DATA PROTECTION POLICY 2024

CONSULTATION DRAFT V3.2.0

1 Introduction

1.1 Background

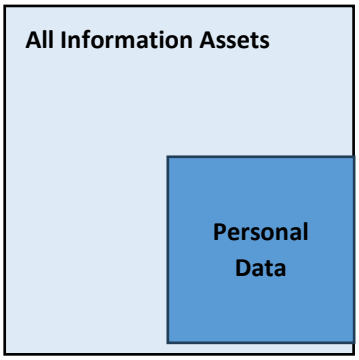
This document sets out St Helena's policy on data protection.

The scope of this data protection policy applies to the processing of personal data on St Helena by both public and private sector organisations.

This differs from information security which is a comprehensive approach to safeguarding all types of information assets by preserving their confidentiality, availability, and integrity.

Data protection is a subset of that information, and specifically focuses on personal data. Data protection can therefore be described as the process of safeguarding personal or private information from damage, loss, or misuse and is concerned with its appropriate and lawful management, processing, storage, and destruction.

"Personal data" as subset of "information" is represented by the graphic below:



At present, no local data protection legislation is enacted on St Helena and the need for both Data Protection (DP) and Freedom of Information (FOI) legislation on St Helena has been discussed at length for some time.

In September 2014, The St Helena Government (SHG) launched the Code of Practice for Public Access to SHG Information which formed the basis of the Public Access to Government Information Ordinance 2021, which is still to be brought into force. This Ordinance was seen as a stepping stone towards FOI legislation; however, the Ordinance is not tasked with providing appropriate wider coverage for the protection of privacy.

Globally, 137 out of 195 (70%) of countries have enacted legislation to secure the protection of data and privacy. This legislation has included recognising privacy within constitutions or within other specific legal provisions.

The St Helena Constitution outlines 16 rights, each referred to as clauses. Each of these clauses are individually appropriated from the European Convention on Human Rights. Specifically, "Clause 13", provides the right to private and family life and for privacy of home and other property.

In other countries, such as the United Kingdom, privacy is not only an individual right but is also seen as a social value. Human dignity is recognised as an absolute fundamental right and in this notion of

dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role.

By formally implementing a policy on data protection in St Helena, we can further protect the privacy of individuals, particularly in light of improved global connectivity and digital advancements. Organisations will have the opportunity to demonstrate trustworthy data practices and alignment to international privacy laws.

1.2 Identification of the Problem, Challenge or Opportunity

1. **Problems**

- Loss of Control
  The implementation of quick, and affordable internet for all is a significant improvement for both residents, and the private and public sector organisations of St Helena, connecting them and their personal data on a global scale.

  Currently, there is no policy or legislation on St Helena to support or safeguard the protection of personal data in what will fast become a digitally connected island with the rest of the world.

  Furthermore, from the individual's perspective, there is a wider "global" feeling that due to technology and the widespread capture and sharing of digital information, individuals are losing control over their personal data. With increasingly powerful data collection and analysis tools, many private and public sector organisations collect all the information they can (often much more than they need) and are not transparent or forthcoming in informing individuals just how much information they have or what they're doing with it. Where there is a distinct lack of safeguards this can lead to manipulation or adverse treatment of individuals.

  The right to privacy and data protection is a right that may impact the effectiveness of other fundamental rights, such as freedom of speech, freedom of thought or freedom of assembly.

  Privacy legislation can restrict government and law enforcement agencies from easily accessing private residents' information to use in unwarranted invasions (hence, the necessity for a warrant before collecting personal data).

- Social Boundaries
  Individuals naturally establish boundaries from others in society and these boundaries can be both a physical and a digital/ informational nature. Given the rise of digital environments, and the improvements in internet connectivity for all on St Helena, individuals will need places of solitude to retreat to, places where they are all free of the "gaze" of others.

  Privacy legislation helps people manage these boundaries and breaches of these boundaries can create awkward social situations and significantly damage our relationships.

  Privacy is about respecting individuals. If a person has a reasonable desire to keep something private, it is disrespectful to ignore that person's wishes without a compelling reason to do so. Even if this doesn't cause major injury, it demonstrates a

lack of respect for that person. In a sense it is saying: “I care about my interests, but I don’t care about yours.”

Privacy is also helpful to reduce the social friction we encounter in life. Most people don’t want everybody to know everything about them – hence the phrase “none of your business.” And sometimes they don’t want to know everything about other people — hence the phrase “too much information.”

- International Trade and Cloud Technologies

  Cloud computing technology gives end users access to storage, files, software, and servers through their internet-connected devices: computers, smartphones, tablets, and wearables. Cloud computing providers store and process data in a location over the internet that’s separate from end users.

  This means businesses of any size can harness powerful software and IT infrastructure to become bigger, leaner, and more agile, as well as compete with much larger companies.

  Unlike with traditional hardware and software, cloud computing helps businesses stay at the forefront of technology without having to make large investments in purchasing, maintaining, and servicing equipment themselves.

  The security of personal data transferred across national borders has been one of the drivers for international consensus on the fundamental principles for the protection of personal data. For example, the principle articulated in the OECD Privacy Framework (OECD 2013) regarding transborder flows of personal data is that a data controller “remains accountable for personal data under its control without regard to the location of the data” (adopted in 1980 and revised in 2013, Article 17).

  Where organisations on St Helena wish to provide digital services to the UK or EU, they will also be bound by the EU and/or UK GDPR. However, due to uncertainty regarding data protection standards in foreign countries, many countries limit extraterritorial transfer of personal data. Such transfers may be permitted in certain circumstances or when the data protection standards in a third country are deemed adequate. For St Helena, without an aligned data protection law, this would present a barrier to entry into the EU/ UK digital markets given the significant burden of compliance, where organisations within St Helena are not already aligned.

- Private Sector

  The absence of data protection law on the island can potentially be advantageous to attracting private sector organisations, as they are not lawfully required to be held to account for how they collect, use, process and store individual’s information. The problem with this is that St Helena may then be viewed as a territory where “dirty” data processing takes place without any controls to protect those individuals and would potentially be a risk from a reputational perspective.

  Conversely, where a significantly or strict policy and legislation is introduced around data protection, it may also discourage some international organisations from wanting to trade digitally in St Helena due to more stringent local laws, which may not be aligned to how they are already operating. In simple terms, St Helena may introduce a law that is stronger than what would be deemed as a global standard in the GDPR and would then create a further barrier to entry into St Helena.

2. Challenges

- Regulator Independence
  Data protection and privacy in general are often subject to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including the protection of individuals' rights. This supervisory body might be a single government official, ombudsman or a body with several members.

  Genuine independence of such an authority is a key factor, with independence being measured by structural factors such as the composition of the authority, the method of appointment of members, the power and timeframe for exercising oversight functions, the allocation of sufficient resources and the ability to make meaningful decisions without external interference.

  The supervisory authority may handle public complaints, even though every individual whose data is collected may also have recourse to an external binding legal process and ultimately the courts on matters of law. In terms of remedies, the authority may have the power to oblige both private and public sector organisations to rectify, delete or destroy inaccurate or illegally collected personal data.

- Existing and Outdated Technology
  Many institutions, in both public and private sectors, may have difficulty identifying all systems that store information and deploying appropriate controls for them.

  This is particularly hard in legacy environments where the original technologists have moved on, and poor documentation makes governance hard to implement.

  It may be that legacy systems and software cannot support the processes required to support lawful processing of data and data subject rights requests that are made. Consideration would need to be made around the risk these systems present vs the costs of compliance.

- Cost of Compliance
  The cost of both private and public sector organisations to implement any new privacy controls will be significant. This will require improvements to be made to people, processes and technology.

  There will be underlying requirements to scrutinise current processes and then make and implement new/ improved controls and processes, whilst ensuring that employees have appropriate levels of awareness to work within legal boundaries.

  These significant improvements will require appropriate investment and resources to be made available by both public and private sector organisations. For example, the costs of achieving an appropriate level of compliance may range from hundreds of pounds for micro enterprises to thousands of pounds for enterprises with over 50 employees.

- Raising Public Awareness
  From having no formal data protection policy or legislation on the island of St Helena, to implementing and maintaining a stronger position on privacy will require

several varying levels of awareness. This awareness is required to cover the following areas:

- Individuals
- Public Organisations
- Private Organisations

For privacy legislation to work as intended on the island, it will require individuals to understand their rights to ensure there are appropriate and understood expectations on how their data is processed. This may require workshop sessions and wider awareness campaigns through varying different channels and mechanisms prior to implementation.

It will also require organisations to understand the "rules" that will govern them and for appropriate and adequate support to be provided to them before, during and after implementation. There may want to be sector focused workshops or tailored information provided. This could include: Health, Education, Law Enforcement, Judicial, Insurance, Hospitality, Technology businesses.

3. Opportunities

- International Data Transfers
  'Adequacy' is a term that the EU use to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU.

  An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector, or international organisation provides an equivalent level of protection for personal data as the EU does.

  The effect of such a decision is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In other words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

  The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and Uruguay as providing adequate protection.

  Where St Helena can align to those standards of legislation and achieve a favourable adequacy decision, it would lead to the free flow of personal data without the need for additional "red tape" opening up significant trade opportunities on a global scale. This will naturally attract investment opportunities in St Helena opening up digital global markets.

- Drive international commerce, trade, and development.
  The above international data transfers underpin modern day business transactions. They help streamline supply chain management and allow organisations to scale and trade globally. This coupled with the implementation of the data cable will attract both inward and local investment on the Island.

- Positioning and reputational advantage.
  Organisations can boost their reputations and win new customers by positioning themselves as guardians of customer data and dependable sources of information about digital identity and data privacy. Some companies have even used their data policies to take on competitors directly, pointing out to customers that their rivals haven't implemented data safeguards comparable to their own.

  Individuals deserve and expect to have awareness of and control over how their personal information is collected/shared/tracked, in-person and online.

  Data is becoming more and more valuable. Also, skills and opportunities for retrieving different types of personal data are evolving extremely fast. Unauthorised, careless or ignorant processing of personal data can cause great harm to persons and to companies.

  Data protection regulations are necessary for ensuring fair and consumer friendly commerce and provision of services. Personal data protection regulations cause a situation, where, for example, personal data can't be sold freely which means that people have a greater control over who makes them offers and what kind of offers they make. This could also attract investment opportunities through the trust that is built between data processor and the consumer.

  If personal data is leaked, it can cause companies significant damage to their reputation and bring along penalties, which is why it's important to comply with the personal data protection regulations. This in turn encourages all organisations to improve their data protection maturity across sectors. Data protection laws ensure that there exists legal recourse for consumers to fight back against violations of those privacy rights.

- Prevention of Fraud and Cyber Crime
  Where a private or public sector organisation applies strong data protection measures and safeguards, they not only protect individuals' or customers' personal data, but protect their own organisation's data too. Therefore, avoiding considerable problems, which may damage their reputation or put at risk their organisations' confidential information.

- Building Trust with Data Subjects
  Whilst regulations like GDPR are giving consumers more authority over the acquisition and use of their data, companies shouldn't stop at what's legally required. For example, if an organisation provides any sort of social platform, and offers privacy settings that give individuals full control over who sees their content and who doesn't, private sharing and storage options and flexible but secure account controls. When you consistently prove that you value their privacy, they'll reward you with their trust and loyalty.

  Individuals whose data you process should also be part of an ongoing conversation about how their data is collected and used. Most individuals are willing to provide their personal information if they get something in return. But if they feel like they can't trust you, this arrangement won't last for long.

1.3 Policy Rationale

The strategic goal for the Island of St Helena is to enact a Data Protection Ordinance to protect the rights and freedoms of individuals whose data is processed by both public and private organisations, locally and internationally.

To ensure that international data protection adequacy is considered and baked into policy and legislative wording for future harmonious global data flows.

At present, there are certain limited circumstances where the SHG and some private organisations must comply with the requirements as set out in the UK and EU GDPR. This Policy aims to also align working practices on St Helena to those core standards and legislative requirements.

St Helena should consider taking a stepped approach to implementing any agreed Data Protection Ordinance to ensure that both public and private sector organisations can ensure they meet its requirements appropriately without the major immediate impact.

2 OVERARCHING POLICY FRAMEWORK

2.1 Strategic Objectives

St Helena Government Vision and Strategy April 2022 – March 2025
Specifically in respect of being "Effective, Efficient and Accountable Public Sector". Where there is a commitment to:

"Ensuring SHG information is properly managed with supporting policies and systems in place. We will ensure that SHG's openness and transparency agenda is further enhanced and underpinned by Data Protection legislation."

Furthermore, the strategic objectives are aligned to St Helena's Digital Strategy and St Helena's Digital Transformation Agenda.

Sustainable Economic Development Strategy 2023-2033 objectives:

a) An open and accessible island –Open and accessible for people and culture, capital and finance
   - Open to business and capital
   - Stable and predictable air and sea access and connectivity
   - Connected, globally

Ministerial priorities, 2024/25

1) Expertise to support the delivery of a financial services sector on the Island with a focus on five key areas:
   - Development of a Beneficial Ownership Register
   - Modernisation of the Bank of St Helena
   - Reform of Financial Services Laws and Regulations
   - Legal Recognition of Decentralised Autonomous Organisations; and

- Reform of Company Law (to include looking at developing the companies' registry in particular to focus on those that have high environmental, social and governance (ESG) values).

2) Creating a business enabling environment
   - Access
   - Telecoms
   - Efficient/effective engagement with SHG

2.2 Policy Objectives and Principles

Strategic Objectives:

1. To increase the public's trust and confidence in how data is used and processed on St Helena.

2. To strengthen transparency and accountability and promote good information governance.

3. To protect the residents of St Helena in a digital world.

4. To stay relevant, become an attractive country for digital commerce, provide an excellent public service and keep abreast of evolving technology.

To do this, this policy will ensure the following:

- Protection of the rights and freedoms of those data subjects whose data is collected and/or processed on the Island of St Helena.

- Development, implementation and annual review of policies governing the collection, processing and secure disposal of personal data on St Helena to ensure accountability for the protection of personal data when it is being processed.

- Collection, processing and storage of personal data where there is a well-founded lawful basis for doing so.

- Monitoring all data processing practices to ensure that work is done in accordance with EU and/or UK data protection legislation where applicable.

- Demonstration of accountability for processing activities by maintaining records of processing activities.

- Data protection and information governance training is provided, on induction and refreshed regularly so that all public and private organisation are aware of their responsibilities and obligations regarding the processing of personal data.

- Demonstration of transparency with data subjects whose data is processed by all organisations so that they feel confident in providing their personal data.

2.3 Scope

This policy applies to all functions and activities undertaken by SHG itself and to support the private and NGO sectors that involve the use and processing of personal data.

3 POLICY OUTLINE

Public and private organisations, as well as NGOs have a responsibility to ensure that the personal data, collected and/or processed, is treated with respect, always kept secure and confidential, and any applicable data protection legislation is complied with.

It is of paramount importance that information, including personal data, is efficiently managed; that appropriate accountability, standards, policies and procedures provide a robust governance framework for wider information management in SHG, and in the private and NGO sectors.

The following policy framework provides for appropriate coverage.

a) Definitions

a. Controller - A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

b. Data Protection Officer - Some organisations need to appoint a Data Protection Officer (DPO) who is responsible for informing them of and advising them about their data protection obligations and monitoring their compliance with them.

c. Data Subject - The identified or identifiable living individual to whom personal data relates.

d. Personal Data - Any information relating to a person (a 'data subject') 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 person.

e. Processing - In relation to personal data, means 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, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

f. Processor - A person, public authority, agency or other body which processes personal data on behalf of the controller.

b) Key Principles

Key principles lie at the heart of any data protection framework/ legislation and they both directly and indirectly influence the other rules and obligations found throughout data protection legislation. Therefore, compliance with these fundamental principles of data protection is the first step for data controllers in ensuring that they fulfil their obligations under the respective law.

- **Lawfulness, fairness, and transparency**
  Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

- **Purpose Limitation**
  Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes.

- **Data Minimisation**
  Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

- **Accuracy**
  Data Controllers, responsible for processing personal data, must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, Data Controllers should accurately record information they collect or receive and the source of that information.

- **Storage Limitation**
  Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

- **Integrity and Confidentiality**
  Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  Finally, the Data Controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Data Controllers must take responsibility for their processing of personal data and be able to demonstrate (through appropriate records and measures) their compliance, in

particular to the Regulator (when in place where an Ordinance is enacted on Data Protection).

c) Lawful Basis for Processing

Prior to processing any personal data, organisations operating in St Helena will always identify and establish the lawful basis. These organisations will not process personal data unless one of the following grounds for processing have been met:

Personal Data

- **Consent** – The data subject has provided their consent to process their personal data for one or more specified purposes.

- **Performance of a Contract** – Processing is necessary for the performance of a contract to which the data subject is a party to.

- **Legal Obligation** – Processing is necessary for compliance with a legal obligation to which the data controllers are subject.

- **Vital Interests** – Processing is necessary to protect the vital interests (life or death situation) of the data subject or of another natural person.

- **Public Task** – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

- **Legitimate Interests** – Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third-party.

Special Category Personal Data

- Explicit consent.
- Employment, social security and social protection (if authorised by law).
- Vital interests.
- Not-for-profit bodies.
- Made public by the data subject.
- Legal claims or judicial acts.
- Reasons of substantial public interest (with a basis in law).
    - Statutory and government purposes
    - Administration of justice and parliamentary purposes
    - Equality of opportunity or treatment
    - Racial and ethnic diversity at senior levels
    - Preventing or detecting unlawful acts
    - Protecting the public
    - Regulatory requirements
    - Journalism, academia, art and literature
    - Preventing fraud
    - Suspicion of terrorist financing or money laundering
    - Support for individuals with a particular disability or medical condition
    - Counselling
    - Safeguarding of children and individuals at risk
    - Safeguarding of economic well-being of certain individuals
    - Insurance

    - Occupational pensions
    - Political parties
    - Elected representatives responding to requests
    - Disclosure to elected representatives
    - Informing elected representatives about prisoners
    - Publication of legal judgments
    - Anti-doping in sport
    - Standards of behaviour in sport
- Health or social care (with a basis in law).
- Public health (with a basis in law).
- Archiving, research and statistics (with a basis in law).

d) Consent

Where processing activities rely on consent, organisations will ensure that consent is collected; that consent must be:

- **Freely given** – the data subject must have a genuine choice, and where there is an imbalance of power between the data controller and the data subject (i.e. employer and employee), consent cannot be considered freely given.

- **Specific** – the data controller must explain its purpose(s) for processing the personal data so that the data subject can consent to the purpose(s) specifically.

- **Informed** – the data subject must be given all the necessary information concerning the processing activity so that they can comprehend how the processing might affect them (privacy notice).

- **An unambiguous indication** – the data subject's statement or clear affirmative action must leave no doubt as to their intention to provide us with their consent.

It will be necessary for auditable records to be maintained when consent has been relied upon for processing personal data. All organisations should always be able demonstrate that consent has been provided.

It will be necessary to ensure that there are easy measures in place for when a data subject wishes to withdraw their consent.

e) Legitimate Interests

Where organisations rely on legitimate interests as a lawful basis for processing personal data, they will be transparent about what their legitimate interests are. Public facing Privacy Notice(s) will display what processing activities rely on legitimate interests and will justify what those legitimate interests are.

All organisations will be required to take into consideration how data subjects may reasonably expect them to use their personal data, and they will cease to process the personal data where the data subject's legitimate interests override their own. They will assess the use of legitimate interests by completing a Legitimate Interest Assessment (LIA).

f) Data Subject Rights

Data subjects are provided with enhanced rights in relation to their personal data that SHG and both private organisations and NGOs hold about them. It will be a priority to ensure that these rights are upheld within all organisations. Aligned to the UK and EU GDPR, data subjects have the following rights:

- **The right to be informed –** Covers some of the key transparency requirements and is about providing individuals with clear and concise information about what you do with their personal data.

- **The right to access –** Commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

- **The right to rectification –** The right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

- **The right to erasure –** This is also known as the 'right to be forgotten'. The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

- **The right to restriction of processing –** Request to restrict processing personal data within the organisation, but this is only applicable in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

- **The right to data portability –** Gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

- **The right to object to processing –** This effectively allows individuals to stop or prevent you from processing their personal data. An objection may be in relation to all of the personal data you hold about an individual or only to certain information. It may also only relate to a particular purpose you are processing the data for.

g) Privacy Notices

When processing personal data, organisations will ensure that they have provided the data subject with a sufficient privacy notice, which includes the following information:

- **The name and contact details of the Data Controller –** Say who you are and how individuals can contact you.

- **The purposes of processing –** Explain why you use people's personal data. Be clear about each different purpose. There are many different reasons for using personal data, you will know best the particular reasons why you use data. Typical purposes could include marketing, order processing and staff administration.

- **The lawful basis for the processing –** Explain which lawful basis you are relying on in order to collect and use people's personal data and/or special category data.

- **The legitimate interests for the processing –** Explain what the legitimate interests for processing are, if they are relied upon as a lawful basis.

- **The recipients, or categories of recipients of the personal data –** Clearly outline who you share data subject's personal data with. This includes anyone that processes the personal data on your behalf, as well all other organisations. You can tell people the names of the organisations or the categories that they fall within. Be as specific as possible if you only tell people the categories of organisations.

- **The details of any transfers of the personal data to overseas –** Tell people if you transfer their personal data to any countries or organisations outside St Helena.

- **Retention periods for personal data –** Say how long you will keep the personal data for. If you don't have a specific retention period then you need to tell people the criteria you use to decide how long you will keep their information.

- **The rights available to individuals in respect of the processing –** Tell people which rights they have in relation to your use of their personal data, e.g. access, rectification, erasure, restriction, objection, and data portability. The rights will differ depending on the lawful basis for processing – make sure what you tell people accurately reflects this. The right to object must be explicitly brought to people's attention clearly and separately from any other information.

- **The right to withdraw consent** – Where consent is relied upon, let people know that they can withdraw their consent for your processing of their personal data at any time. Consent must be as easy to withdraw as it is to give. Tell people how they can do this.

- **The right to lodge a complaint with the regulator –** Tell people that they can complain to a regulator. Individuals have the right to raise a complaint with the regulator where they live, where they work, or where the infringement took place. It is good practice to provide the name and contact details of the regulator that individuals are most likely to complain to if they have a problem.

- **The details of whether individuals are under a statutory or contractual obligation to provide the personal data –** Tell people if they are required by law, or under contract, to provide personal data to you, and what will happen if they don't provide that data. Often, this will only apply to some, and not all, of the information being collected. You should be clear with individuals about the specific types of personal data that are required under a statutory or contractual obligation.

- **The details of the existence of automated decision-making, including profiling –** Say whether you make decisions based solely on automated processing, including profiling, that have legal or similarly significant effects on individuals. Give people meaningful information about the logic involved in the process and explain the significance and envisaged consequences. Whilst this type of processing may be complex, you should use simple, understandable terms to explain the rationale

behind your decisions and how they might affect individuals. Tell people what information you use, why it is relevant and what the likely impact is going to be.

Where the personal data has not been collected directly from the data subject, organisations will ensure that the data subject is also informed about the source used to obtain their personal data.

Fair processing information will be contained within privacy notices and organisations will take every step to ensure that the information displayed within their privacy notices is:

- Concise;
- Transparent;
- Intelligible;
- Easily accessible; and
- Written using clear, plain language.

h) Data Retention

In accordance with the storage limitation principle, individual's personal data will not be kept for longer than necessary by organisations. Specified retention periods and disposal methods for all categories of personal data will need to be in place and documented.

i) Data Protection by Design

Organisations should operate a 'Data Protection by Design' approach. This means that when they begin a new project or processing activity, they put privacy at the forefront of the design.

This approach means that:

- Organisations can identify any issues and mitigating measures to perform to reduce the risks before they become a concern within their processing activities;

- Organisations' employees need to be knowledgeable of how to appropriately manage the personal data processed within their respective organisation;

- Organisations can demonstrate how their processing activities operate with privacy in mind in accordance with the accountability principle; and

- By putting privacy at the forefront, organisations' processing activities are less likely to have a negative impact on the data subjects with whom they deal.

- By utilising a Data Protection by Design approach, organisations will be required to use certain technical and organisational measures to protect the personal data that they process, this involves the following:

    - **Pseudonymisation** - The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual;

- **Encryption** - The process of encoding information. This process converts the original information, known as plaintext, into an alternative form known as ciphertext. Only authorised parties can decipher a ciphertext back to plaintext using a key (password) and access the original information;

- **Data minimisation** - Limiting the collection or processing of personal data to what is directly relevant and necessary to accomplish a specified purpose;

- **Restriction** - To ensure the correct access to the correct information and resources by the correct people; and

An organisation's Information security and cyber security processes and protocols should provide more detailed information about the measures and controls taken to protect personal data and to ensure its security from the time it is collected (or received) to its disposal.

j) Data Protection Impact Assessments

A Data Protection Impact Assessment is a risk assessment that focusses on privacy and is utilised as a tool to identify risks and mitigating measures prior to the implementation or changes to a project or processing activity.

Performing a DPIA helps to determine the possible impact to the rights and freedoms of affected data subjects when considering a new processing activity.

k) Personal Data Breach Management

A Personal Data Breach is an event or action that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. All personal data breaches regardless of the severity of the breach need to be reported to the nominated individual responsible for Data Protection, as soon as practically possible.

Where this breach presents a risk to the individuals concerned, the regulator should be notified within 72 hours.

Where, this breach presents a high risk to individuals, the regulator should be notified within 72 hours and the data subjects informed without undue delay so that they can take appropriate action to protect themselves.

--- END OF DOCUMENT ---