Reference	TIS-DPP-01
Version	2.0
Issue Date	10/02/2021
Review Date	10/03/2026
Approved	MD

DATA PROTECTION POLICY

Document Ref:	TIS-DPP-01	**Version:**	2.0
Issue Date:	10/02/2021	**Review Date:**	10/03/2026
Approved By:	Managing Director		

1. PURPOSE

The purpose of this policy is to ensure that **Total Integrated Services Ltd** (the "Company") fully meets its legal obligations under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. This document completely supersedes all previous policy drafts established under outdated data protection regimes.

As a professional security services provider, the Company routinely processes personal data relating to its workforce (including security guards, mobile patrols, and temporary staff), clients, corporate suppliers, and members of the public (via operational documentation, access control logs, and surveillance systems). This policy outlines the mandatory duties of all personnel to protect that data and guarantee corporate compliance.

2. THE DATA PROTECTION PRINCIPLES

The Company is strictly committed to processing personal data in accordance with the six core principles mandated by the UK GDPR. Personal data must be:

1. **Lawful, Fair, and Transparent:** Processed legally, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation:** Collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.
3. **Data Minimization:** Adequate, relevant, and limited to what is necessary for the stated operational purposes.
4. **Accuracy:** Accurate and, where necessary, kept strictly up to date.
5. **Storage Limitation:** Kept in a form which permits identification of data subjects for no longer than is necessary for the authorized purposes.
6. **Integrity and Confidentiality (Security):** Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

> **The Accountability Overarching Principle:** The Company holds statutory responsibility for, and must be able to actively demonstrate compliance with, all six core principles listed above to regulatory bodies.

3. RESPONSIBILITY & DATA CONTROLLER

- **The Data Controller:** Total Integrated Services Ltd as a corporate entity is the legal Data Controller regarding all personal data processed under this policy framework.
- **Ultimate Responsibility:** The Managing Director holds ultimate executive accountability for ensuring that systemic data protection compliance is consistently applied within the business operations.
- **Day-to-Day Administration:** The designated Management Representative is directly responsible for the ongoing maintenance, regular internal auditing, risk monitoring, and operational updates of this policy document.

4. LAWFUL BASIS FOR PROCESSING & VETTING

The Company does not rely on generic or blanket employee "consent" to process standard workplace files or execute mandatory security background screenings. Instead, processing is justified under the following strict statutory bases:

- **Performance of a Contract:** Necessary to administer employment contracts, manage human resources infrastructure, execute corporate payroll, and deliver contracted security operations directly to clients.
- **Legal Obligation:** Necessary to comply with UK statutory regulations, employment legislation, tax requirements, and mandatory security industry vetting standards (such as **BS 7858** secure screening for security personnel).
- **Legitimate Interests:** Necessary to secure client premises, safeguard company property, protect corporate infrastructure, and ensure overall workplace safety.

4.1. Special Category & Criminal Offense Data

When vetting prospective staff for criminal convictions (in accordance with the Rehabilitation of Offenders Act 1974 and Security Industry Authority rules), the Company processes this information under **Schedule 1 of the Data Protection Act 2018**. Vetting is performed strictly to fulfill legal industry obligations and to verify that deployed personnel do not pose a security threat to clients, property, or vulnerable groups.

5. STAFF AND SECURITY PERSONNEL RESPONSIBILITIES

Adherence to this Data Protection Policy is a strict condition of employment. Any failure to follow these mandated rules will result in immediate internal investigation and formal disciplinary proceedings up to and including termination for gross misconduct.

5.1. General Data Duties

All personnel—including permanent corporate employees, operational coordinators, site managers, and temporary or frontline security guards—are responsible for:

- Ensuring that any personal information they provide to the Company regarding their own employment profile (e.g., address, bank details, emergency contacts, SIA licenses) is accurate and updated immediately.
- Keeping all client logs, incident reports, patrol records, assignment instructions, and gatehouse visitor sheets entirely confidential.
- Ensuring personal data is never disclosed either orally, in writing, or accidentally to any unauthorized third party.

5.2. Physical and Digital Security Controls

- **Physical Records:** All hard-copy files, visitor registers, key logs, and incident notebooks must be kept securely in locked filing cabinets, secure guardrooms, or locked drawers when not in active use.
- **Digital Records:** Any computerised data, patrol management software, or digital logs must be strictly password-protected and accessible only via authorized user accounts.
- **Off-Site Processing:** Employees processing data off-site or at remote client assignments must take strict precautions to prevent unauthorized exposure. The use of unsecured personal home computers or unencrypted external media to store company or client personal data is strictly prohibited.

6. SURVEILLANCE: CCTV AND BODY-WORN VIDEO (BWV)

As a provider of security services, the Company frequently operates surveillance equipment. All imagery and audio captured via Closed-Circuit Television (CCTV) or Body-Worn Video (BWV) is legally classified as personal data.

- Surveillance systems must only be deployed for legitimate security, crime prevention, and safety purposes on authorized sites.
- Clear signage must be prominently displayed across monitored sites to notify the public that recording is actively in progress.

- Footage must be stored securely, accessed only by designated, authorized security personnel, and automatically overwritten or deleted after a set retention period (typically 30 days) unless explicitly preserved as evidence for an active police or internal incident investigation.

7. DATA SUBJECT RIGHTS

Under UK law, data subjects (including employees, clients, contractors, and individuals captured on Company surveillance systems) possess clear legal rights. They have the right to request:

- **Access:** Access to their personal data via a formal Subject Access Request (SAR). The Company must fulfill valid SARs **free of charge** and within **one calendar month** of receipt.
- **Rectification:** The immediate correction of inaccurate or incomplete personal details. The Company reserves the right to request official documentary evidence before updating critical compliance parameters.
- **Erasure:** The deletion of their personal records ("the right to be forgotten"), provided the data is no longer required under explicit statutory retention periods (e.g., HMRC tax records or mandatory BS 7858 screening histories).
- **Restriction/Objection:** The restriction of or objection to specific processing models, including data used for direct marketing purposes.

8. DATA BREACH MANAGEMENT & ICO NOTIFICATION

A personal data breach involves any security incident leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of personal data held by the firm.

- **Immediate Internal Reporting:** Any employee who discovers, suspects, or causes a data breach (such as a lost work laptop, a stolen smartphone, a misplaced site logbook, or a leaked roster) must notify the Management Representative **immediately**.
- **72-Hour Regulatory Window:** If an assessment shows that the data breach presents a risk to the rights and freedoms of the affected individuals, the Company is legally obligated to report the incident to the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach.

9. INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data outside the United Kingdom to third countries unless that country ensures an adequate level of data protection approved by the UK government, or appropriate statutory safeguards (such as approved International Data Transfer Agreements) are securely executed.

10. RETENTION AND SECURE DISPOSAL

Personal data will not be retained for longer than is operationally or legally necessary. Vetting records, client contracts, incident logs, and financial records will be securely archived in strict alignment with UK statutory limitation periods and industry-specific security screening standards.

- **Physical Destruction:** Confirmed end-of-life physical documentation must be completely destroyed via secure cross-cut shredding.
- **Digital Destruction:** Prior to the sale, recycling, or scrapping of any corporate IT equipment, mobile devices, or storage media, all digital personal data must be completely and permanently destroyed using certified formatting, overwriting, or degaussing methodologies.

Approved by: Muhammad Khalid

Signature: 

Date: March 10th, 2026