

THE WHITAKER GROUP OF COMPANIES



GDPR POLICY (General Data Protection Regulation)

Issued May 2018

INTRODUCTION

The Whitaker Group of Companies (***shortened to JHW 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, JHW must collect and use information about people with whom it works. These may include current, past, and prospective employees, clients, customers which are employed, have been employed or may be employed to carry out work for JHW. In addition, the law may require us to collect and use information 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, CCTV or by any other means in which an individual can be directly or indirectly identified.

JHW 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.

THE PRINCIPLES OF DATA PROTECTION

The regulation stipulates that anyone processing personal data must comply with **Six Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

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

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **“special categories” of personal data**. These can be found in the GDPR Act 2018.

HANDLING OF PERSONAL DATA

JHW 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

In addition, JHW will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- 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;
- Performance with handling personal information is regularly assessed and evaluated;

All JHW 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 JHW will take steps to ensure that personal data is always kept secure 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 JHW.

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.

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 Financial Director is responsible for ensuring that the policy is implemented. Implementation will be led and monitored by the Financial 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 JHW and data protection authorities like the ICO.

RIGHTS UNDER GDPR

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 any mistakes in your Personal Information
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	The right to object: —at any time to your Personal Information being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your Personal Information, e.g. processing carried out for the purpose of our legitimate interests.
Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you

For further information on each of those rights, including the circumstances in which they apply, please contact us or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the General Data Protection Regulation.

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. We will send you the appropriate 'Data Subject Access Request Form' to be completed and returned so that we can process your request in the correct manner.

JHW will try to respond and process all legitimate requests within one month. Occasionally it may take us longer than a month depending on the complexity or number of requests. We will keep you fully informed in all cases.

HOW TO CONTACT US

To **Request Access** to your Personal Information (commonly known as a “data subject access request”) please email dm@whitaker-tankers.co.uk

To **Request erasure** of your Personal Information from our systems (“to be forgotten”) please email dm@whitaker-tankers.co.uk

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 dm@whitaker-tankers.co.uk