THE JS HAMILTON MANAGEMENT CO LTD with POLISH BRANCH

GDPR POLICY
(General Data Protection Regulation)

Issued May 2018

Introduction

The JS Hamilton Group of Companies ***(shortened to JSHM for the written purpose of this policy)***, are fully committed to compliance with the requirements of the GDPR Act 2018, which came into force on the 25th May 2018. The company will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, partners or other servants of the company who have access to or process any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the GDPR.

Statement of Policy

To operate efficiently, JSHM must collect and use information about people with whom it works. These may include current, past, and prospective employees, clients, customers which are recruited, have been allocated or may be allocated to carry out work for the clients of JSHM. In addition, the law may require us to collect and use information in order to comply with the requirements of central government. This personal information must be handled and processed within the specific guidelines of the GDPR, this applies to paper records, digital records, or by any other means in which an individual can be directly or indirectly identified.

JSHM regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly.

To this end the Company fully endorses and adheres to the legislation included in the GDPR Act 2018.

Data Protection Principles

JSH will comply with relevant data protection law. GDPR requires that the personal information we hold about comply with the below principles:

1. Data must be processed lawfully, fairly, and transparently
2. Data is collected only for specific legitimate purposes
3. The data is adequate, relevant, and limited to what is necessary
4. The data must be accurate and kept up to date
5. The data is stored only as long as is necessary
6. The data processor ensures appropriate security, integrity and confidentiality of the data collected

Handling of Personal Data

JSHM will, through appropriate management and the use of strict criteria and controls: -

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not shared and processed without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
- Ensure that consent has been freely given by the individual whose data is to be processed and/or shared
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;

All JSHM employees are to be made fully aware of this policy and of their duties and responsibilities under the regulation.

All directors, managers and staff employed by JSHM will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected using secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.
- Personal data is not taken off site unless authorised as safe to do so by a director of JSHM.

All contractors, consultants, partners or other servants or agents of the Company must:

- Ensure that they and all their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the regulation. Any breach of any provision of the GDPR will be deemed as being a breach of any contract between the company and that individual, company, partner, or firm;
- Allow data protection audits by the company of data held on its behalf (if requested);
- Indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.
- It is the individual's responsibility to advise any change of circumstances to the company.

All contractors who are users of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Act regarding information supplied by the company.

The kind of information we hold about you

Personal data, or personal information, means any information about a living individual from which that living individual can be identified. It does not include data where the identity has been removed (anonymous data). Depending on your relationship with JSH, we may collect, store, process and use the following categories of personal information about you, including but not limited to:

・Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
・Date of birth.
・Gender.
・Marital status and dependants.
・Next of kin and emergency contact information.
・National Insurance number, tax reference number and tax codes.
・Copies of passport, visa, discharge book, identity cards and training certification.
・Bank account details, payroll records and tax status information.
・Salary, annual leave, pension and benefits information.
・Location of employment or workplace.
・Recruitment information (including copies of right to work and identification documentation, employment references, employment background check information and other information included in a CV, job application or cover letter or as part of the application process).
・Your SEA and all information included in the Contract of Employment records (including job titles, employment / work history, working hours, training records, education records, professional qualification records and professional memberships).
・Compensation history.
・Absence information, including family leave records such as maternity leave, paternity leave, adoption leave, parental leave and flexible working requests.
・Performance information.
・Disciplinary, capability and grievance information.

・Information about your use of our information and communications systems.
・Photographs.
There are "special categories" of more sensitive personal data which require a higher level of protection.
We may also collect, store, process and use the following "special categories" of more sensitive personal information:
・Trade union membership.
・Information about your health, including any medical condition, health and sickness records, and medical reports, along with vaccination records and copies of seafarers medicals .
・Genetic information and biometric data for identification purposes e.g. passport and/or driving licence.
・Information about criminal convictions and offences including police certificates and fingerprint records.

Use of Your Personal Data

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or from an employment agency or background check provider. We may sometimes collect additional information from third parties including employees (e.g. a recruitment referral), former employers, credit reference agencies or other background check agencies. We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

We will only use your personal information in accordance with applicable laws and regulations.
Most commonly, we will use your personal information in the following circumstances:
1. Where we need to fulfil your contract of employment.
2. Where we need to comply with a statutory or legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:
1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

We obtain all the categories of information in the list above (see point 2) primarily to allow us to fulfil your contract of employment SEA and to enable us to comply with our legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.
・Making a decision about your recruitment / employment or appointment.
・Determining the terms on which you work for us.
・Paying you and, if you are an employee, deducting relevant tax and National Insurance contributions and court order deduction, if applicable.
・Providing the following benefits to you for example; Death in Service Insurance.
・Liaising with the Company's pension provider, if applicable.
・Applying for crew entry visa's, visa waivers and work permits.
・Arranging mandatory immigration formalities to allow for the joining/leaving of a vessel.
・Arranging travel arrangements for your joining/leaving of a vessel.
・Administering your contract of employment.
・Business management and planning, including accounting and auditing.
・Conducting performance reviews, managing performance and determining performance requirements.
・Making salary and compensation decisions.
・Assessing qualifications and suitability for a particular job or task, including decisions about promotions.
・Gathering evidence for possible grievance, capability or disciplinary hearings.
・Making decisions about your continued employment or engagement.
・Making arrangements for the termination of our working relationship.
・Education, training and development requirements.

・Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
・Ascertaining your fitness to work
・Managing sickness absence and other absences from work.
・Complying with health and safety obligations.
・To prevent or detect fraud or other potentially criminal behaviour.
・To conduct data analysis studies to review and better understand employee retention and attrition rates.
・Equal opportunities monitoring.
・Liaising with external Government and regulatory bodies.
・Liaising with external third parties such as employers, shipowners, shipmanagers, professional advisors, business advisors, consultants and training providers.
Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Data sharing

We may have to share your data with third parties, including but not limited to:
・ShipOwners/ShipManagers
・Employers
・Shipping Agents
・Port/immigration officials.
・Border and coastguard official, e.g. United States Coast Guard.
・Training providers.
・Government bodies and ship registries.
・Travel Agencies.
・Doctors/medical practitioners, as and when required.
・Pension providers, if applicable.
・Third party service providers.
・Other entities in the group.
We require third parties to respect the security of your data and to treat it in accordance with the law.
We may transfer the personal information we collect about you to countries outside the EU, in order to fulfil your contract.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to fulfil your contract of employment (such as your joining of a vessel, paying you or providing you with a particular benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers or comply with employment legislation).
It is important that the personal information we hold about you is accurate and up-to-date. Please keep us informed if your personal information changes during your working relationship with us.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Retention of Personal Data

We will only keep your personal data for as long as is necessary for the purpose for which it was first provided and where we have a legal basis for doing so.

We will regularly review our records to ensure that we do not retain records for longer than we deem necessary or are permitted by legislation.

Implementation

The Managing Director is responsible for ensuring that the policy is implemented. Implementation will be led and monitored by the Managing Director who will also have overall responsibility for:

- GDPR training, for staff within the company.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the authority, with the GDPR.
- Ensure any new systems implemented apply the basic data protection by design and default principles
- Is the key contact for any data breaches and will act as point of contact between JSHM and data protection authorities.

Your Rights under GPDR

You have the following rights, which you can exercise free of charge:

Access - The right to be provided with a copy of your Personal Information (the right of access)
Rectification - The right to require us to correct your Personal Information. This enables you to have any incomplete or inaccurate information we hold about you corrected.
To be forgotten - The right to require us to delete your Personal Information—in certain situations
Restriction of processing - The right to require us to restrict processing of your Personal Information—in certain circumstances, e.g. if you contest the accuracy of the data
Data portability - The right to receive the Personal Information you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object to processing- of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground
For further information on each of those rights, including the circumstances in which they apply, please contact us or see the Guidance on individuals' rights under the General Data Protection Regulation :
in UK — from the UK Information Commissioner's Office (ICO) ,
in Poland — from Generalny Inspektor Ochrony Danych Osobowych (GIODO).

If you would like to exercise any of those rights, please email or write to us—see below:
'**How to contact us'**; and let us have enough information to identify you e.g. your full name, business address and customer name. Let us know what right you want to exercise and the information to which your request relates.
When processing a request, we may ask for additional information to confirm that the request is legitimate to ensure that the security of the data is maintained, and data is not disclosed to a person who has no right to receive it. JSHM will try to respond and process all legitimate requests within one month. We will keep you fully informed in all cases.

How to contact us

To **Request Access** or **Erasure** your Personal Information please email **polishoperations@jshmanco.com**

For any other request under your rights, or if you have any questions about this Policy that are not answered above or would like further information on how your information is used and how we maintain the security of your information, please email us at **dskinner@jshmanco.com**