

Jersey Heritage

Data Protection Policy

January 2023

Purpose

We are committed to being transparent about how we collect and use the personal data of our workforce, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data. Jersey Heritage is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy policy.

This policy applies to the personal data of job applicants, employees, contractors, volunteers and former employees, referred to as HR-related personal data.

The Director of Finance and Operations has been appointed as the person with responsibility for data protection compliance. Questions about this policy, or requests for further information, should be directed to them.

Definitions

"Personal Data" is any information that relates to an individual who can be identified from that information. It does not include anonymous data or data that has had the identity of an individual permanently removed.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

"Special Category Data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal Records Data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

We process HR-related personal data in accordance with the following data protection principles:

- Personal Data is processed lawfully, fairly and in a transparent manner;
- Personal Data is collected only for specified, explicit and legitimate purposes;
- Personal Data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- Personal Data is kept accurate and all reasonable steps are taken to ensure that inaccurate Personal Data is rectified or deleted without delay;
- Personal Data is kept only for the period necessary for processing; and
- appropriate measures are adopted to make sure that Personal Data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We tell you the reasons for processing your Personal Data, how we use your Personal Data and the legal basis for processing in our privacy notices. Your Personal Data will not be processed for other reasons.

Where we process Special Category Data or Criminal Records Data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on Special Category Data and Criminal Records Data.

We will update HR-related Personal Data promptly if you advise that your information has changed or is inaccurate.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees or volunteers).

Personal data gathered during the employment, contractor or volunteer relationship is held in your personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which we hold HR-related Personal Data is contained in Jersey Heritage's privacy notices to individuals.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the Data Protection (Jersey) Law 2018.

Individual rights

As a data subject, you have a number of rights in relation to your Personal Data.

Subject access requests

You have the right to make a subject access request. If an individual makes a subject access request, we will tell you:

- whether or not we process your Personal Data and if so why, the categories of Personal Data concerned and the source of the data if it is not collected from the individual;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your Personal Data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Jersey Office of the Information Commissioner if you think we have failed to comply with your data protection rights; and
- whether or not we carry out automated decision-making and the logic involved in any such decision-making.

We will also provide you with a copy of the Personal Data undergoing Processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

To make a subject access request, you should send the request to the Director of Finance and Operations. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within a period of 4 weeks from the date it is received. In some cases, such as where we process large amounts of your data, we may extend our response time by a further 8 weeks from. We will write to you within 4 weeks of receiving the original request to tell you if this is the case.

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your Personal Data. You can require us to:

- rectify inaccurate data;
- stop Processing or erase data that is no longer necessary for the purposes of Processing;
- stop Processing or erase data if your interests override Jersey Heritage's legitimate grounds for Processing data (where Jersey Heritage relies on its legitimate interests as a reason for Processing data);
- stop Processing or erase data if Processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override Jersey Heritage's legitimate grounds for processing data.

To ask us to take any of these steps, you should send the request to HR who will notify the Director of Finance and Operations.

In the limited circumstances where you may have provided your consent to the collection, Processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact HR who will notify the Director of Finance and Operations. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data security

We take the security of HR-related Personal Data seriously. We have internal policies and controls in place to protect Personal Data against loss, accidental destruction, misuse or disclosure, and to ensure that Personal Data is not accessed, except by employees in the proper performance of their duties.

Where we engage third parties to Process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical measures to ensure the security of your Personal Data.

Data breaches

If we discover that there has been a breach of HR-related Personal Data that poses a risk to the rights and freedoms of individuals, we will report it to the Jersey Office of the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of if they need to be reported to the Jersey Office of the Information Commissioner.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

We foresee no requirement to transfer your Personal Data outside of Jersey and the EEA. Should a requirement arise, we will seek your written consent in advance.

Individual responsibilities

You are responsible for helping us keep your Personal Data up to date. You should let us know if data provided to us changes, for example, if you move house or change your bank details.

You may have access to the Personal Data of other individuals and of our customers and clients in the course of your employment, contract/volunteer period. Where this is the case, we rely on you to help meet our data protection obligations to staff and to customers and clients.

Individuals who have access to Personal Data, are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside Jersey Heritage) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove Personal Data, or devices containing or that can be used to access Personal Data, from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store Personal Data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

We will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to Personal Data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Change of purpose

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, where this is required or permitted by law.

Changes to our data protection policy

We reserve the right to update this privacy policy at any time, and we will provide you with a new privacy policy when we make any substantial updates. We may also notify you in other ways from time to time about the Processing of your Personal Data.

Extract from Jersey Heritage Staff Handbook – May 2021