DELYN SAFETY UK
TRAINING & SUPPORT

Data Protection Policy
GDPR

Effective Date: 01/06/2026

Review Date: 01/06/2027

Introduction

Delyn Safety UK is committed to protecting the rights and freedoms of individuals whose personal data we process. We handle personal data relating to employees, clients, contractors and other individuals for a variety of operational and legal purposes.

This policy sets out how we protect personal data and ensure compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)**. Staff must consult the Data Protection Officer (DPO) before initiating any new or significantly changed data-processing activity.

Scope

This policy applies to all employees, directors, contractors, consultants and advisors. It supplements other organisational policies, including those relating to IT, email, security and document retention. Updated versions of this policy will be circulated, and older versions must be deleted or destroyed.

Data Protection Principles

Delyn Safety UK complies with the principles of the **UK GDPR**, which require that personal data must be:

1. Lawful, fair and transparent

Data must be processed lawfully, fairly and in a transparent manner.

2. Purpose limitation

Data must be collected for specified, explicit and legitimate purposes.

3. Data minimisation

Data must be adequate, relevant and limited to what is necessary.

4. Accuracy

Data must be accurate and kept up to date.

5. Storage limitation

Data must not be kept longer than necessary.

6. Integrity and confidentiality

Data must be processed securely to protect against unauthorised or unlawful processing, loss, destruction or damage.

Definitions

Purposes of Processing

Personal data may be used for personnel, administrative, financial, regulatory, payroll and service-delivery purposes, including:

- Compliance with legal and regulatory obligations

- Recruitment, vetting, training and operational management
- Investigating complaints and responding to enquiries
- Monitoring conduct, performance and attendance
- Ensuring safe working practices and system access control

Personal Data

Personal data refers to any information relating to an identifiable individual. Examples include:

- Contact details
- Employment and education history
- Financial and payroll information
- Nationality, marital status, qualifications and CV data

Special Category Data

Special category data includes information relating to:

- Race or ethnicity
- Political opinions
- Religion or beliefs
- Trade union membership
- Health
- Genetic or biometric data

This data requires additional protection and must only be processed under strict legal conditions.

Data Controller

A data controller determines the purposes and means of processing personal data. Delyn Safety UK is a data controller.

Data Processor

A data processor acts on behalf of a controller and processes data under their instructions.

Processing

Processing includes any operation performed on personal data, such as collection, storage, retrieval, use, disclosure, erasure or destruction.

Supervisory Authority

The UK supervisory authority is the **Information Commissioner's Office (ICO)**.

Direction and Process (UK GDPR 2026)

Fair and Lawful Processing

We must not process personal data unless a lawful basis applies. If no lawful basis exists, processing is unlawful and must cease.

Lawful Bases for Processing

At least one of the following must apply:

1. **Consent** – clear, explicit consent for a specific purpose
2. **Contract** – necessary for a contract or pre-contract steps
3. **Legal obligation** – required by law
4. **Vital interests** – necessary to protect life
5. **Legitimate interests** – necessary for our legitimate interests unless overridden by individual rights

Staff must document the lawful basis and ensure it aligns with what the data subject would reasonably expect.

Special Category Data

Processing special category data requires both:

- A lawful basis under Article 6 UK GDPR, and
- A specific condition under Article 9 UK GDPR (e.g., explicit consent, employment law obligations, vital interests, legal claims)

If no valid condition applies, processing must stop.

Responsibilities

Organisational Responsibilities

- Maintain a data inventory
- Ensure procedures uphold individual rights

- Identify lawful bases for processing
- Maintain secure storage and processing
- Detect, report and investigate data breaches

Staff Responsibilities

- Understand data protection obligations
- Follow this policy at all times
- Report breaches immediately
- Avoid unlawful or careless handling of data

Data Protection Officer Responsibilities

- Provide guidance and training
- Review policies and procedures
- Conduct internal audits
- Support DPIAs
- Investigate and report breaches

IT Security Responsibilities

- Maintain secure systems and software
- Monitor security tools
- Approve cloud services
- Ensure encryption and secure storage

Accuracy and Relevance

Personal data must be accurate and relevant. Individuals may request corrections, and disputed accuracy must be recorded and reported to the DPO.

Data Security and Storage

Data must be stored securely:

- Printed data must be locked away
- Printed data must be shredded when no longer needed
- Computers must use strong, regularly changed passwords

- Portable media must be encrypted
- Cloud storage must be DPO-approved
- Servers must be secured and protected
- Data must be backed up regularly
- Personal data must not be stored on mobile devices unless encrypted and approved

Data Retention

Data must not be kept longer than necessary and must follow the organisation's retention schedule.

International Transfers

Personal data must not be transferred outside the UK without DPO approval and appropriate safeguards (e.g., adequacy regulations, IDTA, UK Addendum).

Individual Rights Under UK GDPR

Individuals have the following rights:

1. **Right to be informed**
2. **Right of access**
3. **Right to rectification**
4. **Right to erasure**
5. **Right to restrict processing**
6. **Right to data portability**
7. **Right to object**
8. **Rights relating to automated decision-making and profiling**

We must respond within one month unless an extension is approved by the DPO.

Privacy Notices

Privacy notices must be clear, accessible and provided:

- At the time of data collection (if collected directly)
- Within one month (if collected indirectly)
- Before first communication or disclosure

They must include:

- Controller and DPO contact details
- Purpose and lawful basis
- Recipients
- Retention periods
- Rights of the individual
- ICO complaint rights
- International transfer details
- Automated decision-making information

Subject Access Requests (SARs)

SARs must be fulfilled:

- Free of charge
- Within one month
- In a commonly used electronic format

Data must not be altered after a SAR is received.

Right to Erasure

We must erase data when:

- It is no longer necessary
- Consent is withdrawn
- The individual objects and no overriding interest exists
- Processing is unlawful
- Required by law

Third Parties and Contracts

Contracts with processors must include:

- Confidentiality obligations
- Security requirements
- Sub-processor controls
- Assistance with data subject rights
- Breach notification duties
- Deletion or return of data at contract end

- Audit rights

Criminal Offence Data

Criminal offence data must only be processed where legally justified and must be treated as special category data.

Audits, Monitoring and Training

Regular audits must be conducted. Staff must complete mandatory data protection training and request updated training when roles change.

Reporting Breaches

Breaches must be reported immediately. We must notify the ICO within **72 hours** where required.

Failure to report a breach may result in disciplinary action.

Signature: 

Name: Mike Joy

Date: 01/06/2026

Position: Managing Director