

DATA PROTECTION POLICY

UK GDPR governance and personal-information handling

Document ID	P-13	Issue date	01/01/2026
Version	1	Status	Signed Off

1. PURPOSE AND SCOPE

1.1 2012 Security Ltd will process personal information lawfully, fairly, transparently and securely. This policy applies to directors, employees, workers, contractors and others handling personal information for the Company and covers HR, vetting, payroll, client, operational, CCTV/BWV, access-control, incident, supplier, telephone call-recording and electronic-communications information.

2. DATA PROTECTION PRINCIPLES

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability and demonstrable compliance.

3. LAWFUL BASIS AND SENSITIVE INFORMATION

3.1 A lawful basis must be identified for each processing purpose. Appropriate bases may include contract, legal obligation, legitimate interests, vital interests, public task or consent. Consent must not be used merely because it appears convenient where another basis better reflects the processing.

3.2 Special-category and criminal-offence information requires additional legal conditions and safeguards. Access must be limited and the purpose documented.

3.3 Routine business-call recording does not rely on caller consent. The Company processes call recordings for documented legitimate interests including quality assurance, training, establishing facts, evidential purposes, complaint/dispute resolution and protection of the Company, its workers and clients, subject to the applicable balancing and risk assessments.

4. TRANSPARENCY AND INDIVIDUAL RIGHTS

4.1 Appropriate privacy information must be provided to data subjects. Rights requests must be recognised and escalated promptly. The Company maintains separate procedures for subject access and other data-subject rights.

4.2 The Company publishes call-recording transparency information on its website. Detailed privacy information must remain accurate and accessible and must explain the purposes of processing, lawful basis, retention and relevant individual rights.

5. SECURITY AND ACCESS

- least-privilege and role-based access;
- strong authentication and secure credential handling;
- secure storage and transmission;
- screen locking, encryption and patching where appropriate;
- controlled use of portable media, personal devices and cloud services;
- secure disposal and deletion;
- access to call recordings is restricted to one designated authorised person; access credentials must not be shared and recordings may only be accessed, exported or disclosed for an authorised business purpose.
- prompt reporting of loss, misdirection, phishing, unauthorised access or other suspected breach.

6. DATA SHARING AND PROCESSORS

6.1 Personal information may only be shared where there is a lawful purpose, appropriate authority and a need to know. Processors must be subject to appropriate contractual terms and security requirements. Data-sharing arrangements must reflect the parties' actual controller/processor roles.

6.2 3CX is the Company telephone-system provider for call recording. Call recordings are hosted in the United Kingdom. Applicable supplier, security and data-processing arrangements must be retained and reviewed as appropriate.

7. INTERNATIONAL TRANSFERS

7.1 Transfers outside the UK must use a lawful transfer mechanism, such as adequacy regulations or appropriate contractual safeguards, and must consider any required transfer-risk assessment or supplementary measures.

8. DATA BREACHES

8.1 Suspected personal-data breaches must be reported immediately under the Information Security Incident Response Procedure. The Company will assess risk, maintain a breach record and notify the ICO and affected people where legally required. The statutory ICO notification period is 72 hours after becoming aware of a reportable breach.

9. RETENTION AND DISPOSAL

9.1 Personal information will be retained in accordance with the Company retention schedule, legal, contractual, regulatory and limitation requirements. Records must be securely deleted, destroyed or anonymised when retention is no longer justified.

9.2 Routine call recordings are retained for 12 months and the 3CX configuration is set to delete them automatically at the end of that period. A specific recording may be retained longer only where required for a documented complaint, investigation, legal/evidential matter, regulatory requirement or other authorised hold.

10. MONITORING, CCTV AND WORKER DATA

10.1 Monitoring must be necessary, proportionate and transparent. Higher-risk monitoring should be assessed in advance, including through a Data Protection Impact Assessment where required. Workers must receive appropriate privacy information and access to monitoring outputs must be controlled.

10.2 The Company maintains a Call Recording and Communications Monitoring Data Protection Impact Assessment. It must be reviewed when there is a material change to the purposes, technology, supplier, hosting, access arrangements, retention period, disclosure practices or other relevant risk factors.

11. RESPONSIBILITIES AND TRAINING

11.1 The Managing Director has overall accountability. The Data Protection Lead coordinates compliance, rights requests, breaches and advice. All users are responsible for handling personal information securely and completing appropriate data-protection training.

12. REFERENCES

- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- ICO guidance
- Access Control and Acceptable Use Policy
- Information Security Incident Response Procedure
- IS-02 Subject Access Request Policy
- P-06 Communications and Electronic Communications Policy
- Call Recording and Communications Monitoring Data Protection Impact Assessment

DOCUMENT CONTROL

Document owner	AON - Ann O'Neill
Reviewer	TT - Theo Theodorou
Approver	Managing Director (MD)
Document ID	P-13
Document reference	P-13/1-01/01/26
Version	1
Supersedes	None - first controlled issue
Status	Signed Off
Effective date	01/01/2026
Revision date	1 September 2026
Review date	8 January 2027; earlier on material change

Review date aligned to 8 January 2027.