, Hitchin, SG4 8UB

2.3 **Company Registration Number:** 11392780

2.4 **Contact Details:**

- **Email:** compliance@houndsecurity.co.uk
- **Phone:** 01462 226 325
- **Website:** www.houndsecurity.co.uk

---

3. What Personal Data We Collect

3.1 We collect and process the following categories of personal data:

3.1.1 Customer and Business Contact Information

- Contact name
- Job title
- Company name
- Business telephone number
- Business email address
- Mobile telephone number
- Business address

3.1.2 Financial Information

- Bank account information (when required for payment processing)
- Payment card details (processed by our payment service providers)
- Billing address
- Purchase history and invoices

3.1.3 Account and Service Information

- Account credentials (username and password)
- Service preferences and settings
- Communication preferences
- Customer service correspondence
- Technical support requests and history

3.1.4 Website Usage Information

- IP address
- Browser type and version
- Operating system
- Pages visited and time spent on pages
- Referring website
- Cookies and similar tracking technologies (see our Cookie Policy)

3.1.5 Employment and Recruitment Data (Employees and Candidates Only)

- CV/Resume
- Employment history
- Educational qualifications
- Professional certifications
- References
- Right to work documentation
- Date of birth
- Home address
- National Insurance number
- DBS check results (where applicable and with consent)
- Emergency contact information

3.2 **Special Category Data:** We do not routinely collect special category data (such as health information, racial or ethnic origin, religious beliefs, etc.). However, we may collect:

- Criminal convictions data (DBS checks) for employment purposes where legally justified and with your explicit consent
- Health information only if you voluntarily provide it for reasonable adjustments or emergency situations

3.3 **Children's Data:** Our services are not directed at children under 16 years of age. We do not knowingly collect personal data from children.

---

4. How We Collect Your Personal Data

4.1 We collect personal data through the following methods:

(a) **Directly from you** when you:

- Fill in forms on our website
- Contact us by phone, email, or post
- Request a quote or information about our services
- Place an order or enter into a contract with us
- Register for an account on our website
- Subscribe to our newsletters or marketing communications
- Apply for employment with us
- Attend our premises or events

(b) **Automatically** when you:

- Visit our website (through cookies and similar technologies)
- Use our online services and portals

(c) **From third parties** including:

- Business partners and referral sources
- Publicly available sources (e.g., Companies House, LinkedIn)
- Credit reference agencies (for business credit checks)
- Background check providers (for employment screening with consent)

4.2 We will inform you at the time of collection if we obtain your personal data from a source other than you directly.

---

5. How and Why, We Use Your Personal Data

5.1 We will only use your personal data when the law allows us to. The lawful bases we rely on are:

(a) **Performance of a contract** - where we need to process your data to fulfil our contractual obligations to you (b) **Legal obligation** - where we need to process your data to comply with the law (c) **Legitimate interests** - where we have a legitimate business reason to process your data (d) **Consent** - where you have given us specific permission to use your data

5.2 Purposes and Lawful Bases

Purpose	**Type of Data**	**Lawful Basis**
To set up and manage your account	Contact information, account credentials	Performance of a contract
To process and fulfil orders	Contact, financial, service information	Performance of a contract
To provide customer service and technical support	Contact information, service history, correspondence	Performance of a contract
To process payments and prevent fraud	Financial information, transaction history	Performance of a contract, legal obligation
To send service-related communications	Contact information	Performance of a contract
To improve our website and services	Website usage data, feedback	Legitimate interests (improving our services)
To conduct business analysis and reporting	Aggregated and anonymised data	Legitimate interests (business operations)

Purpose	Type of Data	Lawful Basis
To send marketing communications	Contact information, communication preferences	Consent (you can opt out at any time)
To comply with legal and regulatory requirements	Various data as required by law	Legal obligation
To recruit and manage employees	Employment data, background checks	Performance of a contract, legal obligation, consent (for special category data)
To protect our business and your data	Security logs, IP addresses	Legitimate interests (security and fraud prevention)

5.3 **Legitimate Interests:** When we rely on legitimate interests, we have balanced our interests against your rights and freedoms. Our legitimate interests include:

- Running and growing our business efficiently
- Preventing fraud and maintaining security
- Improving our services based on customer feedback
- Network and information security
- Internal administrative purposes

5.4 You have the right to object to processing based on legitimate interests. See Section 10 for more information about your rights.

---

6. Marketing Communications

6.1 We will send you marketing communications about our products and services if:

- You have given us specific consent to do so, OR
- You are an existing customer and we are marketing similar products/services (soft opt-in)

6.2 You can opt out of marketing communications at any time by:

- Clicking the "unsubscribe" link in any marketing email
- Contacting us at info@houndsecurity.co.uk
- Updating your preferences in your account settings (if applicable)
- Calling us on 0800 689 3591

6.3 Even if you opt out of marketing, we will still send you service-related communications necessary to provide our services to you.

---

7. Who We Share Your Personal Data With

7.1 We may share your personal data with the following categories of third parties:

7.1.1 Service Providers and Processors

We engage third-party companies to perform services on our behalf, including:

- **IT service providers** - for hosting, cloud storage, and technical support
- **Payment processors** - to process card payments and bank transfers
- **Email service providers** - for sending communications
- **CRM and database providers** - for managing customer relationships
- **Professional advisers** - including lawyers, accountants, and insurers
- **Marketing and analytics providers** - to help us improve our services

7.1.2 Business Partners

- **Installation and maintenance partners** - to deliver and maintain security equipment
- **Monitoring service providers** - to provide 24/7 security monitoring services
- **Subcontractors** - who assist in service delivery

7.1.3 Legal and Regulatory Bodies

- Law enforcement agencies, courts, and regulatory bodies when required by law
- HMRC, tax authorities, and auditors for compliance purposes

7.1.4 Business Transfers

- Potential buyers or investors in the event of a business sale, merger, or acquisition

7.2 **Data Processor Agreements:** All third-party service providers who process personal data on our behalf are required to:

- Process your data only on our instructions
- Maintain appropriate security measures
- Comply with UK GDPR requirements
- Sign a Data Processing Agreement with us

7.3 **No Data Selling:** We will never sell, rent, or trade your personal data to third parties for marketing purposes.

7.4 **Your Consent:** If we need to share special category data (such as DBS results) with third parties, we will only do so with your explicit consent, unless legally required otherwise.

---

8. International Data Transfers

8.1 **Location of Data Processing:** Your personal data is primarily processed and stored within the United Kingdom.

8.2 **Transfers Outside the UK/EEA:** Some of our service providers may be located outside the UK or European Economic Area (EEA). When we transfer your personal data internationally, we ensure appropriate safeguards are in place, including:

(a) **Adequacy Decisions:** Transferring data only to countries that the UK Government has determined provide an adequate level of data protection

(b) **Standard Contractual Clauses (SCCs):** Using UK-approved Standard Contractual Clauses with data recipients

(c) **Additional Safeguards:** Implementing supplementary security measures where necessary

8.3 You can request more information about the safeguards we use for international transfers by contacting our Data Protection Officer (see Section 15).

---

9. How Long We Keep Your Personal Data

9.1 We will only retain your personal data for as long as necessary to fulfil the purposes for which it was collected, including to satisfy any legal, accounting, or reporting requirements.

9.2 **Retention Periods by Category:**

Data Category	**Retention Period**	**Reason**
Customer account and contact information	Duration of business relationship + 6 years	Legal obligations (limitation period for contracts)
Financial records and invoices	6 years after end of financial year	Legal obligations (tax and accounting requirements)
Marketing consent records	Until consent is withdrawn + 3 years	Evidence of consent
Customer service correspondence	Duration of relationship + 3 years	Business needs and complaint handling
Website analytics data	26 months	Business intelligence and service improvement
CCTV footage (if applicable)	30 days (unless required for investigation)	Security and legal obligations
Employment records (current employees)	Duration of employment + 6 years	Legal obligations
Employment records (unsuccessful applicants)	6 months after recruitment process	Potential discrimination claims

Data Category	Retention Period	Reason
DBS certificates	6 months after verification (certificate details not retained)	Legal compliance and best practice

9.3 **Deletion and Anonymisation:** After the retention period expires, we will either:

- Securely delete or destroy your personal data, OR
- Anonymise it so that you can no longer be identified

9.4 **Legal Holds:** In some circumstances, we may need to retain personal data for longer periods if required by law, for legal proceedings, or to protect our legal rights.

---

10. Your Rights as a Data Subject

10.1 Under UK GDPR, you have the following rights regarding your personal data:

10.1.1 Right to Be Informed

You have the right to know how your personal data will be processed. This Privacy Policy provides that information.

10.1.2 Right of Access

You have the right to request a copy of the personal data we hold about you. This is known as a "Subject Access Request" (SAR).

10.1.3 Right to Rectification

You have the right to request that we correct any inaccurate or incomplete personal data we hold about you.

10.1.4 Right to Erasure ("Right to be Forgotten")

You have the right to request that we delete your personal data in certain circumstances, including:

- The data is no longer necessary for the purpose it was collected
- You withdraw your consent (where consent was the lawful basis)
- You object to processing and there are no overriding legitimate grounds
- The data has been unlawfully processed
- The data must be erased to comply with a legal obligation

Please note that this right is not absolute, and we may need to retain certain data to comply with our legal obligations or establish legal claims.

10.1.5 Right to Restrict Processing

You have the right to request that we restrict the processing of your personal data in certain circumstances, such as:

- You contest the accuracy of the data

- The processing is unlawful, but you don't want the data erased
- We no longer need the data, but you need it for a legal claim
- You have objected to processing pending verification of our legitimate grounds

10.1.6 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transfer it to another data controller where:

- The processing is based on consent or contract performance, AND
- The processing is carried out by automated means

10.1.7 Right to Object

You have the right to object to processing of your personal data where:

- Processing is based on legitimate interests or public interest
- Processing is for direct marketing purposes (we will stop immediately)
- Processing is for research or statistical purposes (unless required for public interest)

10.1.8 Rights Related to Automated Decision-Making and Profiling

You have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects.

We do not currently use automated decision-making or profiling.

10.2 **How to Exercise Your Rights:**

To exercise any of these rights, please contact us at:

- **Email:** info@houndsecurity.co.uk or dpo@houndsecurity.co.uk
- **Post:** Hound Security Limited, 10 The Paddocks, Codicote, Hitchin, SG4 8YX
- **Phone:** 0800 689 3591

10.3 **Response Time:** We will respond to your request within one month. If your request is complex or we receive multiple requests, we may extend this by a further two months and will inform you of this.

10.4 **Identification:** To protect your privacy, we will need to verify your identity before processing your request. We accept the following forms of identification:

- Passport
- Driving Licence
- Birth Certificate
- Recent utility bill (dated within the last three months)

10.5 **Fees:** You will not have to pay a fee to exercise most of your rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

10.6 **Third Parties:** If we have shared your data with third parties, we will inform them of any rectification, erasure, or restriction requests where possible, unless this is impossible or involves disproportionate effort.

---

11. How We Protect Your Personal Data

11.1 We take the security of your personal data seriously and have implemented appropriate technical and organisational measures to protect your data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

11.2 **Security Measures Include:**

(a) **Technical Measures:**

- Encryption of data in transit (using SSL/TLS)
- Encryption of sensitive data at rest
- Secure password policies and authentication systems
- Regular security updates and patch management
- Firewalls and intrusion detection systems
- Secure backup and disaster recovery procedures
- Anti-virus and anti-malware protection

(b) **Organisational Measures:**

- Access controls and role-based permissions (staff only have access to data they need)
- Staff training on data protection and security
- Confidentiality agreements with all staff and contractors
- Regular security audits and assessments
- Clear data protection policies and procedures
- Incident response and breach notification procedures
- Secure disposal of data (shredding, secure deletion)

11.3 **Physical Security:** Our premises are secured with:

- Access control systems
- CCTV monitoring (where appropriate and with signage)
- Secure storage for physical documents
- Visitor management procedures

11.4 **Third-Party Security:** We require all third-party service providers to maintain appropriate security standards and comply with UK GDPR requirements.

11.5 **Data Breach Notification:** In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will:

- Notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach
- Notify you without undue delay if the breach is likely to result in a high risk to you
- Document all breaches and our response

---

12. Cookies and Website Tracking

12.1 Our website uses cookies and similar tracking technologies to improve your browsing experience and analyse website usage.

12.2 **What are Cookies?** Cookies are small text files placed on your device when you visit our website. They help us remember your preferences and understand how you use our site.

12.3 **Types of Cookies We Use:**

- **Strictly necessary cookies** - essential for website functionality (no consent required)
- **Analytics cookies** - help us understand how visitors use our site (requires consent)
- **Functionality cookies** - remember your preferences (requires consent)
- **Marketing cookies** - track your browsing for advertising purposes (requires consent)

12.4 **Managing Cookies:** You can control and manage cookies through your browser settings or our cookie preference centre. For full details, please see our Cookie Policy at [INSERT COOKIE POLICY URL].

12.5 Blocking cookies may affect the functionality of our website.

---

13. Links to Other Websites

13.1 Our website may contain links to third-party websites, plug-ins, and applications.

13.2 Clicking on those links or enabling those connections may allow third parties to collect or share data about you.

13.3 We do not control these third-party websites and are not responsible for their privacy practices.

13.4 We encourage you to read the privacy policy of every website you visit.

---

14. Changes to This Privacy Policy

14.1 We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors.

14.2 We will notify you of any significant changes by:

- Updating the "Last Updated" date at the top of this policy
- Posting a prominent notice on our website
- Sending you an email notification (if we have your email address)

14.3 We encourage you to review this Privacy Policy periodically to stay informed about how we protect your personal data.

---

15. Contact Us and Complaints

15.1 If you have any questions, concerns, or requests regarding this Privacy Policy or how we handle your personal data, please contact us:

General Enquiries:

- **Email:** compliants@houndsecurity.co.uk
- **Phone:** 01462 226 325
- **Post:** Hound Security Limited, 142 High Street, Codicote, Hitchin, SG4 8UB

15.2 **Making a Complaint:**

If you believe we have not handled your personal data in accordance with UK GDPR, you have the right to lodge a complaint with us. We will investigate and respond to your complaint promptly.

If you are not satisfied with our response, you have the right to complain to the supervisory authority:

Information Commissioner's Office (ICO)

- **Website:** www.ico.org.uk
- **Phone:** 0303 123 1113
- **Email:** casework@ico.org.uk
- **Post:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

15.3 We would appreciate the opportunity to address your concerns before you approach the ICO, so please contact us first if possible.

---

16. Definitions

For ease of reference, the following terms have the meanings set out below:

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or online identifier.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data.
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

Term	Definition
Data Subject	An identified or identifiable natural person whose personal data is processed.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them.
UK GDPR	The UK General Data Protection Regulation as transposed into UK law under the Data Protection Act 2018.
ICO	The Information Commissioner's Office, the UK's independent supervisory authority for data protection.

End of Privacy Policy

Document Control:

- **Classification:** Public
- **Version:** 5.0
- **Issued Date:** December 18, 2025
- **Next Review Date:** December 18, 2026
