Scope

Applies to all Triton Inspections operations in the UK, Norway and Europe, including offshore and client-site activities. Covers all personal data processed by Triton Group entities and by third parties acting on our behalf.

Purpose

Set a clear framework to:

- Comply with UK DPA 2018, UK GDPR, EU GDPR, and the Norwegian Personal Data Act.
- Safeguard data subject rights.
- Define how personal data is collected, used, stored, shared, retained, and disposed.

Our Commitments

We commit to fulfil applicable data protection obligations and to continually improve our controls within the Integrated Management System. We will:

- Process data lawfully, fairly, and transparently.
- Limit processing to specified, explicit, and legitimate purposes.
- Minimise data to what is necessary.
- Keep data accurate and up to date.
- Limit storage to what is necessary.
- Protect data with appropriate technical and organisational measures.
- Demonstrate accountability through records, audits, and reviews.

Legal Bases & Jurisdictions

Processing is grounded in recognised lawful bases: consent, contract, legal obligation, vital interests, public task (where applicable), and legitimate interests balanced against data subject rights. We follow guidance from the UK ICO and Datatilsynet. Poland will be added when operations commence. International transfers use approved safeguards where required.

Data Subject Rights

We uphold: right to be informed, access, rectification, erasure, restriction, portability, objection, and rights related to automated decision-making and profiling. Requests are logged, verified, and answered within statutory timescales. Outcomes are recorded in the IMS.

Data Security

We maintain layered controls proportionate to risk:

- Role-based access and MFA.
- Encryption at rest and in transit; pseudonymisation/anonymisation where appropriate.
- Secure configuration, patching, backups, and monitoring.
- Supplier hardening and contractual security clauses.
- Staff training and least-privilege access.
  Security risks and controls are tracked in the Risk Register and reviewed in Management Review.

Verification of Client and Platform Systems

Where client systems govern storage, permits to access personal data, incident response, or disposal, Triton relies on those controls after verifying adequacy via contract review, DPIA (where required), the Client Site/Platform Checklist, and periodic attestations. Duplicate registers are avoided where client controls are demonstrably effective.

Data Breach Management

We maintain detection, escalation, assessment, notification, and learning processes.

- Assess risk to rights and freedoms.
- Notify the relevant authority within 72 hours where required and inform affected individuals without undue delay when risk is high.
- Log all incidents, root causes, decisions, and corrective actions in the NCR Register; track to closure.

Data Retention

Retain personal data only as long as necessary for the stated purpose or as required by law or contract. Apply Triton's Data Retention Schedule. On expiry, securely delete or anonymise. Evidence of disposal is retained.

Third-Party Processors

Before engagement we:

- Perform due diligence proportionate to risk.
- Execute GDPR-compliant Data Processing Agreements with clear instructions, confidentiality, security, sub-processor control, and audit rights.
- Require breach notification and cooperation.
- Maintain an up-to-date processor inventory in the Legal Register.

Worker Awareness & Participation

- Mandatory induction and periodic refresher training for all who access personal data.
- Quarterly HSE & Compliance Attestations include data protection confirmations.
- Worker Representative channel and SHE Report used for raising concerns and improvement ideas. Inputs feed Management Review.

Objectives & Improvement

Current IMS objectives:

- ≥95% completion of mandatory data protection training and quarterly attestations.
- ≥95% SARs answered within legal timescales with zero justified complaints upheld.
- Annual breach-response drill and DPIA spot-checks for new or changed processing. Performance is monitored on the IMS dashboard and through audits and NCR trends.

Strategic Direction & Review

This policy supports Triton's strategic aim to operate securely, lawfully, and efficiently. It provides the framework for setting and reviewing privacy objectives in accordance with ISO 9001, ISO 14001, and ISO 45001 integration. Reviewed at least annually or on material change, communicated to all personnel, available on Triton Nexus, and accessible via Triton Group's website.