Data Retention Policy

1. Policy Statement.

1.1 This data retention policy sets out the obligations of Solent Stevedores Limited and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control.

1.2 This policy applies to our entire organisation including our officers, employees, Customers and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

1.3 We are registered under the Information Commissioner's Office under registration number ZA381762.

2. Objectives.

2.1 It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- Our own servers.
- Any third party servers.
- Email accounts.
- Desktops.
- Employee-owned devices.
- Backup storage.
- Paper files.

2.2 This policy applies equally to paper, electronic retention and any other method used to store personal data. The period of retention only commences when the record is closed.

2.3 We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of your personal data under the General Data Protection Regulations.

2.4 The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a 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.

2.5 This Policy sets out the procedures that are to be followed when dealing with personal data and how we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. 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.
4. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
5. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
6. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 Regulation in order to safeguard the rights and freedoms of the data subject.
7. 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 organisational measures.
8. The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

2.6 With this in mind, this policy should be read in conjunction with our other policies which are relevant such as our data protection policy and IT security policy.

3. Security and Storage.

3.1 All data and records are stored securely to avoid misuse or loss. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

3.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

3.3 Examples of our storage facilities are as follows:

- Lockable storage units such as desk draws, filing cabinets etc.
- Locked rooms.
- Central archive room at head office.
- Employee electronic files encrypted, and password protected
- All electronic systems password protected.
- Payroll information processed in Head Office only with password protected access.

3.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.

- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on Solent Stevedores Limited Services Ltd central computer system instead of individual PCs.

4. Retention.

4.1 Data retention is defined as the retention of data for a specific period of time and for back up purposes.

4.2 We shall not keep any personal data longer than necessary but acknowledge that this will be dependent on the different types of documents and data that we have responsibility for.

4.3 The UK Limitation Act 1980 contains a 6 year time limit for many legal proceedings and Companies House and HM Revenue and Customs require 6 years of records to be retained. As such, our general data retention period shall be for a period of six years.

4.4 Our specific data retention periods are set out below:

Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period	Data accuracy and minimisation review date
Customers	Labour Information. Invoicing and Accounting records. Performance Data	Invoice Charging To be paid Bonus Payments by customer	Customers Payroll Processor Bank. Accountants. HMRC DP World Southampton and London Gateway.	6 years 6 Years 6 Years	Annual Review on completion of end of year accounts.
Potential employees	Application forms. Interview notes Records of Advertising	Recruitment and selection Recruitment and selection Unlawful Discrimination. Equality and Diversity Monitoring to comply with Equality and Diversity Act 2010	Port Authorities. Associated British Ports. DP World. Home Office Recruitment and Employment Confederation. Any other governing body.	Rolling 12 months 3 months 12 months	Monthly Monthly Annual Review

Employees	Contact Information. Date of Birth, Gender. Marital Status. Next of Kin. National Insurance no. Right to Work in the UK. Bank Details. Contract. Location of work. References. Application Information. Performance Information. Disciplinary and Grievance information. Photograph for ID passes. Information on unspent convictions. Copy of Driving License. Absence Records. Fitness to work documents. Holiday Requests. And authorisation. Issue of company policies and procedures to Permanent employees.	Determining the terms of employment. Right to work in UK. To Pay wages. To comply with HMRC obligations. Providing benefits such as Life Assurance and Injury Management. Pension to comply with legislation. Accounting and auditing. Record of achievement Gathering evidence for possible grievance or disciplinary hearings. Making decisions on continued employment. Arrangements for the termination of work. Dealing with legal disputes involving Permanent and non-permanent employees, Managing sickness absence.	Payroll processors. Banking Service processors. Retirement administration processors. Aviva. Financial Services Ltd. Company Insurers. HRMC. Company Accountants. Injury Management Insurers. IT Maintenance Processor. Company Solicitors. Customers: ABP DP World Southampton and London Gateway.	6 Years 6 years	Every 6 years for permanent and non-permanent Employees. Leavers – after last day of service. When the company receive a subject access request.

		Equal opportunities monitoring. To comply with employment law legislation.			
Employees	Medical Records Processed and stored by OH Company, owned by individual.	Legislative requirement, working in a Safety Critical Environment	Occupancy Health Ltd.	40 Years	Maintained and monitored by Occupancy Health Ltd.
Health and Safety	Training Records. Accident and Incident Reports. RIDDOR reports.	Evidence of Training. To comply with Health and Safety Legislation. Education, training and development requirements		6 years	Periodically.
Sensitive data	Maternity and Paternity. Parental Leave Correspondence with HMRC. Retirement Benefit Scheme. Death in Service	Statutory Maternity Pay regulations 1986. Payroll Processor. Retirement Benefit scheme Regulations 1986	HMRC. Company Insurance Provider. Next of kin	6 years	Within process timelines of each individual case.
Contractors	Work Requests. Record of work completed. Invoices	Evidence of work complicated. Service logs. Safety certificates. Payment.		6 years	Annual Review Or according to appliance requirements.
Employee	Transferring money from Company to individual bank accounts.	To make up short falls in pay.	Finance Department.	6 years	As and when each adjustment is made.

4.4 From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

5. Destruction and Disposal.

5.1 Upon expiry of our retention periods, we shall delete confidential or sensitive records categorised as requiring high protection and very high protection. These documents will be deleted, or Paper destroyed by shredding or by secured waste removal and disposal. We shall either delete or anonymise less important documents.

5.2 Our Divisional Data Protection Officers are responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.