Data Protection Policy

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 Data Protection Bill (DPB) 2018 and the new General Data Protection Regulation (GENERAL DATA PROTECTION LAWS).

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

This policy complies with the requirements set out in the 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)
- Data Protection Act 1998

This policy 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

The 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.

Data Protection Policy

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 employees' and 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 the GENERAL DATA PROTECTION LAWS.
MAST provides comprehensive, clear and transparent privacy notices to its employees, workers, consultants and contractors.
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 the 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.

3.7 Consent

MAST ensures that consent mechanisms meet the standards of the GENERAL DATA PROTECTION LAWS. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent can be withdrawn by the individual at any time.

3.8 The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

3.9 The right of access

Individuals have the right to obtain confirmation that their data is being processed.
MAST will verify the identity of the person making the request before any information is supplied.
A copy of the information will be supplied to the individual free of charge; however, MAST may impose a 'reasonable fee' to comply with requests for further copies of the same information.
Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.
All requests will be responded to without delay and at the latest, within one month of receipt.
In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
Where a request is manifestly unfounded or excessive, MAST holds the right to refuse to

respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
In the event that a large quantity of information is being processed about an individual, MAST will ask the individual to specify the information the request is in relation to.

3.10 The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where appropriate, MAST will inform the individual about the third parties that the data has been disclosed to.
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
Where no action is being taken in response to a request for rectification, MAST will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

3.11 The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

MAST has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

3.12 The right to restrict processing

Individuals have the right to block or suppress the MAST's processing of personal data.
In the event that processing is restricted, MAST will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

MAST will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until MAST has verified the accuracy of the data
- Where an individual has objected to the processing and MAST is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests

restriction instead

- Where MAST no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, MAST will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
MAST will inform individuals when a restriction on processing has been lifted.

3.13 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. MAST will provide the information free of charge.
Where feasible, data will be transmitted directly to another organisation at the request of the individual.
MAST is not required to adopt or maintain processing systems which are technically compatible with other organisations.
In the event that the personal data concerns more than one individual, MAST will consider whether providing the information would prejudice the rights of any other individual.
MAST will respond to any requests for portability within one month.
Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
Where no action is being taken in response to a request, MAST will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

3.14 The right to object

MAST will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purpose of scientific or historical research and statistics.

MAST will stop processing the individual's personal data unless the processing is for the establishment, exercise or defense of legal claims, or, where MAST can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for **direct marketing purposes**:

- MAST will stop processing personal data for direct marketing purposes as soon as an objection is received.
- MAST cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where the processing activity is outlined above, but is carried out online, MAST will offer a method for individuals to object online.

4. 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.

5. 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, which facilitate decision-making in relation to whether the ICO will be informed.
Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

Data Protection Policy

6. Staff's Obligations When Processing Personal Data - Data security

All MAST staff must comply with all security measures introduced by Maritime Asset Security & Training (MAST) Ltd to protect personal data processed by the Company. In particular, all staff are responsible for ensuring that the procedures below are followed:

a) Confidential paper records will be kept in a locked filing cabinet or drawer, with restricted access.
b) Confidential paper records will not be left unattended or in clear view anywhere with general access.
c) Digital data is coded and/or password-protected, in all locations that it is stored on: on a local hard drive, on a network drive, and within various web based data base applications. The data is regularly backed up off-site.
d) Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
e) Memory sticks will not be used to hold personal information unless they are password-protected.
f) All electronic devices are password-protected to protect the information on the device in case of theft.
g) Where possible, MAST enables electronic devices to allow the remote blocking or deletion of data in case of theft.
h) Staff will not use their personal laptops or computers for MAST purposes, unless with the prior approval of the CEO.
i) All necessary members of staff are provided with their own secure login and password.
j) Circular emails to MSO and SO are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
k) Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from MAST premises accepts full responsibility for the security of the data.
l) Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
m) Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of MAST containing sensitive information are supervised at all times.
n) MAST will not publish any personal information, including photos, on its website or company social media without the permission of the affected individual.
o) When uploading information to MAST website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

7. Confidentiality

All MAST staff should be aware that the obligations placed on you by this policy are in addition to the duty of confidentiality which you owe to Maritime Asset Security & Training (MAST) Ltd in respect of all information (including personal data) processed by the Maritime Asset Security & Training (MAST) Ltd about its clients, employees, suppliers and any other persons. You must keep all such information confidential and not disclose it unless authorised to do so.

8. Further Assistance

If you have any questions about this Policy or are in any doubt about a particular situation you should check with the Compliance Department.