Data Protection Statement

Issue No: 02
Date Issued: MAY18
Approved by: CEO
Author: COMPLIANCE
Owner (Dept): COMPLIANCE
Date Reviewed: NOV26
End User: PUBLIC STATEMENT

1. MAST Statement on Data Protection

Maritime Asset Security and Training (MAST) Ltd is the Data Controller and is committed to protecting the rights of individuals in line with the new GENERAL DATA PROTECTION LAWS (Data Protection Bill 2018 and the General Data Protection Regulation).

Maritime Asset Security & Training (MAST) Ltd is committed to keeping your personal data, and any other personal data collected, used or stored by us as secure and private as possible.

Consequently, MAST makes all MAST aware of the purposes for which Maritime Asset Security & Training (MAST) Ltd will process any personal information and the obligations that both Maritime Asset Security & Training (MAST) Ltd are under when processing personal data.

This policy complies with the requirements set out in GENERAL DATA PROTECTION LAWS and DPB, which come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the GENERAL DATA PROTECTION LAWS.

2. Applicable Legislation

- Data Protection Bill 2018 and General Data Protection Regulation (GENERAL DATA PROTECTION LAWS)

This statement will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection

Regulation 12 steps to take now'

3. Detail

3.1 Applicable data

GENERAL DATA PROTECTION LAWS define **personal data** as the following:
'Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'
Personal data can include: name, job title, date of birth, passport data, home address, home telephone number, private email address, emergency contact, staff number, bank account number, NI number etc.

'**Special categories**' *of personal data (sensitive personal data) relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Special category data can include: racial and ethnic origin, health records, criminal record check etc.*

ALL MAST staff MUST comply with data protection regulations and this policy when processing any personal data on behalf of the Maritime Asset Security & Training (MAST) Ltd.

3.2 Principles

In accordance with the requirements outlined in the GENERAL DATA PROTECTION LAWS, personal data will be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.
b) Collected for specified, explicit and legitimate purposes and processed in a manner that is compatible with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they

are processed.

d) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Kept no longer than is necessary for the purposes for which the personal data are processed;

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.3 MAST as controller / processor

MAST has data controller responsibilities for its personnel records, those of its clients and suppliers. MAST will occasionally fulfill data processor role.

3.4 Accountability

MAST implements appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in GENERAL DATA PROTECTION LAWS.
MAST provides comprehensive, clear and transparent privacy notices to its employees, workers, consultants, contractors and Clients.
Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
Data protection impact (DPI) assessments are used, where appropriate.

3.5 Data protection officer (DPO)

MAST has an appointed DPO who will:

- Inform and advise MAST and its staff about their obligations to comply with the GENERAL DATA PROTECTION LAWS and other data protection laws.
- Monitor the MAST's compliance with the GENERAL DATA PROTECTION LAWS, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

Maritime Asset Security and Training (MAST) Ltd has a Data Protection Officer who can be contacted through phillip.cable@mast-security.com

The individual appointed as DPO will have professional experience and knowledge of data protection law. The DPO will operate independently and will not be dismissed or penalised for performing their task.

3.6 Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under GENERAL DATA PROTECTION LAWS, data will be lawfully processed under the following conditions:

a) The consent of the data subject has been obtained.
b) Processing is necessary for:
- Compliance with a legal obligation.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party,

Special category data will only be processed under the following conditions:

a) Explicit consent of the data subject,
b) Processing relates to personal data manifestly made public by the data subject.
c) Processing is necessary for:
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the staff.

4. <u>What are an individual's rights?</u>

Individuals have the following rights pertaining to their personal data that MAST processes:

1) to be informed – that means an individual has the right to be informed about the collection and use of their personal data
2) rights to access and port data - that means an individual has the right to access their personal data and supplementary information.
3) to rectify - that means an individual is entitled to have personal data rectified if it is inaccurate or incomplete.
4) to erase - is also known as 'the right to be forgotten' . That means right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5) to restrict individual's data – that means an individual has a right to 'block' or suppress processing of personal data.
6) to object to processing.
7) to withdraw consent if processing is based on consent.

5. Privacy by design and privacy impact assessments

Where applicable to MAST services, MAST will act in accordance with the Data Protection Laws by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how MAST has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the MAST's data protection obligations and meeting individuals' expectations of privacy.

6. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
MAST will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be

informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of MAST becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, MAST will notify those concerned directly.

Effective and robust breach detection, investigation and internal reporting procedures are in place at MAST.