Data Protection Policy & Privacy Notice

Issue No: 07
Date Issued: JUL15
Approved by: CEO
Author: COMPLIANCE
Owner (Dept): COMPLIANCE
Date Reviewed: JUN26
End User: MAST STAFF

1. Statement on Data Protection

Maritime Asset Security & Training (MAST) Ltd is committed to protecting the rights and freedoms of individuals and ensuring that personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

MAST acts as a Data Controller and, where applicable, a Data Processor, and is committed to ensuring that all personal data is handled lawfully, securely and transparently.

This document also serves as the organisation's Privacy Notice, explaining how personal data is collected, used, stored and protected.

---

2. Scope

This policy applies to:

- All employees and contractors
- All personal data processed by MAST
- All systems, devices and processes used to handle data

---

3. Data Protection Principles

MAST complies with the UK GDPR principles. Personal data shall be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Processed securely using appropriate technical and organisational measures

---

4. Lawful Basis for Processing

MAST processes personal data under one or more of the following lawful bases:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Legitimate interests

Special category data is processed only where additional conditions under UK GDPR are met.

---

5. Privacy Notice – How We Use Personal Data

MAST collects and processes personal data relating to:

- Employees and contractors
- Clients and their personnel
- Suppliers and partners

Purpose of Processing

Personal data is used for:

- Employment and HR management
- Delivery of security services
- Compliance with legal and regulatory obligations
- Business administration and communication

Your Rights

Individuals have the right to:

- Access their personal data
- Request rectification or erasure
- Restrict or object to processing
- Data portability
- Lodge a complaint with the Information Commissioner's Office (ICO)

---

6. Data Protection Governance

6.1 Data Protection Officer (DPO)

MAST has appointed a Data Protection Officer responsible for:

- Monitoring compliance
- Providing advice and guidance
- Delivering staff training
- Acting as a contact point with the ICO

Contact: phillip.cable@mast-security.com

6.2 GDPR Compliance Programme

MAST maintains a structured programme to ensure compliance, including:

- Data Protection Impact Assessments (DPIAs)
- Records of processing activities
- Internal audits and reviews
- Privacy by design and default
- Data breach procedures

---

7. Staff Responsibilities

All staff must:

- Comply with this policy and UK GDPR requirements
- Handle personal and sensitive data securely
- Only access data where authorised
- Report data breaches immediately

Failure to comply may result in disciplinary action.

---

8. Data Security and IT Controls

MAST implements robust technical and organisational security measures, including:

8.1 Technical Controls

- Firewalls protecting internal systems
- Up-to-date antivirus and endpoint protection software
- Password-protected devices and systems

- Secure user authentication and access controls
- Regular system updates and security patching
- Remote device locking and data wiping capability

8.2 Operational Controls

- Role-based access to systems
- Secure backups (including off-site storage)
- Secure data transfer protocols
- Monitoring and review of system access

8.3 Physical Security

- Paper records stored in locked cabinets
- Restricted access to sensitive areas
- Visitors supervised at all times
- Locally hosted servers stored in secure environments with controlled access

---

9. Data Storage and Location

Personal data is stored securely using:

- Secure network drives
- Approved databases and IT systems
- Microsoft Office applications
- Controlled access portals

Data is stored and processed within:

- The United Kingdom and/or European Economic Area (EEA), or

- Other jurisdictions with adequate data protection safeguards

Where international transfers occur, appropriate legal safeguards (e.g. Standard Contractual Clauses) are implemented.

---

10. Data Retention

Personal data is retained only for as long as necessary to fulfil its purpose or meet legal obligations. Retention periods are defined and reviewed regularly.

---

11. Data Breaches

A personal data breach is any incident leading to:

- Loss, destruction, or alteration of data
- Unauthorised disclosure or access

MAST will:

- Investigate all breaches
- Notify the ICO within 72 hours where required
- Inform affected individuals where there is a high risk

---

12. Data Protection Training

All staff receive data protection training:

- At induction

- On a regular basis (minimum annually)

Training covers:

- GDPR principles
- Handling sensitive data
- Cyber security awareness
- Data breach identification and reporting

Training records are maintained by the HR Department.

---

13. Confidentiality and Contracts

All employees are bound by confidentiality obligations.

Confidentiality clauses are included as standard within:

- Employment contracts
- Client agreements
- Supplier contracts

---

14. Conflict of Interest and Data Segregation

MAST ensures that:

- Client data is kept separate and secure
- Access is restricted to authorised personnel only
- Procedures are in place to prevent conflicts of interest

---

15. Sharing Personal Data

Personal data is only shared:

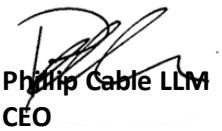
- Where necessary for business purposes
- With authorised third parties
- Under appropriate contractual and security controls

---

16. Further Information

For any queries regarding this policy or your data, contact the HR Department.
Individuals also have the right to contact the Information Commissioner's Office (ICO).

Signed



Phillip Cable LLM
CEO