



SAFEDATASTORAGE

Data Protection Policy

| | |
|----------------------|----------------------|
| Document Ref. | POL 18 |
| Version: | 5 |
| Reviewed: | 12 March 2026 |

Data Protection Policy

1. Purpose

Safe Data Storage Ltd is committed to protecting the privacy and security of personal data. This policy outlines how the organisation ensures compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The purpose of this policy is to ensure that personal data is processed lawfully, fairly, securely and transparently.

2. Scope

This policy applies to:

- All employees
- Directors
- Contractors
- Third-party processors acting on behalf of Safe Data Storage Ltd

It applies to all personal data processed by the company, including:

- Customer data
- Employee data
- Supplier data
- Data stored within backup systems and disaster recovery environments

3. Definitions

Personal Data

Any information relating to an identified or identifiable individual.

Processing

Any operation performed on personal data including collection, storage, use, transmission, or deletion.

Data Subject

The individual whose personal data is processed.

Controller

The organisation that determines the purpose and means of processing personal data.

Processor

An organisation that processes personal data on behalf of a controller.

4. Data Protection Principles

Safe Data Storage Ltd processes personal data in accordance with the following principles under **Article 5 of the UK GDPR**:

Personal data must be:

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. **Kept only as long as necessary**
6. **Processed securely**
7. **Accountable and demonstrably compliant**

The organisation maintains appropriate policies, procedures and records to demonstrate compliance with these principles.

5. Lawful Basis for Processing

Safe Data Storage Ltd processes personal data only where a lawful basis applies, including:

- Contractual necessity
- Legal obligations
- Legitimate interests
- Consent (where required)

The lawful basis for processing is documented where applicable.

6. Roles and Responsibilities

Overall responsibility for data protection compliance rests with the **Company Director / Data Protection Lead**.

Responsibilities include:

- Ensuring compliance with UK GDPR
- Maintaining data protection policies
- Responding to data protection enquiries
- Managing data breach reporting
- Ensuring staff awareness and training

All employees are responsible for:

- Protecting personal data
- Following company data protection procedures
- Reporting suspected breaches immediately

7. Information Security

Safe Data Storage Ltd implements appropriate **technical and organisational measures** to protect personal data from unauthorised access, loss, or disclosure.

These measures include:

- Encryption of data in transit and at rest where appropriate
- Secure authentication and access control
- Role-based access to systems and data
- Secure backup and disaster recovery processes
- System logging and monitoring
- Regular software updates and patching
- Secure device management
- Secure disposal of data and equipment
- Staff training and awareness

Access to personal data is restricted to authorised personnel only.

8. Data Storage and Backup

As a provider of **online backup and disaster recovery services**, Safe Data Storage Ltd may store customer data on secure systems and infrastructure.

Controls include:

- Secure storage environments
- Access restrictions to authorised personnel
- Encryption where applicable
- Monitoring of access and system activity
- Secure recovery and restoration procedures

Customer data remains the responsibility of the **data controller (the client)** where Safe Data Storage Ltd acts as a **data processor**.

9. Data Retention

Personal data will not be retained longer than necessary.

Safe Data Storage Ltd maintains a **Data Retention Schedule** which defines retention periods for different types of data.

Data that is no longer required will be securely deleted or anonymised.

10. Data Subject Rights

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights related to automated decision-making

Requests relating to these rights will be handled in accordance with UK GDPR requirements.

11. Data Breach Management

A **personal data breach** is any incident that results in the loss, unauthorised access, disclosure or alteration of personal data.

All employees must report suspected breaches immediately.

Safe Data Storage Ltd will:

1. Investigate the breach
2. Assess the risk to individuals
3. Take steps to mitigate the impact
4. Notify the **Information Commissioner’s Office (ICO)** within **72 hours** where required
5. Inform affected individuals if there is a high risk to their rights and freedoms

All breaches are recorded and reviewed.

12. Third-Party Processors

Where Safe Data Storage Ltd uses third-party service providers that process personal data, the organisation ensures that:

- Appropriate **Data Processing Agreements (DPAs)** are in place
- Processors meet UK GDPR security standards
- Data is processed only according to documented instructions

13. International Data Transfers

Where personal data is transferred outside the United Kingdom, Safe Data Storage Ltd ensures appropriate safeguards are in place.

These may include:

- UK adequacy decisions

- International Data Transfer Agreements (IDTAs)
- Standard contractual clauses

14. Training and Awareness

All staff receive appropriate training in:

- Data protection principles
- Secure data handling
- Recognising data breaches
- Company data protection procedures

Training is provided during initial training and annually thereafter.

15. Complaints

Individuals who believe their data has been processed unlawfully may contact Safe Data Storage Ltd.

If a complaint cannot be resolved internally, individuals may contact:

Information Commissioner's Office (ICO)

<https://ico.org.uk>

Telephone: 0303 123 1113

16. Policy Review

This policy will be reviewed **annually** or when significant regulatory or operational changes occur.

Appendix – Related Policies

This policy should be read alongside:

- Information Security Policy
- Access Control Policy
- Data Retention Policy
- Incident Response / Data Breach Procedure
- Acceptable Use Policy