Tel: 0203 397 1686

2012 SECURITY LTD
Third Floor Office (T4)
Rainham House
New Road
Rainham
Essex
RM13 8RA
2012enquiries@2012security.co.uk
www.2012security.co.uk

Data Protection Policy

1. Purpose

2012 Security Ltd is committed to ensuring the lawful, fair, and transparent processing of personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out how the Company manages personal data to:

- Protect the rights of individuals
- Maintain client and stakeholder confidence
- Ensure legal and regulatory compliance
- Support operational integrity within the security industry

2. Scope

This policy applies to all personal data processed by the Company, including:

- Employee and contractor data
- Client and customer data
- Incident reports and operational records
- CCTV and surveillance data
- Visitor and access control records

It applies to all employees, contractors, and any person acting on behalf of the Company.

3. Data Controller Status

2012 Security Ltd acts as a Data Controller and is registered with the Information Commissioner's Office (ICO).

4. Definitions

- Personal Data: Any information relating to an identifiable individual
- Special Category Data: Sensitive data (e.g. health, ethnicity, biometrics)
- Criminal Offence Data: Data relating to convictions or offences
- Processing: Any operation performed on personal data

5. Data Protection Principles

The Company will ensure that personal data is:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Retained only as long as necessary
6. Secured appropriately against unauthorised access or loss
7. Processed in line with accountability obligations

6. Lawful Basis for Processing

The Company will only process personal data where a lawful basis exists, including:

- Contractual necessity (e.g. employment, service delivery)
- Legal obligation (e.g. HMRC, licensing requirements)
- Legitimate interests (e.g. security operations, incident prevention)

Consent will only be relied upon where it is appropriate and can be freely given, and individuals will have the right to withdraw consent at any time.

7. Types of Data Processed

7.1 Employee and Contractor Data Includes:

- Personal and contact details
- Employment records
- Payroll and tax information
- Training and performance records
- Health information (where required)

7.2 Operational and Security Data

Includes:

- Incident reports
- Patrol logs
- Canine deployment records
- Access control logs
- Visitor records

7.3 CCTV and Surveillance Data

The Company may operate:

- CCTV systems
- Body-worn cameras (where applicable)

Controls include:

- Clear signage informing individuals
- Defined purpose (crime prevention, safety, evidence)
- Restricted access to footage
- Secure storage and controlled retention

8. Data Subject Rights

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data (Subject Access Request)
- Rectify inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Data portability
- Object to processing
- Not be subject to automated decision-making

Requests will be responded to within one month.

9. Data Security

The Company implements appropriate technical and organisational measures, including:

- Access controls and role-based permissions
- Password protection and encryption
- Secure storage of physical records
- Locked cabinets for confidential documents
- Screen locking on unattended devices
- Secure handling of portable devices

Personal data must not be shared, removed, or accessed without authorisation.

10. Data Sharing and Third Parties

Where third parties process data on behalf of the Company:

- A Data Processing Agreement (DPA) will be in place
- Third parties must demonstrate appropriate security measures
- Data sharing will be limited to what is necessary

11. International Data Transfers

Where personal data is transferred outside the UK, appropriate safeguards will be implemented, including:

- Adequacy regulations
- Standard contractual clauses

12. Data Breach Management

All data breaches must be reported immediately.

The Company will:

- Assess risk and impact
- Record the breach in a breach register
- Report to the ICO within 72 hours where required
- Notify affected individuals where there is high risk

13. Data Retention

Personal data will only be retained for as long as necessary. Retention periods are defined in the Company's Data Retention Schedule (see below).

14. Responsibilities

All Employees and Contractors

- Comply with this policy
- Protect personal data
- Report breaches or concerns immediately

Management

- Ensure compliance and oversight
- Provide training and awareness
- Monitor adherence

Data Protection Lead Ann O'Neill

Responsible for:

- Data protection compliance
- Policy review and audit
- ICO liaison

15. Training and Awareness

- All staff receive data protection training at induction
- Refresher training is provided as required
- Staff are made aware of breach reporting procedures

16. Monitoring and Review

This policy will be reviewed annually or following:

- Legislative changes
- Data breaches
- Operational changes

Data Retention Schedule (ACS-Ready)

Data Type	Examples	Retention Period	Reason
Employee Records	Contracts, personnel files	6 years after employment ends	Legal / employment claims
Payroll Records	PAYE, tax, NI	6 years	HMRC requirement
Right to Work Docs	ID, visas	Duration of employment + 2 years	Home Office compliance
Training Records	SIA, internal training	3 years (or duration of employment)	Compliance / audit
Disciplinary Records	Warnings, investigations	12 months (or longer if serious)	Employment management
Accident Reports	Incident logs, RIDDOR	3 years (minimum)	Legal requirement
CCTV Footage	Surveillance recordings	30 days (unless required for investigation)	ICO guidance
Bodycam Footage	Operational recordings	30–90 days	Evidence / operational need
Incident Reports	Security incidents	3–6 years	Legal / client requirements
Access Control Logs	Entry/exit records	12 months	Security / audit
Visitor Logs	Sign-in records	12 months	Security
Client Contracts	Agreements, SLAs	6 years after contract ends	Legal
Supplier Records	Contracts, invoices	6 years	Financial compliance
Complaints Records	Client complaints	3 years	Audit / dispute resolution
Insurance Records	Claims, policies	6 years	Legal / insurer requirement

Signed T Theodorou

On behalf of 2012 Security Ltd