PLYMOUTH AND SOUTH DEVON FREEPORT

DATA PROTECTION POLICY

CONTENTS

DATA PROTECTION POLICY

Introduction

Information is a strategic asset of Plymouth and South Devon (PASD) Freeport that must be managed accordingly.

To operate efficiently, PASD Freeport must collect and use information about people with whom it works and for whom it provides services. These include members of the public, current, past and prospective employees, clients, customers, and suppliers. The Freeport is also required to collect and process information to comply with specific legislation.

This policy ensures that PASD Freeport complies with the Data Protection Act 2018 and all the provisions in that act, which implement the EU's General Data Protection Regulation (GDPR) into UK law.

This policy applies to the Member Steering Group, Board of Directors and its sub-Committees, Partners, Employees and contractual third parties and agents of PASD Freeport.

It is the responsibility of all Freeport staff to exercise appropriate controls to minimise the risk of breach of this policy.

Anyone found to be in breach of this policy may be subject to disciplinary actions.

Information processing

The Freeport will only process or store information that it has a legal basis for processing. Any information that does not have a legal basis for processing will be prohibited.

The Freeport's Publication Scheme will be published on the Freeport website.

The Freeport is registered with the Information Commissioner and will pay the requisite fee at least once a year.

Data protection principles

The Freeport will adhere to the following data protection principles set out in the Data Protection Act.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability
- Processing of Special Categories of data

Processing of special categories of data

Special Categories of data is a term that is interchangeable with the term Sensitive personal data.

The Freeport will treat the following types of data as Special Categories of data:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership

- Health data
- Data concerning a natural person's sex life or sexual orientation

The Freeport will only process Special Categories of data when the following circumstances have been met:

Explicit consent has been provided by the data subject.

- It is necessary for the Freeport to conduct in the field of employment and social security and social protection law.
- It is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- The personal data has been made public by the data subject.
- It is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- It is necessary for reasons of substantial public interest, and proportionate to the aim pursued, whilst respecting the essence of the right to data protection and providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- It is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee.
- It is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical.

The Freeport will record all activities which process Special Categories of data in the Information Asset Register, with accompanying criteria for processing each specific piece of data.

Where special category data is processed, this must be done in accordance with the Appropriate Policy Document contained in Appendix A.

Data Protection Officer

The Freeport Operations Director is designated as the Data Protection Officer (DPO)

The Freeport will publish the contact details of the DPO on the Freeport website.

The Data Protection Officer will ensure members, Board of Directors and its sub-Committees, Partners, Employees and contractual third parties and agents of PASD Freeport comply with the requirements of the Data Protection Act / GDPR.

The Data Protection Officer will ensure the following functions are conducted.

- Ensure all comply with the Data Protection Act 2018 / GDPR (the Act).
- Monitoring of compliance with the Act.
- Raise awareness / provide training around compliance of the Act as appropriate.
- Assign responsibilities for staff involved with data processing as appropriate.
- Ensure Data Protection Impact Assessments are carried out & monitor performance against the DPIA as appropriate.
- Cooperate with Plymouth City Council as the Accountable Body.
- Act as the contact point for Plymouth City Council as the Accountable Body.

The Freeport Chief Executive will be designated as the Senior Information Risk Owner, (SIRO) to take overall ownership of the management of information risks relating to the delivery of the Freeport's corporate objectives.

Information publication

The Freeport will publish its Information Asset Register.

The Freeport will abide by the Publication Scheme set out by Plymouth City Council as the Accountable Body for non-personal information to ensure transparency is maintained.

Access to personal information by the data subject

An individual may request a copy of any data held about them, or information about the reasons it is kept and processed and the people to whom it is disclosed. The information must be provided, in clearly understandable terms within I month of the receipt of a valid request.

There will be no charge for a standard Subject Access Request. A charge will be levied for a Subject Access Request which is deemed to be manifestly unfounded, excessive or a repeated request.

A person seeking information will be required to prove their identity and provide sufficient information to enable the Freeport to locate the requested information. The timescale of one month will begin on the day a PASD Freeport member of staff receives proof of identity and sufficient information from the person seeking the information.

Information may be withheld where the Freeport isn't satisfied that the person making the request is who they say they are, or where the requester is an organisation or body that the Freeport isn't satisfied is authorised to receive the information.

The Freeport will disclose, in accordance with Data Protection legislation, all personal information regarding a particular data subject, regardless of the content.

The Freeport will redact any third-party information from a Subject Access Request disclosure, unless explicit consent has been given from that third party to disclose the information or the Freeport deems it to be reasonable, in all the circumstances, to disclose the information.

Freeport staff must not alter any personal information to prevent disclosure under a Subject Access Request.

Access to personal information by third parties

An organisation may request a copy of any data held about an individual providing the appropriate Data Protection Act exemption is supplied. A formal written exemption form is required to supply the information, which will detail a specific legitimate reason to requesting the information.

Information sharing

The Freeport will only share personal information in the following circumstances: -

- There is a legal requirement to share information that has an exemption in the Data Protection Act.
- For the provision of services with partners.

In situations where there is not a legal exemption to share information, an Information Sharing Agreement will be put into place with the partner.

Information sharing agreements can be put into place for all other Information Sharing situations.

Provision of information

All information will be provided in a common format that is reasonably requested by the data subject.

Information will be provided in a paper format where requested but may be subject to a charge for

materials.

Information will be provided in a portable electronic format when the following criteria are met:

- The information has been provided to the Freeport by the data subject.
- The information is being processed based on the data subject's consent or for the performance of a contract or memorandum of understanding.
- The information is being processed by automated means.
- The information is not in paper format.

Other information rights

An individual may request that data held about them by the Freeport is erased if the following conditions are met:

- The information was provided with consent and the data subject wishes to withdraw consent.
- The information was provided with time limited consent, and the time limit has expired.
- It is no longer necessary for the information to be held.
- The information was processed based on legitimate interest and there is no overriding legitimate interest to prevent the Freeport erasing the data.
- The information is not being lawfully processed by the Freeport.

The Freeport will not erase any information under which it has a legal basis to hold the information for the provision of a statutory duty and will retain information where it is required to do so through our MOU with Government for a period of 7 years.

The Freeport will ensure all data erasure requests are completed within one calendar month.

An individual may request that data held about them by the Freeport is rectified if the personal data is inaccurate or incomplete. The Freeport will rectify personal information which is factually incorrect within one month of receiving a data rectification request.

The Freeport will ensure that individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Any data subject can request enforcement of these rights by writing to the Freeport's Data Protection Officer.

Information retention

The Freeport will retain information for 7 years in accordance with our MOU with government.

- Personal information stored in electronic format will be securely deleted when it reaches the disposal date.
- Special Categories of personal information stored in electronic format will be securely deleted when it reaches the disposal date.
- Personal information stored in paper format will be securely shredded when it reaches the disposal date.

Consent for use of information

The Freeport will ensure that consent arrangements are clear and specific about the intended use of the collected information and that consent is freely given and is not a condition of the provision of a service.

The Freeport will ensure that:

- Consent is obtained from a parent or guardian where the information about a child under the age of 12.
- If consent is required for using information about a child over the age of 12 years, the consent is provided by the data subject, the parent or guardian.
- Where possible, consent will be required for a fixed time at the end of which, either consent will be requested again or the information deleted.
- That data subjects are made aware of their right to withdraw consent at any time, without any reason needing to be given.

The Freeport will document all instances where consent is obtained and ensure that these are formally managed to comply with the data subject's rights.

Breach management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

It is the responsibility of all employees to report any suspected data breach to the Data Protection Officer.

The Freeport will ensure that the SIRO and the Information Commissioner are informed immediately of any breach that meets the criteria for escalation.

Data Protection Impact Assessment (DPIA)

The Freeport will ensure that an individual's rights in relation to privacy and data protection are a key consideration in the development and life cycle of any new project, process or policy.
The Freeport will implement appropriate technical and organisational measures to ensure it has integrated privacy and data protection into our processing activities.

The Freeport will conduct a mandatory Data Protection Impact Assessment

- Where the processing of personal data is likely to result in high risk to the rights and freedoms of individuals.
- When new technologies are being implemented to process personal information.
- When new processes are being implemented to manually process personal information.

All Data Protection Impact Assessments will be conducted by the Data Protection Officer and signed off by the SIRO. Data Protection Impact Assessments will be made available to the Information Commissioner's Office on request.

Suppliers and partners

Where an organisation processes personal data for the Freeport, the Freeport will ensure that its contract with that organisation contains clauses in which the supplier or partner guarantees that they will process that data in accordance with Data Protection legislation.

Any contract with any organisation that processes personal data for the Freeport must set out:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.

- The type of personal data and categories of data subject; and
- The obligations and rights of the controller.

Any contract with any organisation that processes personal data for the Freeport must also include as a minimum the following terms, requiring the data processor (i.e. the partner organisation) to:

- Only act on the written instructions of the Freeport.
- Ensure that people processing the data are subject to a duty of confidence.
- Take appropriate measures to ensure the security of processing.
- Only engage sub-processors with the prior consent of the controller and under a written contract.
- Assist the Freeport in providing subject access and allowing data subjects to exercise their rights.
- Assist the Freeport in meeting its Data Protection Act obligations.
- To delete or return all personal data to the Freeport as requested at the end of the contract.
- Submit to audits and inspections.

A supplier or partner cannot enlist or change a sub-processor without the consent of the Freeport or, where general consent has already been given, without notifying the Freeport in advance.

Any organisation that processes personal data for the Freeport must have Information Asset Registers with mapped data flows.

The Freeport will pass on a copy of the relevant section within its own Information Asset Register.

Any organisation that processes personal data for the Freeport must have an approved breach management process, including clauses requiring appropriate escalation to the Freeport and the Information Commissioner as soon as a breach becomes known.

Privacy notices

The Freeport will ensure that privacy notices are displayed at the point of collection of any information, both physical and electronic.

Audit trails

The Freeport will ensure that all IT systems that process personal data will have audit trails which keep a log of the following activities:

- Additions of personal records
- Changes to personal records
- Deletions of personal records

The audit trails must have their integrity protected by technical controls and must be kept for a minimum of 12 months. The Freeport must make the audit trails available to the Information Commissioner on request.

Information security

The Freeport will apply appropriate security measures to protect the data it controls.

Complaints

Any complaint or concern expressed by an individual in connection with the Data Protection Act must be reported to the Data Protection Officer immediately. The Data Protection Officer will investigate the complaint and take the appropriate action. If a compensation payment is requested for

a breach of the Data Protection Act legislation, this will be dealt with by the Senior Information Risk Officer (SIRO).

There are several ways to contact the Data Protection Officer or to raise a complaint regarding Data Protection:

Email – complaints@pasdfreeport.com

Or in writing to: -

Data Protection Officer
Plymouth and South Devon Freeport
Suite 8
Endeavour House,
2 Vivid Approach
Plymouth
PL1 4RW

1. Data Protection Complaint Resolution – Stage 1

We will provide a written response to formal complaints within 10 working days of receiving the complaint. The response will say whether the complaint is upheld and the action we propose to take to resolve it. If the complaint is not upheld the response will set out the steps the complainant can take if they remain unsatisfied.

2. Investigating the Complaint

The Data Protection Officer will investigate the complaint.

3. Data Protection Complaint resolution – Stage 2

If the complainant is not happy with our stage 1 response, our decision will be reviewed by the Freeport Chief Executive Officer.

4. Decision Letter (Final Response)

Following investigation of a stage 2 complaint the Freeport CEO will write to the complainant setting out their decision which will be final. If the complaint is upheld, it will set out the action we propose to take to resolve it.

Complaint recording

PASD Freeport will maintain a record of all formal Data Protection complaints received including details of the complainant, brief details of the complaint, the stage it reached and any action we have promised to take to resolve it. Any personal details will be held in accordance with our Data Protection Policy.

Complaint reporting

The register of complaints will be reviewed annually to assess the number of complaints received, the number that were upheld and understand any patterns to inform improvements.

Responsibilities

The Freeport Operations Director will be responsible for the operation of the Data Protection Complaints Procedure. The Freeport Chief Executive Officer will be accountable to the Board of Directors for any Data Protection Complaints.

Appendix A: Safeguards in relation to processing of Special Category Data

PASD Freeport recognises its obligations to comply with the requirements laid down in the General Data Protection Regulation and the Data Protection Act 2018.

As part of the Freeport's statutory and corporate functions, we may process Special Category Data and Criminal Conviction Data. In accordance with Schedule 1 Part 4 of the Data Protection Act, this document, explains how the Freeport complies with the Data Protection Principles when processing Special Category Data and Criminal Conviction data and also the Freeport's policy in relation to the retention and erasure of this information.

A1 What is Data Processing?

The GDPR defines this as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

A2 What is Special Category Data?

The GDPR defines this as 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.

A3 What is Criminal Conviction Data?

The GDPR defines this as personal data relating to criminal convictions and offences or related security measures. The Data Protection Act adds that this also includes allegations of the commission of offences, criminal proceedings and sentencing.

A4 The scope of data processing which is subject to this Policy as set out in the Data Protection Act

- Sch. 1, Part 1, para. 1: Employment, social security, and social protection.
- Sch. 1, Part 2, para. 6: Statutory etc. and government purposes.
- Sch.1, Part 2, para. 7: Administration of justice.
- Sch. 1, Part 2, para. 8: Equality of opportunity or treatment.
- Sch. 1, Part 2, para. 9: Racial and ethnic diversity at senior levels of organisations
- Sch. 1, Part 2, para. 10: Preventing or detecting unlawful acts.
- Sch. 1, Part 2, para. 11: Protecting the public against dishonesty
- Sch. 1, Part 2, para. 12: Regulatory requirements relating to unlawful acts and dishonesty etc.
- Sch. 1, Part 2, para. 14: Preventing fraud.
- Sch. 1, Part 2, para. 18: Safeguarding children and of individuals at risk.
- Sch. 1, Part 2, para.19: Safeguarding of economic well-being of certain individuals.
- Sch. 1, Part 2, para. 21: Occupational pensions
- Sch. 1, Part 2, para. 24: Disclosure to elected representatives

A5 Procedures for securing compliance with the Data Protection Principles in relation to the processing of Special Category and Criminal Conviction Data

Principle 1- Lawfulness, Fairness and Transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

PASD Freeport will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful.
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent.

Principle 2 - Purpose Limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

PASD Freeport will:

- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in an appropriate privacy notice.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose, that is compatible, we will inform the data subject first.

Principle 3 - Data Minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

PASD Freeport will only collect personal data necessary for the relevant purpose and ensure it is not excessive. We will only process information necessary for and proportionate to our purposes. Where personal that is not relevant to our stated purposes data is provided to, or obtained by us, we will erase it.

Principle 4 - Accuracy
Personal data shall be accurate and, where necessary, kept up to date.
PASD Freeport will ensure that the personal data we hold is accurate and kept up to date as necessary. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that it is erased or rectified without delay. If we decide not to either erase or rectify it, we will document our decision.

Principle 5 - Storage Limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
PASD Freeport will only keep personal data in identifiable form as long as is necessary, for the purposes for which it is collected. When information is no longer in use it is retained only for the periods set out in our corporate retention schedule. These periods are determined variously by the needs of the business, relevant legislative and regulatory requirements and the requirements or guidelines of the National Archives.

Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

Principle 6 - Integrity and Confidentiality
Personal data shall be 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 technical or organisational measures.

PASD Freeport will ensure that there are appropriate organisational and technical measures in place to protect personal data.

Electronic information is processed within systems which have been subjected to robust Data Protection Impact Assessments.

- Hard copy information is processed within our secure premises.
- Our electronic systems and physical storage have appropriate access controls applied.
- The systems we use to process personal data allow us to erase or update personal data at any point in time.

Principle 7 - The Accountability Principle

The controller shall be responsible for, and be able to demonstrate, compliance with these principles.

PASD Freeport will:

- ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.
- carry out a Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the Freeport's personal data handling, and that this person has access to report to the highest management level of the Freeport.
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with Data Protection Law

A6 Data Controller's policies in relation to the Retention and Erasure of Personal Data

Where special category or criminal convictions personal data is processed, the Freeport will ensure that:-

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous.
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.