

Data Protection Policy

Company Name	TPO Projects Ltd
Effective Date	May 5th 2025
Review Date	May 4th 2026
Legislation	UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018)

1. Introduction and Scope

TPO Projects Ltd is committed to protecting the privacy and security of personal data, and maintaining the confidentiality of the data entrusted to us by our employees, clients, contractors, and suppliers.

This policy applies to all employees, directors, sub-contractors, and third parties acting on our behalf (Data Processors). It covers all personal data we process, regardless of where that data is held or how it is collected.

2. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person (Data Subject). This includes names, ID numbers, location data, and IP addresses.
- **Special Category Data:** Sensitive data requiring extra protection, such as health records, religious beliefs, race, political opinions, and biometric data.
- **Processing:** Any operation performed on personal data, such as collection, recording, storage, retrieval, use, disclosure, or destruction.
- **ICO:** The Information Commissioner’s Office, the UK supervisory authority for data protection.

3. The Seven Key Principles of UK GDPR

TPO Projects Ltd commits to adhering to the following seven principles when handling personal data:

Principle	Meaning and TPO Projects Action
1. Lawfulness, Fairness & Transparency	Data is processed lawfully, fairly, and transparently in relation to the Data Subject. <i>Action: We provide clear Privacy Notices to employees and clients.</i>

2. Purpose Limitation	Data is collected only for specified, explicit, and legitimate purposes. <i>Action: We only collect data required for contractual, legal, or legitimate operational needs.</i>
3. Data Minimisation	Data collected must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. <i>Action: We review data collection forms regularly to ensure relevance.</i>
4. Accuracy	Personal data must be accurate and, where necessary, kept up to date. <i>Action: Employees are responsible for notifying HR of changes to personal details.</i>
5. Storage Limitation	Data is kept in a form which permits identification of Data Subjects for no longer than is necessary. <i>Action: We have a defined Retention Schedule based on legal requirements (e.g., 6 years for financial records).</i>
6. Integrity & Confidentiality	Data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. <i>Action: We use strong passwords, encryption, and physical security measures.</i>
7. Accountability	The Data Controller (TPO Projects) is responsible for, and must be able to demonstrate, compliance with the other six principles. <i>Action: We maintain records of all processing activities and implement internal data protection audits.</i>

4. Rights of the Data Subject

We recognize and respect the following rights of individuals concerning their data:

1. **Right to be Informed:** The right to be provided with clear, transparent, and easily understandable information about how we use their data (via Privacy Notices).
2. **Right of Access (Subject Access Request - SAR):** The right to obtain a copy of the personal data we hold about them. TPO Projects will respond to SARs within one month.
3. **Right to Rectification:** The right to have inaccurate personal data corrected or completed if it is incomplete.
4. **Right to Erasure ('Right to be Forgotten'):** The right to have data deleted in specific circumstances (e.g., when the data is no longer necessary for the purpose for which it was collected).
5. **Right to Restrict Processing:** The right to block or suppress further use of their data in certain situations.
6. **Right to Data Portability:** The right to obtain and reuse their personal data for their own purposes across different services.
7. **Right to Object:** The right to object to processing based on legitimate interests or direct marketing.
8. **Rights in Relation to Automated Decision Making and Profiling.**

5. Security Measures and Breach Reporting

5.1 Technical and Organisational Measures

- **Access Control:** Access to digital and physical data (e.g., personnel files) is strictly limited to those employees who require it for their duties.
- **IT Security:** All company devices (laptops, phones) used for processing personal data must be password-protected and automatically locked when unattended.
- **Data Transfer:** Personal data should not be transferred out of the UK or EEA unless explicit measures (e.g., standard contractual clauses) are in place to ensure compliance with UK GDPR standards.

5.2 Data Breach Procedure

In the event of a suspected or actual personal data breach (e.g., lost laptop, unauthorized access, ransomware attack):

1. **Immediate Action:** The employee or contractor must immediately inform the **Data Protection Lead (DPL)**, detailing what data was involved, where the breach occurred, and the volume of data affected.
2. **Assessment:** The DPL will immediately assess the risk to individuals' rights and freedoms.
3. **Reporting to ICO:** If the breach is likely to result in a risk, the DPL must report the breach to the ICO **within 72 hours** of becoming aware of it.
4. **Notification to Data Subjects:** If the breach is likely to result in a **high risk** to individuals' rights and freedoms, the Data Subjects must be informed without undue delay.

6. Training and Accountability

- **Induction:** All new employees and sub-contractors must receive mandatory training on data protection principles during their induction.
- **Responsibility:** The **Health & Safety/Compliance Director** acts as the designated **Data Protection Lead (DPL)** for TPO Projects and is responsible for overseeing compliance with this policy.

TPO Projects Ltd may amend this policy from time to time to remain compliant with UK law. All changes will be communicated to staff.

Signed by T. Oram



Position Managing Director