MNG Maritime

Data Protection Policy (DPP)

Version 1.0

October 2018

Foreword

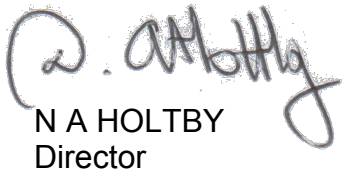
MNG Maritime's Data Protection Policy (DPP) has been drawn up to conform with the EU's *General Data Protection Regulation* (GDPR), enforceable on 25 May 18 in the UK under the *Data Protection Act 2018* (DPA18).

Any questions regarding the document should be addressed to:

MNG Maritime Ltd
Chester House
81-83 Fulham High Street
LONDON
SW6 3JA

info@mngmaritime.com

M N GRAY MBE
Director
MNG Maritime Ltd



N A HOLTBY
Director
MNG Maritime Ltd

Drafted: 26 October 2018
Last Reviewed: 26 October 2018

Definitions

"(Data) Controller" has the meaning ascribed to it in Article 32 of DPA18

"(Data) Processing" shall have the meaning ascribed to it in DPA18.

"(Data) Processor" has the meaning ascribed to it in Article 32 of DPA18.

"(Data) Subject" shall have the meaning ascribed to it in DPA18.

"**DPA18**" means the UK primary legislation the *Data Protection Act 2018*, as subsequently amended, which repealed the *Data Protection Act 1998*.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such date (General Date Protection Regulation).

"Personal Data" shall have the meaning ascribed to it in DPA18.

"Processing" means any function that is applied on personal data, whether automated or not, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure through transmission, dissemination, alignment, combination restriction, erasure or destruction.

"Register of Systems": means a register of all systems or contexts in which personal data is processed by the Company.

"Responsible Person" means the person within the Company responsible for data protection.

"Sensitive Processing" shall have the meaning ascribed to it under Article 35 of DPA18.

"**Technical and Organisational Security Measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

"**The Company"** means MNG Maritime Ltd., its holding Company, Hill College Holdings Ltd., and any sister companies and subsidiary companies of either that might exist.

Principles

1. The Company will comply with the *Data Protection Act 2018*, which replaces the *Data Protection Act 1998* from 25 May 2018. In order to carry out the services of this engagement and for related purposes such as updating and enhancing the Company's client records, analysis for management purposes and statutory returns, legal and regulatory compliance and crime prevention the Company may obtain, process, use and disclose personal data about client PMSC personnel.

2. The United Kingdom is scheduled to leave the European Union on 31 March 2019. DPA18 will continue in force beyond that date, although it is unclear, legally, how clauses relating to the sharing of data outside the EU and EEA will then be applied. Until/unless any policy guidance is given to the contrary and this policy is duly amended, it is assumed that the protections afforded to companies and individuals within the EU/EEA under GDPR an reflected in this policy will remain extant.

3. The Company is committed to ensuring that personal data be:

   (a) processed lawfully, fairly and in a transparent manner in relation to individuals;

   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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 in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

   (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.

Scope of Policy

4. This policy/privacy notice applies to anyone who interacts with, or is employed/contracted by the Company in any way. This may also include the personal data of employees of the Company's client PMSCs or agencies who have contracted one of the Company's services, or have enquired about doing so.

5. This policy applies to individuals if they ask the Company about, contract or use any of the services, or if they work as a contractor or MSO for a PMSC that contracts, uses or enquires about the Company's services. It also applies to individuals if they seek employment with the Company, or if they send the Company personal information in unsolicited employment applications. It describes how the Company handles their information, regardless of the way the information was acquired (for example, by email, through the website, by phone, personally etc.).

Lawful Bases for Collecting Information

6. The Company processes an individual's personal information for a number of lawful reasons, including managing all aspects of the Company's relationship with the individual, to help the Company improve its services and products, to meet its own legal obligations (for example, with regard to licensing) and in order to exercise its rights or handle claims. By law, the Company must have a lawful reason for processing personal information. The Company processes standard personal information about individuals if this is:

(a) necessary to provide the services set out in a contract − if the Company has a contract (e.g. FLARMCON) with an individual, or the employer/contracting entity (e.g. PMSC or manning agency) of an individual, the Company will process that personal information in order to fulfil that contract (that is, to provide the PMSC and therefore the individual with services);

(b) in the Company's or a third party's legitimate interests − details of those legitimate interests are set out in more detail below;

(c) required or allowed by law.

(d) to manage the Company's relationship with PMSCs, its business and third parties who provide products or services for the Company (for example, to check that the PMSC has received a service that it has requested and paid for, to validate invoices and so on)

(e) to investigate complaints;

(f) to keep the Company's records up to date and to provide PMSCs with marketing as allowed by law;

(g) to develop and carry out marketing activities and to show PMSCs information that is of interest to them, based on the Company's understanding of their preferences (the Company may combine information the PMSC gives

us with information the Company receives about the PMSC from third parties to help understand the PMSC better);

(h) for statistical research and analysis so that the Company can monitor and improve products and services, or develop new ones;

(i) to contact PMSCs about market research the Company is carrying out;

(j) to enforce or apply the Company's website terms of use, the Company's FLARMCON terms and conditions or other contracts, or to protect the Company's (or PMSCs' or other people's) rights, property or safety;

(k) to exercise the Company's rights, to defend it from claims and to keep to laws and regulations that apply to us and the third parties the Company works with; and

(l) to take part in, or be the subject of, any sale, purchase, merger or takeover of all or part of the Company's business.

7. The Company processes special category information about individuals because:

(a) it is mandated by STCW regulations that the Company verifies that all seafarers, including maritime security personnel are physically fit to be employed at sea;

(b) it is mandated by the Company's ISO certification that it verifies whether individuals are mentally fit to be employed in armed security roles by the Company;

(c) it is mandated by the Company's ISO certification that it verifies that its employees who handle firearms do not have any disbarring criminal convictions;

(d) it is necessary for an insurance purpose (for example, arranging, providing or managing an insurance contract, dealing with a claim made under an insurance contract, or relating to rights and responsibilities arising in connection with an insurance contract or law);

(e) it is necessary to establish, make or defend legal claims (for example, claims against the Company for insurance);

(f) it is in the public interest, in line with any laws that apply;

(g) it is information that the individual has made public; or

(h) the Company has the individual's permission. As is best practice, the Company will only ask an individual for permission to process their personal information if there is no other legal reason to process it. If the Company needs to ask for an individual's permission, it will make it clear that this is what the Company is asking for, and ask the individual to confirm their choice to give us that permission. If the Company cannot provide a product or service without

the individual's permission the Company will make this clear when it asks for the individual's permission. If the individual later withdraws their permission, the Company will no longer be able to provide them with the product or service that relies on having their permission.

How Personal Information is Collected

8. The Company normally collects personal information from PMSCs and manning agencies and from individual MSOs or job applicants. The Company collects personal information about individuals:

(a) through their own direct contact with the Company, including by phone, by email, by responding to job applications or filling in forms, or face-to-face (for example, in interviews, or directly collected by one of the Company's employees, e.g. on ship).

(b) through the contact of their employer/contracting entity (PMSC or manning agency) who books a transfer, flight or shuttle transit, or applies for a visa on their behalf, or contracts the Company for any other service the execution of which requires an individual's personal data.

9. Where PMSCs or manning agencies provide the Company with information about employees and contractors, they confirm that those employees and contractors have seen a copy of this privacy notice and that those individuals are comfortable with them giving the Company their information.

10. The Company also collects information from other people and organisations. For all of the Company's client or agency employees or contractors (including seafarers), the Company may collect information from:

(a) a person's employer or contracting entity, if they are a contractor or employee of a PMSC;

(b) a person's recruitment or employment agency, if they are an MME or other contractor to the Company;

(c) a Port agency or visa application agency, if the Company is using their services on their behalf, or if they have used their services in the past;

(d) any other sub-contracted entities who work with the Company in relation to a person's employment or work as a security contractor, even if the Company does not deliver the service it to them directly, such as providing them with hotel services, transport, taxis, flights or shuttle services;

Description of Personal Information Collected

11. The Company processes two categories of personal information about individuals and (for employees) their next of kin:

(a) standard personal information (for example, contact details, information that the Company uses to identify individuals or companies or manage the Company's relationship with them); and

(b) special categories of information (for example, mental and physical fitness, qualification information, personal documentation, photographs and criminal record information).

12. **Standard Personal Information**. Standard personal information includes:

(a) contact information, such as name, username, address, email address and phone numbers;

(b) residence, nationality, age, date of birth, place of birth and national identifiers (such as National Insurance number or passport number and respective expiry dates, as well as scans of such documents);

(c) Seamen's book details (including number, expiry date and scans of such documents);

(d) visa-specific application information (such as names and personal details of parents);

(e) employment information;

(f) details of any interaction with the Company, such as any complaints or incidents;

(g) financial details, such as details about payments and bank details;

(h) relevant qualifications (such as seafarers' certificates (STCW), security and weapons qualifications and other relevant skills and attributes);

(i) details of any services used by individuals, supplied by the Company (for example stays on the Company's vessels, use of the Company's shuttle(s), stays in hotels booked by the Company and attendance on courses run by the Company, including course results).

(j) information about how individuals use the Company's website, or other technology (including on board wifi access), including IP addresses or other device information.

13. **Special Categories**. Special category information includes:

(a) photographs of individuals (for visa applications);

(b) information about physical or mental health;

(c) information relating to drug and alcohol testing conducted by the Company on its employees, or conducted on behalf of PMSCs on their employees/contractors/sub-contractors; and

(d) the results of any criminal record checks the Company may have made, or that may have been made on the Company's behalf.

Sharing Personal Information

14. The Company shares personal information within the Company's Group, with agents arranging services on the PMSC's or individual's behalf and with people acting on the Company's behalf (for example, brokers, port and shipping agents, sub-contractors and other companies). The Company also shares PMSC's and individuals' information in line with the law (for example, to meet conditions of licensing, statutory or regulatory requirements or approvals). The Company sometimes needs to share PMSCs' and individuals' information with other people or organisations for the purposes set out in this privacy notice. For all the Company's PMSC clients, including their individual personnel, and the Company's own personnel, including MME, the Company shares personal information with:

(a) other members of the Company's Group;

(b) the Company's PMSC clients or employment agencies, where the individual has a relationship with that client (as an employee, contractor or sub-contractor) and that client has a legitimate right to the information (e.g. behaviour information, drug and alcohol test results, training results, performance evaluations etc.);

(c) insurance agents or brokers in the course of implementing a policy or presenting a claim;

(d) suppliers who help deliver products or services on the Company's behalf;

(e) other third parties with whom the Company works in order to provide its products and services, such as agents working on the Company's behalf, other insurers, actuaries, auditors, solicitors, translators and interpreters, tax advisers, debt-collection agencies, fraud-detection agencies, regulators, licence issuers, flag states, data-protection supervisory authorities;

(f) people or organisations that the Company has to, or is allowed to, share individuals' personal information with by law (for example, for fraud-prevention, statistical or licensing purposes);

(g) the police and other law-enforcement agencies to help them perform their duties, or with others if the Company has to do this by law or under a court order;

(h) if the Company (or any member of the Company's group) sell or buy any business or assets, the potential buyer or seller of that business or those assets; and

(i) a third party who takes over any or all of the Company Group's assets (in which case personal information the Company holds about its clients may be one of the assets the third party takes over).

Transferring Personal Information Outside the EEA

15. In the execution of the Company's operations the Company may transfer elements of Personal Information outside the EEA. The Company takes steps to make sure that, when it transfers personal information to another country, appropriate protection is in place, in line with data-protection laws.

16. Sharing Personal Information is required in order to apply for visas, or book travel or shuttles from time to time. In such cases, the data which the Company is required to submit varies from country to country, but normally includes: passport and seaman's book information, passport photographs, transport details and timings and next of kin details. The agents with whom the Company may share these data are based in UAE, Oman, Sudan, Israel, India and Malaysia, but may occasionally include other non-EEA countries. Under the terms of the Company's licensing and approvals from St Kitts and Nevis certain Personal Information, including sensitive Personal Information must be provided to representatives of their Government.

Retention of Personal Information

17. The Company keeps individuals' personal information in line with set periods calculated using the following criteria:

(a) How long the individual's PMSC has been a client of the Company, the types of services the PMSC uses, and when the PMSC will stop being a client. For employees and contractors of the Company, how long the individual has been employed.

(b) How long it is reasonable to keep records to show that the Company has met the obligations it has to the PMSC and by law.

(c) Any periods for keeping information which are set by law or recommended by regulators, professional bodies or associations.

(d) Any relevant proceedings that apply.

Rights of Individuals

18. Individuals have the right to access their information and to ask the Company to correct any mistakes and delete and restrict the use of their information. They also have the right to object to the Company using their information, to ask them to transfer any information they have provided, to withdraw permission they have given to the Company to use their information and to ask the Company not to use automated decision-making which will affect them. Individuals have the following rights (certain exceptions apply):

(a) **Right of access**: the right to make a written request for details of personal information and a copy of that personal information;

(b) **Right to rectification**: the right to have inaccurate information corrected or removed;

(c) **Right to erasure** ('right to be forgotten'): the right to have certain personal information erased;

(d) **Right to restriction of processing**: the right to request that personal information only be used for specific purposes;

(e) **Right to object**: the right to object to processing of personal information in cases where processing is based on the performance of a task carried out in the public interest or the Company has let the individual know that the processing is necessary for the Company's or a third party's legitimate interests;

(f) **Right to data portability**: the right to ask for the personal information made available to the Company to be transferred to the individual or a third party in machine-readable formats;

(g) **Right to withdraw consent**: the right to withdraw any consent previously given to handle personal information. If consent is withdrawn, this will not affect the lawfulness of the Company's use of an individual's personal information prior to the withdrawal of consent and the Company will let the individual know if, as a consequence, the Company will no longer be able to provide the selected services;

(h) **Right in relation to automated decisions**: individuals have the right not to be subject to a decision based solely on automated processing which produces legal effects concerning them or similarly significantly affects them, unless it is necessary for entering into a contract with them, it is authorised by law or the individual has given their explicit consent. The Company will let individuals know when such decisions are made, the lawful grounds relied on and the rights the individual has.

19. Other than the right to object to the use of data for direct marketing (and profiling to the extent used for the purposes of direct marketing), the individual's rights are not absolute: they do not always apply in all cases and the Company will inform individuals in correspondence how it will be able to comply with such a request. If a request is made, the Company will request confirmation of identity if necessary, and provision of information that helps better understand the request. If the request cannot be satisfied, an explanation will be offered.

20. In order to exercise individual rights please contact info@mngmaritime.com, either directly, or through the PMSC or employment agency.

Security Measures

21. **Organisational Measures**. The Company has adopted the following organisational measures to assess, develop and implement controls that secure information and protect personal data:

(a) **Information Security Policy**. The Company has an Information Security Policy as part of its Security Management System.

(b) **Business Continuity**. The Company has a business continuity policy including protocols and measures in place to back-up personal data and ensure that it can be recovered and maintained in the even of an incident.

(c) **Risk Assessment**. The Company conducts regular risk assessments of all aspects of the Company's activity.

(d) **Policies and Procedures**. The Company has a robust Security Management Policy as part of ISO 28000.

(e) **Management Information & Reporting**. Regular security reports and information are passed to management to ensure that adequate resources and funding are made available for data security.

(f) **Awareness & Training**. A culture of security and data protection awareness ensures that employees, contractors and any third-party working for or with the organisation, know what is expected of them and how to maintain compliance. Regular and ongoing training sessions for MNG personnel ensure that the latest information, guidance, legislation and regulations are known and understood.

(g) **Reviews & Audits**. The Company conducts regular reviews and audits to ensure that data protection functions, activities and systems are still effective and fit for purpose.

(h) **Due Diligence**. The Company conducts appropriate due diligence of its sub-contractors, agents and partners to ensure that data passed to a third party, whether inside or outside the EU/EEA, is afforded the same level of protection as that imposed by the Company.

22. **Technical Measures**. The Company has adopted the following measures and controls to systems and technological aspects of the Company, such as devices, networks and hardware.

(a) **Building Security**. The Company operates from a secure building affording access control measures to the estate, the building the floor and the offices. Each floor is covered by CCTV, security lighting and alarms.

(b) **Disposal**. The Company enforces correct disposal of paperwork and devices. Shredding and certified disposal of paper format hard-copy records is enforced, and printing of network documents discouraged. IT disposal is managed to guarantee effective and complete erasure of any personal data or access.

(c) **Cyber Security**. The Company employs measures to protect its IT infrastructure from advanced forms of hacking, vulnerabilities and constantly evolving threats.

(d) **Passwords**. Employees are aware that they must not share passwords or leave systems unlocked when unattended.

Breach Reporting

23. **Data Protection Points of Contact**. If any individual has any questions, comments, complaints or suggestions in relation to this notice, or any other concerns about the way in which the Company processes information or they wish to report a breach, they should contact the Data Protection Officer at info@mngmaritime.com. An individual also has a right to make a complaint to a local privacy supervisory authority. The Company's company registration is in the UK, where the local supervisory authority is the Information Commissioner:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom

Phone: +44 1625 545 745