FORTH PORTS LIMITED

DATA PROTECTION POLICY

Contents

POLICY STATEMENT

This is the Data Protection Policy of Forth Ports Limited (the **"Company**") and each of its subsidiaries and subsidiary undertakings from time to time (the "**Group**"). Our contact details are accessible from www.forthports.co.uk.

This Policy outlines the obligations of the Group and its Employees and Workers relating to Personal Data under the Data Protection Act 1998 and the General Data Protection Regulation (from 25 May 2018) ("**Data Protection Legislation**"). Data protection rules are enforced by the UK Information Commissioner (ICO) and more information can be found at www.ico.gov.uk. The Company is primarily responsible for data protection compliance and has notified as such with the Information Commissioner.

Personal Data means any information held in any form that can identify individuals. This means information, including opinions, about other Group Employees, Workers, customers, site visitors and other third parties the Group deals with. Personal Data includes photos, email address, bank details, medical information, etc.

The Group will only obtain, store and use Personal Data for legitimate business purposes and/or where there is a statutory or contractual requirement to do so. These purposes include:-

- Recruitment and employment (including post-employment management)
- Conducting the everyday business of the Group
- Advertising and marketing the services of the Group
- Compliance with the legislation that applies to the Group, including health and safety
- Working with the relevant authorities to investigate breaches of the law, including crime and fraud
- Addressing complaints, grievances and claims
- Paying employees and pensioners
- Driving licence checks
- Statistical, financial modelling, accounting and reference purposes
- Insurance claims
- Training records
- Retention of customer data (current, previous and potential)
- Pension records
- Risk management
- SQA Centre – Qualification accreditation
- Security
- Complying with legal obligations.

The Company does not use data for automated decision-making.

The Group will not share personal data to third parties unless set out in this Policy or intimated to the affected person in writing (e.g. through a contract of employment).

Personal Data on IPOS databases is sent outwith the European Economic Area to TCS, Hyderabad for IT system testing. This transfer is undertaken in accordance with data protection laws to ensure that the processing of Personal Data is undertaken in a way which guarantees that Personal Data is processed to the same standards as required in Europe. Customer information may be shared with our shareholders which includes Public Sector Pension Investment Board, based in Canada.

SCOPE AND LIABILITY

This Policy applies to all Employees and Workers of the Group. "**Employees**" means all Group employees, potential employees and executive directors and "**Workers**" means all contractors and agency staff engaged by the Group.

This Policy covers all activities that the Group is responsible for managing, except Occupational Health records, which are subject to a separate policy.

Breach of this Policy by an Employee or Worker may be considered to be gross misconduct, and under the Disciplinary Procedure or Worker contract may result in dismissal.

Wilful or reckless breach of Data Protection Legislation by any person is a criminal offence and the individual committing the breach may be liable to criminal prosecution and/or fines. This includes actions such as theft of Personal Data.

The Group is not responsible for compliance with Data Protection Legislation by any third parties who are independently in control of Personal Data, such as Port of Tilbury Police. However, the Group takes sensible precautions to verify that such third parties have adequate protection in place.

DATA PROTECTION OBLIGATIONS

Data Protection Legislation contains principles (the "**Principles"**) which apply to the Group and its Employees and Workers which guide the use of Personal Data. Ultimately, the Group is responsible for, and needs to be able to demonstrate compliance with, the Principles and the Group looks for all Employees and Workers to recognise this responsibility to ensure the integrity of protection of Personal Data. These Principles are as set out in Appendix 1.

Sensible and reasonable steps should be taken to protect Personal Data, including:-

- Where Personal Data is lost, misplaced, accessed in a way which is unauthorised or otherwise subject to a security incident, Employees and Workers **must immediately upon becoming aware of the** incident notify their Line Manager. Line Managers must notify the Group HR Manager or Group General Counsel & Company Secretary for third party data.

- Personal Data must not be:-
    - used without a legitimate business reason;
    - recorded or used if inaccurate
    - disclosed or discussed except to Group Employees or Workers who need the information for their work
    - released by telephone unless the caller has been identified
    - faxed unless:
        a) a call ahead to check the number is made
        b) a fax cover sheet marked 'CONFIDENTIAL' is used
        c) a call to confirm receipt is made
    - removed from Group premises in hard copy, unsecured or unencrypted format;

- Personal Data must be securely erased when no longer needed by deleting from the Company's IT system(s) and shredded if paper copies;

- Visitors to Group premises should be identified and offices locked and alarmed out of hours

- Computer and manual filing systems must be kept secure

- If working remotely, work only in a secure location utilising VPN or Wifi which meets Company standards

- Ensure sub-contractors processing Personal Data on behalf of the Group (including those deleting or removing files) have adequate and certifiable security in place (including a written contract between the Group and the sub-contractor).

.
If you are concerned about any matter to do with Personal Data, please contact either the Group HR Manager or the Group General Counsel & Company Secretary immediately.

SENSITIVE PERSONAL DATA AND CCTV/DRONE IMAGES
Extra care should be taken with any Personal Data that is classed as "Sensitive" (also known as "special categories") of Personal Data. Information classed as Sensitive Personal Data is set out in Appendix 2.

All CCTV footage, including Drone Images, should be treated as Sensitive Personal Data and handled in accordance with the CCTV Policy.

GENERAL RESPONSIBILITIES
The relevant company in the Group will decide how and why data is processed and provide information to employees on how their data will be processed. The Group complies with the requirement for security of data including the notification to the Information Commissioner's Office of Personal Data breaches within 72 hours, where required.

The HR Department is responsible for this policy including responding to requests for access to information from Employees.

The Group General Counsel & Company Secretary is responsible for requests from the public and other third parties.

Further information on how to request information is set out in Appendix 3.

All Managers are responsible for ensuring that their staff are aware of and comply with this policy.

Employees have the right to know the legal basis for processing the data, data retention periods and that they have the right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way the Company is handling the data.

Employees can request their data is deleted comprehensively on the IT systems when their Personal Data is no longer required (e.g. when an employee no longer works for the Group). This is known as the "right to be forgotten". Please note however that certain limitations apply and data cannot be deleted due to other overriding legislative requirements e.g. PAYE, Occupational Health Medical Records.

A standard clause will be added to the Group's commercial contracts and terms and conditions for the supply of goods and/or services and/or facilities confirming the Group's Data Protection Policy and

the data protection obligations of the customer/supplier/vendor. Suggested wording is annexed hereto at Appendix 4.

ACCESS TO PERSONAL DATA AND OTHER RIGHTS

Individuals (which includes employees) have a number of rights relating to the use of their Personal Data which are set out at Appendix 1. In particular, individuals may request access to any Personal Data the Group holds about them. A number of exemptions exist to the right of access. In particular, information may not be disclosed if it contains the Personal Data of a third party. Please see our Access Policy at Appendix 3 for further detail.

TELEPHONE AND VHF RADIO RECORDING/EMAIL MONITORING

The Group carries out telephone and VHF radio recording and email monitoring. Please refer to the Group's Mobile Telephone/Device/Radio/Audio Equipment Policy and the Group's Network and Computer Security Policy for more information.

REVIEWING THE POLICY

The HR Department will ensure that this Policy meets the requirements of current legislation.

The HR Department has responsibility for this Policy and its good practice and compliance.

The Group reserves the right to amend or replace this Policy at its sole discretion and without notice.

Employees will be informed if there are any changes which might affect them.

OTHER RELEVANT GROUP POLICIES

- CCTV Policy
- Disciplinary Procedure
- Whistleblowing Policy
- Mobile Telephone/Device/Radio/Audio Equipment Policy
- Network & Computer Security Policy
- Occupational Health Policy
- Recruitment Policy
- Social Media Policy

APPENDIX 1 – FURTHER INFORMATION

The Principles
The following Principles of Data Protection Legislation apply to the Group and its Employees and Workers:

- Personal Data should be processed fairly, lawfully and in a transparent manner
- Personal Data should not be used for purposes that have not been specified
- Keep Personal Data accurate and up-to-date
- Ensure Personal Data is adequate, relevant and not excessive for its purpose
- Do not keep Personal Data for longer than is necessary for its purpose (and aim to anonymise data wherever possible)
- Observe the rights of individuals to access and control their Personal Data (as more fully set out below under "Data Subject Rights")
- Keep Personal Data secure.

The Group does not transfer Personal Data outside the European Economic Area without adequate protection and without informing the Employee or Worker of this (unless it originates from the data subject).

Data Subject Rights
Employees, workers and customers have certain rights which include:-

- The right to know why Personal Data is being processed
- The right to understand what legitimate interest there is in processing Personal Data (where that is relevant)
- Who will receive the data and how long the data will be retained
- The right of access to data as detailed in Appendix 3
- The right to have their data deleted (the "right to be forgotten"), rectified or modified
- The right to request information is restricted from processing where there is a question around the accuracy of the information, the processing is unlawful, there is no need to process the data or there is an objection to the data and a decision is pending
- The right to have certain data transferred to a third party (known as the right to data portability)
- The right to withdraw consent to the data being processed (where consent is relied upon) or otherwise object to certain processing
- The right to complain to the ICO (their details are accessible from www.ico.gov.uk)
- The right to understand any consequences of not giving data (e.g. if there is no statutory or contractual requirement).

The Group reserves the right to implement specific procedures to manage such rights. Employees and workers should contact the Group HR Manager should they have any questions in connection with these rights.

APPENDIX 2 - SENSITIVE PERSONAL DATA

Sensitive Personal Data
Sensitive Personal Data is information relating to:-

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade Union membership
- Physical or mental health or condition (including pregnancy)
- Sexual life
- Commission or alleged commission of an offence
- Any court proceedings or findings
- Genetic and biometric data.

All CCTV footage will be treated as Sensitive Personal Data and handled in accordance with the CCTV Policy.

The Company does not retain sensitive personal data except Trade Union Membership (for payroll deductions), Occupational Health, Drug & Alcohol 'for cause' and random test results and Court Proceedings. This Personal Data is required for statutory and contractual requirements and will be processed in accordance with applicable data protection laws.

APPENDIX 3 – ACCESS POLICY

The following procedure applies to requests for access to Personal Data:-

- Where an individual making a request is not known to the Group, identification must be provided before any Personal Data is released.

- If Sensitive Personal Data is requested additional precautions must be taken to identify the requester and validate the address for delivery of information.

- Requests for access to Personal Data should be made by completing the Subject Access Request Form available from the HR Department or available on the Intranet.

- Unless an exemption applies, information shall be supplied within one month after receipt of the request and any identification or clarification.

- All requests for access to Personal Data should be referred without delay to the HR Department for Employee Personal Data and Group General Counsel & Company Secretary for all other third party Personal Data.

- We can refuse any manifestly unfounded or in some cases excessive requests. We will write to the individual to explain why the request was refused. The individual can appeal this decision by writing to the HR Manager, stating why he/she disagrees with our decision. The HR Manager will ensure the appeal is heard by a Senior Manager within 7 working days.

APPENDIX 4 – STANDARD CLAUSE

The following clause shall be included in all contracts or purchase orders for the supply of services and/or goods and/or facilities. The wording of this clause may be varied as required or appropriate in the individual circumstances with guidance from the legal department:

Note - Port of Dundee Limited or Port of Tilbury London Limited or other Group subsidiaries will be substituted for the Company (Forth Ports Limited) for their respective contracts or purchase orders.

***delete as applicable**

1. Data Protection

1.1 The Vendor/Customer* confirms that it has read and understood the Company's Data Protection Policy, a copy of which is available at www.forthports.co.uk or upon written request to the Company. The Company and, where applicable, the Vendor/Customer* shall handle or process Personal Data in terms of and compliance with Data Protection Legislation and the Data Protection Policy.

1.2 The Vendor/Customer*and the Company shall comply at all times with Data Protection Legislation and shall not perform their obligations under this agreement in such a way as to cause the other party to breach any of their obligations under Data Protection Legislation. The Vendor/Customer * shall immediately notify the Company in the event that it becomes aware of a breach of Data Protection Legislation in connection with this agreement by the Vendor/Customer*, its employees, contractors or those for whom it is legally responsible.

1.3 The Vendor/Customer* shall at all times during and after termination of this agreement, indemnify the Company and keep the Company indemnified against all losses, damages, costs, expenses or other liabilities (including legal fees) incurred by the Company for any breach of the Vendor's/Customer's* obligations relating to Personal Data and the Data Protection Legislation.

APPENDIX 5 – HR DOCUMENT MANAGEMENT POLICY

Type of Employment Record	Statutory/ Code of Practice Reference	Format & Location	Retention Period/ Recommendation
Job applications and interview records of unsuccessful candidates	The Information Commissioner: Employment Practices Code Part 1: Recruitment and Selection (1.7.5)	Paper or electronic	9 months after notifying. Application forms should give applicants the opportunity to object to their details being retained.
HR and training records (includes Performance Management).	Health & Safety Records Employment Records	Paper or electronic.	OH records permanently retained. Paper personnel & training records destroyed 6 years after employment ceases. Electronic records permanently retained.
Written particulars of employment, contracts of employment and changes to terms and conditions.	Employment Rights Act 1996	Paper or electronic.	Whilst employment continues and up to 6 years after employment ceases.
Working time opt-out forms.	Regulations 5 and 9, Working Time Regulations 1998 (SI 1998/1833) (WTR 1998)	Paper or electronic. Originals are not required by the WTR 1998.	Two years from the date on which they were entered into.
Collective workforce agreements and past agreements that could affect present employees.	TULRA & Trade Union Act 2016	Paper or electronic.	Permanently or 10 years after ceasing to be effective.
Consents for the processing of personal and sensitive data.	Schedule 1, DPA, GDPR	Paper or electronic	For as long as the data is being processed and/or up to 6 years afterwards.

Type of Employment Record	Statutory/ Code of Practice Reference	Format & Location	Retention Period/ Recommendation
Disclosure and Barring Service (DBS) formerly Criminal Records Bureau (CRB), checks and disclosures of criminal records forms	ROA and Information Commissioner's Employment Practices Code Part 1.7.4 and 2.15.3	Paper or electronic	Should be deleted following recruitment process unless assessed as relevant to on-going employment relationship. Once the conviction is spent, should be deleted unless it is an excluded profession.
Immigration checks	Immigration, Asylum and Nationality Act 2006	Paper or electronic	Two years after the termination of employment.
Psychometric Tests/Assessment Centre Data	The Information Commissioner : Employment Practices Code Part 1 and Specific Test Guidelines	Paper or electronic	9 months after job application where applicant unsuccessful. Destroyed after 2 years for employees. Deleted after period of validity expires – varied by provider.
Drug & Alcohol Test Results	General Data Protection Regulations	Paper or electronic	If positive kept for 6 years. If non-negative destroyed after 12 months.
SQA Centre	Company Policy SQA requirements	Paper or electronic	Detailed in the policy document and vary between 3 months and 6 years.