



Calafort Phort Láirge

Port of Waterford

Data Protection Policy

Version:	2.0
Document Owner:	
Approved by:	
Publication Date:	June 2024
Date for next review:	

Contents

1. Purpose	3
2. Scope	3
3. Policy Statement	3
4. Data Protection Principles	4
5. Lawful Use of Personal Data	4
5.1 Requirements for lawful use of Personal Data	4
5.2 Requirements for lawful use of Special Category Personal Data	5
6. Transparency Requirements	6
7. Sharing of Personal Data with Third Parties	6
8. Data Subject Rights under Data Protection legislation	7
9. Handling Data Subject Requests	7
10. Security for Personal Data and Handling Breaches	8
13. Summary of Responsibilities	10
Annex: Procedure for Making a Data Access Request	11
DATA ACCESS REQUEST FORM	12

1. Purpose

Port of Waterford (“the Port”), is required by law to comply with the following Irish and EU legislation relating to the processing of Personal Data (jointly referred to as “Data Protection legislation”):

- The Data Protection Acts 1988 - 2018
- [General Data Protection Regulation](#) (GDPR) 2018

The purpose of this Policy is to outline Port of Waterford’s approach to complying legislation in its day-to-day operations.

2. Scope

This Policy applies to all staff members, including agents and contractors and data processors (third parties who process personal data on behalf of the Port. This Policy sets out mandatory requirements applicable where these parties collect and handle personal data. This policy must be followed to ensure the lawful processing of personal data within the Port.

Personal Data is defined in GDPR as “any information relating to an identified or identifiable natural person (‘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.”

The legislation applies equally to digital documents and paper/hard copy documents, therefore the Policy must be followed regardless of the format in which personal data is held.

3. Policy Statement

In order to carry out its statutory, commercial and administrative functions, Port of Waterford (“the Port”) needs to collect and process personal data relating to individuals for the purposes of its day to day activities (such as payroll, pension, safety, security, access control, marketing and financial processing).

The Port takes the confidentiality of all personal data particularly seriously and consequently takes all reasonable steps to comply with the principles of GDPR. The Port collects and processes personal data, only where necessary to meet specific legitimate purposes, and to retain that information only for as long as those purposes remain. The Port will also not pass personal data with any third party, except where required by law, statutory obligations or legitimate purposes balanced against the rights and interests of the data subject. These principles are explained further in section 4 below.

The Port is committed to ensuring that all employees, agents, contractors and data processors comply with legislation and protect the confidentiality of any personal data held by the Port, and the privacy

rights of individuals. More information is provided on the specific responsibilities in Section 11 – Summary of Responsibilities.

4. Data Protection Principles

GDPR imposes certain obligations on organisations' handling of personal data, these obligations are outlined in the principles of the GDPR (listed below) which specify requirements for how it must be collected, used, kept, and not disclosed to any other person unlawfully. The Port must comply with these GDPR principles:

- **Lawfulness, Fairness and Transparency:** Collected and used for a specified lawful purpose which is transparent to the data subject (the lawful purposes for which data can be processed are outlined in section 5. Lawful Use of Personal Data below and information on transparency is contained in section 6).
- **Purpose Limitation:** Not used or disclosed in a manner incompatible with the specified purpose for collection and use.
- **Data Minimisation:** Adequate, relevant and limited to what is necessary for the specified purpose for collection and use.
- **Accuracy:** Kept accurate, complete and where necessary up to date.
- **Storage Limitation:** Not be kept for longer than is necessary for the specified purpose for collection and use.
- **Integrity and Confidentiality:** Processed in a manner that protects its security, including protection against unauthorised or unlawful sharing or use and against accidental loss, destruction or damage

5. Lawful Use of Personal Data

5.1 Requirements for lawful use of Personal Data

Personal data can be collected and processed only where one of the following lawful purposes applies (and not further processed for purposes incompatible with these original purposes):

1. **Consent:** when the data subject agrees to let their personal data be used for a specific purpose.
2. **Contract:** when using the data subject's personal data is necessary to fulfil a contract they are a party to.
3. **Legal Obligation:** when the Port is subject to a legal obligation to process the personal data.

4. **Vital Interests:** in exceptional circumstances, where the processing is necessary to protect the life of a data subject or another person.
5. **Public Interest:** when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Port.
6. **Legitimate Interest:** when using the data subject's personal data is necessary to fulfil a legitimate interest pursued by the Port or a third party, balanced against the rights and interests of the data subject.

5.2 Requirements for lawful use of Special Category Personal Data

Data Protection legislation recognises that some personal data is more deeply personal to an individual and therefore requires additional protection due to its sensitivity. For this reason, it defines 'Special Category Personal Data' which requires additional protections.

Special Category Personal Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Examples of special category personal data include employees' sick leave requests or dietary preferences (kosher, halal etc.).

The protections required for Special Category Personal Data are also required for any personal data relating to criminal convictions and offences (Criminal Data).

Lawful Use of Special Category Personal Data and Criminal Data: Use of such data is generally prohibited, unless one of the following conditions are met, in addition to the application of one of the legal bases listed above:

1. **Explicit Consent:** Where a data subject has given explicit consent to the processing for the specific purposes.
2. **Employment and Social Security:** When the use of data is required by law relating to employment, social security.
3. **Vital Interest (consent not possible):** When the data subject is unable to express their consent and the processing of their personal data is necessary to protect their life or the life of another person.
4. **Publicly Shared Data:** When the personal data involved has been manifestly made public by the data subject.
5. **Legal Claims and Court Proceedings:** When the use of data is necessary for the establishment, exercise, or defence of legal claims or where courts are acting in their judicial capacity.

6. **Substantial Public Interest:** When the use of data is necessary for substantial public interest on the basis of law which is proportionate to the purpose pursued and protects the rights and interests of the data subject.
7. **Specific Medical Reasons:** Where the use of data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to a contract with a health professional (subject to conditions and safeguards).
8. **Public Health Interest:** Where the use of data is necessary in the interest of public health such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices on the basis of law (with measures and safeguards).
9. **Archiving:** Where the use of data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of law (with subject to conditions and safeguards).

6. Transparency Requirements

Where the Port processes personal data certain information must be made available to the data subjects in order to comply with [Article 13](#) and [14](#) (GDPR), such as the purposes of the processing, any third parties their data will be shared with, information on their rights etc. Where the personal data is collected directly from the individuals, this information should be provided at the point of collection. Where the data is not collected directly from the data subjects the Port is still obliged to provide data subjects with the information, except where providing the information is impossible or would involve a disproportionate effort, where the disclosure is required by law or where the data must remain confidential under an obligation of professional secrecy (see [Article 13](#) and [14](#) (GDPR) for more information).

7. Sharing of Personal Data with Third Parties

All staff have an individual responsibility to ensure that they adhere to this Policy and Data Protection legislation when interacting with external parties. Any sharing of personal data with third parties must comply with the principles outlined in section 4.

In addition to this, the Port must comply with [Article 28 \(GDPR\)](#) when outsourcing services to third parties (service providers) involving the processing personal data. In order to meet this requirement the Port shall use only service providers who provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures to meet the requirements of Data Protection legislation. In addition, the relationship with the service provider must be defined from a data protection perspective. This should be done through a contract containing the minimum content

as defined in [Article 28 \(GDPR\)](#), outlining the responsibilities of both parties regarding the personal data processed to provide the service.

Transfers of personal data outside the European Economic Area (EEA) constitute an international transfer, such transfers are subject to specific conditions and safeguards which must be implemented before the transfer takes place. The specific requirements depend on the country of destination, for further clarification, please contact the Port's Data Protection Officer (DPO) at dpo@portofwaterford.com.

8. Data Subject Rights under Data Protection legislation

Data Protection legislation grants individuals (data subjects) certain rights concerning the processing of their personal data. Individuals have the following rights:

- **Access to personal data:** Data subjects may request information on how the Port uses their personal data and can request access to a copy of their personal data.
- **Data rectification:** Data subjects may request that any inaccurate personal data held by the Port regarding them is corrected.
- **Data erasure:** Data subjects may request the erasure of their personal data processed by the Port.
- **Restriction of processing:** Data subjects may request that the processing of their personal data be suspended by the Port.
- **Data portability:** Where processing is carried out under the consent and in an automated means, data subjects may request to be provided with a copy of their personal data in a machine-readable format or have this transferred to another organisation.
- **Object to processing:** Data subjects may object to the processing of their personal data on grounds relating to their particular situation.
- **Not to be subject to automated decision making:** Data subjects have the right not to be subject to a decision based solely on automated processing where this has a legal or similar effect.
- **Lodge a complaint and seek judicial remedy:** Data subjects have the right to request assistance from the Data Protection Commission and to seek judicial remedy.

Such rights are not absolute and their exercise may be subject to specific conditions and exemptions as established by Data Protection legislation.

Where your data is processed by the Port, you as a data subject may exercise these rights by contacting the DPO in person, at dpo@portofwaterford.com or by calling 051-89900. For the purpose of exercising your right of access please see the procedure contained in the Annex (at the end of this policy) and for the most efficient response, use the access request forms contained therein.

9. Handling Data Subject Requests

To exercise the rights mentioned above, individuals may submit requests to the Port concerning their personal data. It is likely that individuals will direct their requests to the DPO email address. However, they can potentially exercise their rights by submitting a request to any employee of the Port, this is particularly likely where employees regularly interact with clients or external partners. Where such a request is received, the DPO must be notified immediately and the following considerations should be taken into account in handling such requests:

- **Time limit:** The Port must process the request and reply to the data subject within one calendar month of receipt, unless an extension is necessary due to the volume and complexity of the request.
- **No formal requirements:** Requests can be submitted in any form (e.g., orally or in writing), individuals are not required to label a request as a data protection-related request.
- **Avoid data breaches:** Only the data subject or an agent acting on their behalf can exercise rights related to their data. If there are reasonable doubts about the identity of the requester, proof of identity should be requested, where an agent is acting on behalf of the data subject, proof of authorisation must be requested. Complying with a request from an individual not entitled to exercise the right will amount to a data breach.
- **Assess legitimacy of requests:** The rights granted by Data Protection legislation are not absolute. Before complying with a request, it should be verified as to whether the conditions laid down by the law are met, or if any exemptions apply.
- **Document actions taken:** The Port must be able to prove that requests were handled in compliance with the law in case of inspections or complaints. All information related to the handling of received requests must be stored for an appropriate duration to demonstrate compliance.

10. Security for Personal Data and Handling Breaches

The security of personal data is of paramount importance to the Port. In addition to the principles contained within this policy, staff are also advised to read the Company employee handbook which contains guidance on acceptable use of devices and company assets.

A personal data breach is a breach of security leading to the loss of confidentiality, integrity or availability of personal data.

Where an individual becomes aware of a suspected personal data breach, they must immediately report it to the DPO (either in person, by emailing dpo@portofwaterford.com or by calling 051-899800). All individuals in scope of this Policy (all staff members, including agents and contractors and data processors) are responsible for the detection and immediate reporting of any suspected personal data breaches.

Below is a non-exhaustive list of some scenarios involving (suspected or materialised) personal data breaches:

- A member of HR is dealing with a complaint raised by an employee against their manager and drafts an email they intend to send to the individual making the complaint with specific clarification questions regarding the issue, but they accidentally send the email to the wrong employee.
- The Port is impacted by malware that encrypts and exfiltrates personal data relating to employee pensions.
- An employee's laptop containing unencrypted payroll data is lost.
- HR files containing information on disciplinary proceedings is accidentally saved in a folder that all members of staff have access to. An individual involved in the disciplinary that should not have access to such data, views and amends some of these documents.

Where a breach of personal data is likely to result in a risk to the rights and freedoms of natural persons, the Data Protection Commission (DPC) must be informed of the breach within 72 hours of the Port becoming aware of it. In addition to notifying the DPC, where the data breach is likely to result in a high risk to the rights and freedoms of natural persons, then the Port must inform the impacted data subject(s) of the breach without undue delay. Any decisions as to whether to report/communicate should be made in line with guidance provided by the DPO.

Where the breach also involves an attempted or successful cyber-attack or otherwise impacts the security of the Port's systems, networks, applications or equipment it will be handled in accordance with the Port's Cybersecurity Incident Response Plan [<G:\DOC\IT docs\Cyber Security\Cyber Security Compliance support\POW CIRP v1.0 Final.pdf>].

11. Other Data Protection Obligations

In addition to the requirements covered so far in this policy the GDPR also imposes the following obligations on organisation when processing personal data:

- **Records of Processing Activities (RoPA):** Article 30 (GDPR) requires that the Port, as a Data Controller, must maintain a record of processing activities under its responsibility (see [Article 30 \(GDPR\)](#) for the specific requirements).
- **Data Protection Impact Assessments (DPIA):** Where the processing of personal data conducted by the Port is likely to result in a high risk to individuals (for example where special category personal data is processed on a large scale) Article 35 (GDPR) requires that a DPIA be conducted (see [Article 35 \(GDPR\)](#) for the specific requirements).

12. Data Protection Officer

Within the Port, the Data Protection Officer (DPO) has responsibility for the co-ordination of Data Protection activities. Queries and clarifications should be directed to the DPO:

Address: Data Protection Officer, Port of Waterford, 3rd Floor Marine Point, Belview Port, Waterford X91 W0XW

Email: DPO@portofwaterford.com

More complete information is available from the Office of the Data Protection Commissioner at: <http://www.dataprotection.ie>

This Policy document will be reviewed regularly and updated as appropriate, in line with any legislative or other relevant development.

13. Summary of Responsibilities

Department Responsibilities: Key post holders have responsibility for ensuring that:

- All personal data being processed within their department complies with the Data Protection legislation and this Policy.
- All contractors, agents and other non-permanent staff engaged to work on behalf of the port, are aware of and comply with this Policy.
- All personal data held is kept securely and is disposed of in a safe and secure manner when no longer needed.

Staff Responsibilities: Staff must ensure that:

- Participate in any assigned data protection and information security trainings.
- Personal data which they hold or process is kept securely.
- Personal data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- Any personal data breaches they witness or cause are immediately reported to the DPO.

Annex: Procedure for Making a Data Access Request

Making an access request

If you wish to make a data access request, the most efficient manner is to make this request in writing using the Data Access Request form contained below and send it to the Data Protection Officer.

To help us to respond to your request, please be as specific as possible about the information you wish to access. Please include any additional details that would help to locate your information - for example, a staff number, names of departments/offices that you were associated with, etc.

If you would like to authorise a third party to submit a data access request on your behalf (e.g. a family member or solicitor), you must provide written authorisation (completing section 7 of Data Access Request form) to allow us to disclose your personal data to that third party.

Fees

No application fee is required to process your data access request.

Identification

In order to ensure that personal data is not disclosed to the wrong person, you must provide proof of identity before any personal data can be released to you. Acceptable forms of identification include: a copy of your passport or driving licence, a staff ID card, a copy of top of your bank statement or utility bill.

Please provide only copies of these documents, these will be acceptable in most cases, however we reserve the right to ask to see original documents where necessary. Where you provide copies of such documents, they will be securely destroyed once we have verified your identity.

DATA ACCESS REQUEST FORM

**For the exercise of rights enshrined in Data Protection Acts, 1988 to 2018
EU General Data Protection Regulation**

SECTION 1 – YOUR DETAILS (PLEASE USE BLOCK CAPITALS)

Surname:	
First Names(s):	
Postal or Email Address (for responses to be sent to)	
Telephone number: (include only if you wish to be contacted via this)	

SECTION 2 – YOUR RELATIONSHIP WITH PORT OF WATERFORD

Please complete the below information to help the Port Identify you.

Are you a current/former member of staff?	YES / NO* <i>(*delete as appropriate)</i>
If yes, please provide details on the period of employment and your role:	
If you are not a current/former member of staff, please indicate your relationship with the company, including dates of interest:	

SECTION 3 – PERSONAL DATA REQUESTED *In the box below, please provide as much detail as you can about the specific personal data you wish to access in order to help us locate it quickly.*

In accordance with the General Data Protection Regulation, I request access to the following personal data	
--	--

that I believe Port of Waterford holds about me:	
--	--

SECTION 4 – IDENTIFICATION

In order for us to protect the security of personal data, it is necessary for you to provide proof of your identity. Acceptable forms of identification include:

- Copy of passport or driving licence
- Staff/student ID Card
- Copy of bank statement
- Copy of utility bill

Please send copies, these are acceptable in most cases, however we reserve the right to ask to see original documents where necessary. Copies of such documents sent with your access request form will be securely destroyed once we have verified your identity.

Please complete either section 6 or section 7 as appropriate

SECTION 5 – DECLARATION OF DATA SUBJECT

I confirm that I am the data subject named in Section 1 and I am requesting access to my own personal data. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. Data submitted on this form will only be used for the purposes of this data access request and recorded for statistical purposes for a period of 12 months.

Signed:	Date:
---------	-------

SECTION 6 – DECLARATION OF DATA SUBJECT FOR AGENT TO ACT ON THEIR BEHALF Please complete this section if you wish someone else to submit a data access on your behalf (e.g. family member, solicitor).

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my data access request. I have

enclosed evidence of my identity referred to in Section 5 and confirm that I want my personal data to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. Data submitted on this form will only be used for the purposes of this data access request and recorded for statistical purposes for a period of 12 months.

Signed:	Date:
---------	-------

Name of agent:	
Relationship to data subject:	
Postal or Email Address: (for responses to be sent to)	
Telephone number: (Include only if you wish to be contacted via this)	

RETURNING YOUR COMPLETED FORM:

Please send your completed form (with proof of identity and fee) to:

Agnes Paslawska
 Data Protection Officer
 Port of Waterford
 3rd Floor Marine Point
 Belview Port
 Waterford X91 W0XW

For assistance, telephone: (051) 899 800

FOR INTERNAL USE ONLY:

Reference No:	DP/
Date request received:	
Fee attached:	YES/NO
Identity verified:	YES/NO
If yes:	
Original ID supplied in person:	YES/NO
If yes, original evidence of ID checked and returned to requester:	YES/NO
Copy ID attached to request:	YES/NO
If yes, ID verified and documents shredded by:	