



Data Retention Policy

1. Policy Statement.

- 1.1 This data retention policy sets out the obligations of South Coast Port Services 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 ZA195737.

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 through an internal protected portal of our payroll service provider.

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 South Coast Port 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 to be used by all Data Processors who create and manage documentation and electronic records as 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	Calculate Charges to customers	Payroll Processor Payroll Processor	6 years	Annual Review on completion of end of year accounts.
	Invoicing and Accounting records	Invoice Charging To be paid	Payroll Processor Bank. Accountants. HMRC	6 years	Annual Review on completion of end of year accounts.
	Performance Data	Bonus Payments by customer	DP World Southampton and London Gateway	6 years	Annual Review on completion of end of year accounts.

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
Potential Employee's	Application forms. Psychometric Tests. Interview notes	Recruitment and selection	Port Authorities. Associated British Ports. DP World. Home Office	Rolling 12 months	Monthly
	Non-Permanent Employees pending documentation checks	Recruitment and selection	Port Authorities. Associated British Ports. DP World. Home Office	3 months Pending 9 months retention	Monthly
	Records of Advertising	Unlawful Discrimination. Equality and Diversity Monitoring to comply with Equality and Diversity Act 2010	Recruitment and Employment Confederation. Any other governing body.	12 months	Annual Review
	Pre-Employment Medicals	Fitness to work in Safety critical environment	OH Provider.	12 months if employment not offered. 6 Years for employees.	Employment end date.
Employee's	Contact Information.	Determining the terms of employment	Data Processors.	6 Years after employment end date.	Employment end date.
	Date of Birth, Gender.	Legal requirement. Dock Regulations for use of machinery and working in high risk areas. GPG reporting	GPGR Payroll Processors.	6 Years after employment end date	Employment end date.
	Marital Status.	To comply with HMRC obligations	Death in Service Insurance Provider	6 Years after employment end date	Employment end date.
	National Insurance no.	To comply with HMRC obligations	HMRC	6 Years after employment end date	Employment end date.
	Proof of right to work in the UK.	Right to work in UK home office legislation	Port Security Authorities. Home Office Inspectors. Any other governing body.	6 Years after employment end date	Employment end date.

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
Employee's cont.	Bank Details.	To Pay wages.	Payroll Data Processor. Payroll Provider.	6 Years after employment end date.	Employment end date.
	Contract.	Determining the terms of employment.	Internal Data Processor.	6 Years after employment end date.	Employment end date.
	Location of work.	Determining the terms of employment.	Internal Data Processor.	6 Years after employment end date.	Employment end date.
	References.	Evidence of authenticity of person as required by Maritime Security Regulations in the UK 2002.	Internal Data Processor Port Security Authorities.	6 Years after employment end date.	Employment end date.
	Application Information.	Determining the terms of employment. Suitability to job role.	Internal Data Processor.	6 Years after employment end date.	Employment end date.
	Performance Information.	Making decisions on continued employment. Record of achievement.	Internal Data Processors.	6 Years after employment end date.	Employment end date.
	Disciplinary and Grievance information.	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.	Internal Data Processors.	6 Years after employment end date. 6 Years after employment end date 6 Years after employment end date	Employment end date. Employment end date. Employment end date.

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
Employees cont.	Photograph.	ID passes required for working in the Port Southampton. Maritime Security Regulations in the UK 2002.	Port Security Authorities.	6 Years after employment end date.	Employment end date.
	Information on unspent convictions.	Maritime Security Regulations in the UK 2002.	Port Security Authorities.	6 Years after employment end date.	Employment end date.
	Copy of Driving Licence.	Requirement for driving allocations of work.	Port Security Authorities.	6 Years after employment end date.	Annual Review.
	Absence Records. OH Reports Fitness to work documents.	Managing sickness absence. Monitoring Wellbeing.	Internal Data Processors.	6 Years after employment end date.	Employment end date.
	Holiday Requests. And authorisation.	To Pay wages.	Internal Data Processors.	6 Years.	Annual Review.
	Issue of company policies and procedures to Permanent employees.	Rules of engagement with SCPS.	Internal Data Processors.	6 Years after employment end date	Employment end date.
	Issue of hand book to non-permanent employees	Rules of engagement with SCPS.	Internal Data Processors.	6 Years after employment end date.	Employment end date.
	Medical Records Processed and stored by OH Company, owned by individual.	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002.	Occupancy Health Ltd.	40 Years.	Maintained and monitored by Occupancy Health Ltd.
Health and Safety	Accident/Incident and near miss forms, accident records/ reports/RIDDOR reports/investigations and other correspondence/papers relating to an injury/ill health to an employee that happens out of or in connection to the work activity, including RIDDOR reports where necessary.	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 superseded by RIDDOR 2013 Social Security Act 1975 Limitations Act 1980.	HSE. Data Processors. Customers.	40 Years.	Annual Review.

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
Health and Safety cont.	First aid reporting forms non work-related incidents but injured person received first aid from the first aider on site.	Health and Safety (First Aid) Regulations 1981.	First Aider. Data Processor.	6 Years.	Annual Review.
	Records documenting the issues of personal protective equipment/ other special equipment to an employee and records of tests /examinations and control systems.	Limitations Act 1980 Management of health and safety at work regulations 1980.	Data Processor. HSE.	6 Years.	Annual Review.
Sensitive Data	Maternity and Paternity Leave. Parental Leave. Calculations. Certificates (MatB1s) & other medical evidence.	Statutory Maternity Pay regulations 1986. Payroll Processor.	Data Processor. HMRC.	6 years.	6 years after the end of the Paternity / Maternity leave ends.
	Correspondence with HMRC.	HMRC Regulations.	Data Processor. HMRC.	6 Years	Employment end date.
	Retirement Benefit Scheme.	HMRC.	Insurance Provider.	6 Years after the end of the benefit.	Reviewed on Individual basis when required.
	Death in Service.	Company Benefit.	Next of kin Company Insurance Provider.	3 Years from date beneficiary Payment concluded.	Annual Review.
	Employment Tribunal claims.		External Solicitors. ACCAS. HM Tribunal Services.	3 Years from date the claim is concluded.	Within process timelines of each individual case.
Contractors	Contact Details. Names. Email Addresses. Place of Work. Type of business /Position with in business.	Work Requests. Record of work completed. Invoices Evidence of work completed. Service logs. Safety certificates. Payment.	External Contractors.	6 years.	Annual Review or according to service requirement.

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
Payroll	Transferring money from Company to individual bank accounts.	Wage payments. To make up short falls in pay.	Payroll. Departments Per division. Finance Department. Canute Chambers.	6 years.	6 years after the end of the tax year.
	Statutory sick pay records	Statutory compliance.	Payroll. Departments Per division.	6 years.	6 years after the end of the tax year.
	Redundancy Settlement Agreements.	Statutory compliance.	Payroll. Departments Per division.	6 years.	6 years after the end of the tax year.
	Wage/salary records. Records in relation to hours worked and payments made to workers.	HMRC.	Payroll. Departments Per division. Finance Department. Canute Chambers.	6 years.	6 years after the end of the tax year.
GDPR Integrity	Information Breaches.	General Data Protection Regulations 2018.	Divisional Data Protection Officer. Data Protection Controller Officer. ICO.	6 years Best Practice.	Every three months from May 2018.
	Subject Access requests.	General Data Protection Regulations 2018.	Divisional Data Protection Officer. Data Protection Controller. HR Data Processors.	6 years Best Practice.	Every three months from May 2018.
	GDPR Controller. Risk Management Quarterly Review.	General Data Protection Regulations 2018.	Data Protection Controller. Divisional Data Protection Officers.	6 years Best Practice.	Every three months from May 2018.

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.