GOVERNMENT OF BERMUDA
Ministry of Finance Headquarters

(the "MOF")

Personal Information Protection Policy

Introduction

The Bermuda **Personal Information Protection Act 2016** ("**PIPA**" or the "**Act**"), related regulations and guidance notes control the way all personal information is held and used. This policy describes how personal information must be collected, handled, stored, disclosed and otherwise used to meet the MOF's information protection standards and to comply with the Act.

Definitions of the terms "**personal information**" and "**use**" are set out in clauses 0 and 0 below entitled '*Personal information*' and '*Using personal information*' respectively.

The Act does not apply to personal information in the following circumstances:

a) where it is used for personal or domestic purposes;

b) where it is used for artistic, literary or journalistic purposes with a view to publication in the public interest so far as it is necessary to protect the freedom of expression;

c) where it is used in business for the purpose of contacting an individual (being a person to whom personal information relates) in his capacity as an employee or official of an organisation;

d) where an individual has been deceased for at least 20 years;

e) where an individual has been in existence for at least 150 years;

f) to the transfer of personal information to an archival institution where access to the personal information was unrestricted or governed by an agreement between the archival institution and the donor of the personal information prior to the implementation of the Act; and

g) where personal information is used for judicial purposes or by members of the House of Assembly or the Senate in Bermuda where such use relates to the exercise of political functions and the use of the personal information is covered by parliamentary privilege.

The MOF regards the lawful and correct treatment of personal information as integral to its successful operations, and to the maintenance of the confidence of persons with whom we interact. To this end, we fully endorse and adhere to the principles of the Act.

Purpose

The purpose of this policy is to ensure that:

everyone involved in the use of personal information at the MOF is fully aware of, and complies with, the requirements of the Act; and

individuals are aware of their rights under the Act.

Scope

This policy sets out how the Ministry of Finance handles the personal information of customers, suppliers, employees, workers and other third parties.

This policy applies to all personal information used by the MOF regardless of the media on which that information is stored or whether the personal information relates to past or present employees, workers, customers, clients or supplier contacts or any other individual.

All employees, workers, and consultants of the MOF and other authorised third parties who have access to any personal information held by or on behalf of the MOF ("**Personnel**") must read, understand and comply with this policy when using personal information on the MOF's behalf.

The consequences for the MOF of breaching the Act are significant and may amount to a fine up to $250,000, publication of the offence and/or loss of employment with the MOF. All Personnel are required to comply with the terms set out in this policy as the same may be amended periodically at all times. Any breach of this policy may result in disciplinary action.

Personal information

In this policy, "**personal information**" means any information which relates to a living individual who can be identified from that information or from other information, which is in the possession of, or is likely to come into the possession of, the MOF or its representatives or service providers.

Certain personal information is considered to be particularly sensitive and is subject to stricter rules regarding its use. Personal information is deemed to be "**sensitive personal information"** if it relates to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

The MOF only holds personal information which is directly relevant to its dealings with an individual. Examples of personal information that the MOF holds include (but are not limited to) an individual's name, email address, home address, phone number, age and bank account details. All information held is stored and used in accordance with the Act and this policy.

Using personal information

The terms "**use**" or "**using**" in relation to personal information means carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

Personal information is generally collected by the MOF in order to:

A. ensure that the MOF can facilitate efficient transactions with, and perform its obligations and exercise its rights under contracts with, third parties including, but not limited to, its customers, partners, associates and affiliates;

B. efficiently manage its employees, contractors, agents and consultants;

C. efficiently and effectively manage its business and contracts; and

D. meet all relevant obligations imposed by law.

Personnel may not use personal information for any reason other than for the lawful purposes for which it was collected and used. An explanation of the lawful grounds by which personal information may be used by the MOF is provided in clause 0 below entitled '*PIPA key principles and rules*'.

Personal information may be disclosed within the MOF and may be passed from one department to another in accordance with the PIPA principles set out in clause 0 below and this policy. Under no circumstances will personal information be passed to any department or any individual within the MOF that does not reasonably require access to that personal information in order to achieve the purpose or purposes for which it was collected and is being used.

PIPA key principles and rules

The MOF adheres to the key principles and rules set out in the Act relating to the use of personal information. Accordingly, any person using personal information must comply with the following key principles and rules:

Responsibility and compliance. The MOF has adopted suitable measures and policies to effect its obligations and to protect the rights of individuals set out in the Act. The MOF has designated a Privacy Officer for the purposes of compliance with the Act and communicating with the Privacy Commissioner.

Conditions for using personal information. The MOF uses personal information in accordance with the conditions set out in Section 6 of the Act and its Privacy Notice. Where consent is required to use personal information, Personnel shall take all reasonable steps to ensure that consent is obtained and a record of such consent is maintained.

Sensitive personal information. Personnel must ensure that consent is obtained from individuals for the use of their sensitive personal information. The MOF and its Personnel will not, without lawful authority, use sensitive personal information to discriminate against any person contrary to any provision of Part II of the Human Rights Act 1981. Failure to protect and use sensitive personal information lawfully by Personnel may result in disciplinary action.

Fairness. The MOF shall use personal information in a lawful and fair manner, ensuring that individuals are informed clearly, openly and honestly about how their personal information will be used. Personnel shall only handle personal information in ways that individuals would reasonably expect.

Privacy notices. The MOF has adopted a clear and easy to understand Privacy Notice which includes a statement of its practices and policies with respect to personal information.

Purpose limitation. Personal information must be used only for specified, explicit and lawful purposes. Personal information must not be used in any manner which is incompatible with those purposes.

Proportionality. The personal information that is used must be adequate, relevant and limited to the minimum information necessary for the lawful purposes for which it is used.

Integrity of personal information. Personal information must be accurate and, where appropriate, kept up-to-date. Any personal information which is incorrect must be rectified as soon as possible.

Security safeguards. Personal information must be protected against unauthorised or unlawful use, accidental loss, destruction or damage through appropriate technical and organisational measures.

Breach of security. The Privacy Officer is responsible for ensuring that breaches of security are reported to the Privacy Commissioner and individuals are informed without undue delay. Records must be kept on any personal information breaches, regardless of whether notification is required.

Transfer of personal information to an overseas third party. Transfer of personal information outside of Bermuda must be made in accordance with the provisions of Section 15 of the Act which require:

A. assessment of the level of protection provided by the overseas third party for that personal information;

B. consideration of the laws applicable to the overseas party and the recommendations of the Information Commissioner (as defined in the Act) regarding the transfer of personal information to that jurisdiction;

C. that the MOF may rely on a comparable level of protection where it reasonably believes that the protection provided by the overseas third party is comparable to the level of protection required by the Act;

D. where clause 00C above is not satisfied, the MOF shall employ contractual mechanisms, corporate codes of conduct (such as binding corporate rules), or other means to ensure that the overseas third party provides a comparable level of protection;

E. notwithstanding clauses 00A to D above, the MOF may transfer personal information to an overseas third party for use by that overseas party on behalf of the MOF or for the overseas third party's own business purposes, if:

F. the transfer of the personal information is necessary for the establishment, exercise or defense of legal rights; or

G. the MOF assesses all of the circumstances surrounding the transfer of personal information to the overseas third party and reasonably considers the transfer of personal information is:
    - *small scale;*
    - *occasional; and*
    - *unlikely to prejudice the rights of an individual.*

Personal information about children in the information society. Should the MOF be required to collect or use personal information about individuals under the age of fourteen (14) ("**child**"), a Privacy Impact Statement in the form set out in the Schedule of this policy should be completed, and Personnel must obtain consent from a parent or guardian prior to the child's personal information being collected or otherwise used. The MOF shall not seek to obtain personal information from a child about other individuals, including in particular, personal information relating to the professional activity of parents or guardians, financial information or sociological information except that personal information about the identity and address of the child's parent or guardian may be used for the sole purpose of obtaining consent. If the MOF provides a service delivered by means of digital or electronic communications (known as an information society service) targeted at children, it shall ensure that its privacy notice is understandable and appropriate to the age of the children targeted.

Consent

Personal information may only be used if the purpose of the use satisfies one of the lawful grounds permitted under the Act. There are various legitimate reasons for which personal information can be collected and used. One such reason is if the individual has consented to the use of their personal information. Other applicable reasons are described in clause 0 below entitled '*Grounds for using personal information*'.

If consent is being relied on to justify using a person's personal information, it must satisfy each of the following criteria:

A. the consent must be limited to specific use activities;

B. the individual must have been informed the about the use activities in sufficient detail so as to be able to fully understand what they are consenting to;

C. the consent must be freely given. In other words, the individual must have a genuine free choice as to whether they give the consent. Consent will not be freely given where there is a significant imbalance of power such that the individual does not really have a free choice about giving consent;

D. the performance of a contract or delivery of a service cannot be made conditional upon the individual giving their consent to the information use, unless the information use is required in order to perform the contract or deliver the service;

E. the consent must be given by way of an unambiguous statement or some other clear, active communication by the individual, such as signing a form. Consent cannot be inferred from silence or inactivity (for example, the use of pre-ticked boxes); and

F. the consent to the use of personal information must be clearly distinguished from other matters that the individual is asked to agree to (for example, it should not be buried within the terms of a broader contract that the individual is asked to sign).

Where the use relates to sensitive personal information, an individual's explicit consent must be obtained, ideally by way of a signed statement or other means which very clearly and demonstrably indicate the consent of the individual.

A record of consents should be retained by MOF to evidence that it has been authorised to use an individual's personal information.

It is important to note that individuals have the right to withdraw their consent at any time and it must be as easy to withdraw consent as it was to provide it in the first place. It is important that there are appropriate processes in place to promptly action any withdrawal of consent.

Grounds for using personal information

As noted above, consent is not the only basis on which personal information can be collected and used. There are other lawful grounds for using personal information that the MOF may be able to rely upon.

This section describes the lawful grounds for use which are most likely to be relevant to the MOF's activities. If you are unable to satisfy one of these grounds, then you should contact the MOF's Privacy Officer for advice as to whether the proposed use can be undertaken.

Non-sensitive personal information

The legal grounds for the use of non-sensitive personal information include:

A. where an individual has given their consent to the use of their personal information. The requirements for obtaining a valid consent are explained in clause 0 above under the heading '*Consent*';

B. where the use is in the MOF's legitimate interests and does not cause unwarranted prejudice to the individual;

C. where the use is necessary for the performance of a contract to which an individual is a party, or for the taking of steps (at the request of the individual) with a view to entering a contract; and

D. where the use is required by Act.

Sensitive personal information

Sensitive personal information is subject to stricter legal controls and the circumstances in which it can be used are more limited than in respect of other personal information. The legal grounds for using sensitive personal information include:

A. where an individual has given their explicit consent;

B. where the use is necessary for the purposes of carrying out the obligations and exercising rights of the MOF;

C. where the use is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights; and

D. in the context of recruitment or employment where the nature of the role justifies such use.

The lists above set out the commonly applicable grounds for using personal information and sensitive personal information but are by no means exhaustive. If you are unable to satisfy one of these grounds, then you should contact the Privacy officer for advice as to whether the proposed use can be undertaken.

Fair use of personal information

Any forms (whether paper-based or web-based or electronic) that gather personal information on an individual should contain a statement explaining what the personal information is to be used for and to whom within the MOF it may be disclosed.

Regardless of how personal information is obtained (whether it is obtained from an individual or from a third party), the individual must be provided with information about the use of their personal information by the MOF at or before the time the personal information is collected or, if the personal information is obtained from a third party, within a reasonable time after obtaining the personal information or at the time of the first communication with the individual, whichever is earlier.

The information provided to an individual must include the following:

A. the categories of personal information collected in relation to the individual;

B. if the personal information is not obtained from the individual directly, the source or sources of the personal information;

C. the purpose or purposes for which personal information will be used, including the legal grounds for the use (see clause 0 '*Grounds for using personal information*' above). If the legal grounds involve legitimate interests, a description of those legitimate interests must also be provided;

D. if personal information is used based on the individual's consent, an explanation of the individual's right to withdraw their consent at any time;

E. the categories of personal information that may be disclosed to third parties and the reasons for these disclosures;

F. if the collection and use of personal information is a contractual requirement, whether the individual is obliged to provide the personal information on that basis, and the possible consequences of a failure to provide the information;

G. the period for which the personal information will be retained, or (if it is not possible to provide a specific time period) the criteria that will be used to determine the retention period;

H. a general description of the MOF's policies and practices with respect to protecting the confidentiality and security of personal information;

I. the existence of the individual's rights; and

J. any other information that is necessary to guarantee that the use of the personal information is fair in the circumstances.

This information must be provided in a concise, transparent, intelligible and accessible form, using clear and plain language that will be easy for the individual to understand.

If any information described above changes after it has been provided to the individual, the individual must be provided with an updated copy of the information.

Third party service providers

Where the MOF instructs a third party to collect, store or use personal information on its behalf (an "**information processor**"), the third party must enter into a written agreement with the MOF (an "**information processor agreement**") that:

A. provides details of the use of personal information that they are being instructed to carry out;

B. requires the third party to process the personal information only in accordance with the MOF's written instructions and to the extent necessary for them to fulfil their obligations to the MOF's under the agreement;

C. requires the third party to implement appropriate technical and organisational measures and controls to ensure the confidentiality and security of the personal information; and

D. imposes any additional information use obligations required by the Act.

Guidance on the additional legal obligations that the agreement must include can be obtained from the Privacy Officer.

The information processor agreement should be approved by the Privacy Officer and signed by or on behalf of the MOF and the information processor before any personal information may be transferred to the information processor.

When contracting with an information processor, it is important that the MOF conducts appropriate due diligence both at the outset of the relationship and on a periodic basis thereafter, to ensure that the information processor is capable of complying, and does comply, with the requirements of the Act and referred to in clauses 0B to D above.

Disclosure of personal information

The MOF must ensure that personal information is not disclosed to unauthorised third parties. All Personnel should exercise caution when asked to disclose any personal information to a third party. This clause does not apply to authorised third parties such as information processors (see clause 0 '*Third party service providers*' above).

Personal information should not be disclosed orally or in writing to third parties without the consent of the individual and the approval of the Privacy Officer.

In some limited circumstances, the Act permits the disclosure of personal information without the need to obtain the prior consent of an individual. Such disclosures may be permitted where this is necessary:

A. to safeguard national security;

B. for the prevention or detection of crime, in the substantial public interest, and where obtaining consent from the individual would prejudice that purpose;

C. for the administration of justice;

D. to comply with applicable law; and

E. to protect the vital interests of the individual (this refers to life and death situations), but only when their consent cannot be obtained.

Requests for personal information from third parties must be supported by appropriate paperwork and any disclosures must be approved by the Privacy Officer.

Transfers of personal information to overseas third parties

Specific legal requirements apply to the transfer of personal information to an overseas third party as set out in clause 00 above. Here, the transfer of information includes sending personal information to another country or allowing that personal information to be accessed remotely in another country, regardless of whether the MOF transfers personal information overseas itself or an information processor does so when acting on the MOF's behalf.

Personal information must not be transferred overseas unless the recipient country ensures an adequate level of protection for the rights and freedoms of individuals.

Before any transfer of personal information to overseas third party takes place, the Privacy Officer must first determine whether the transfer is lawful.

Retention and disposal of personal information

Personal information must not be retained for longer than is necessary for the lawful purposes for which it is used. To achieve this, each category of personal information used by the MOF will be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods will be monitored, and, upon their expiry, the relevant personal information must be deleted or anonymised so that it is no longer possible to identify the individual to whom the personal information relates.

Some information may need to be kept for longer periods than others, for example where it is necessary to retain certain records in order for the MOF to comply with its legal obligations.

Personal information must be disposed of securely in a way that protects the rights and privacy of individuals and ensures the permanent erasure of the information (e.g. shredding, disposal as confidential waste, or secure electronic deletion). Hard drives of redundant PCs should be wiped clean before disposal.

Information protection, information security and recovery

It is imperative that the MOF safeguards the personal information in its possession or control by applying appropriate technical and organisational security measures to protect the information.

In addition to the specific security policies that apply, all Personnel must comply with the following when using and/or transmitting personal information:

A. Personal information, whether held electronically or in paper form, must be kept securely at all times. Personnel must ensure that appropriate technical and organisational measures are in place to prevent unauthorised or accidental access,

use, disclosure, loss or damage when personal information is being used (including but not limited to when it is at rest or in transit). Technical measures, for example, include the use of encryption tools to protect personal information held in electronic form must be implemented. Organisational measures include, for example, storing paper records containing personal information in locked cabinets.

B. In the event personal information is lost, damaged, compromised, misdirected or stolen, or otherwise used in an unauthorised manner, the Privacy Officer must report such breach to the Privacy Commissioner and, where required under the Act, to any affected individual.

C. Care must be taken to ensure appropriate security measures are in place for the deletion or disposal of personal information in accordance with clause 0 '*Retention and disposal of personal information*' above.

D. Personal information should not be disclosed except in accordance with clause 0 '*Third party service providers*' and clause 0 '*Disclosure of personal information*' above.

Access to personal information

Individuals have a number of legal rights in relation to their personal information. These rights include:

A. the right to obtain information regarding the use of and access to the personal information which the MOF holds or which is held on the MOF's behalf in respect of the individual;

B. the right to receive a copy of any personal information which the MOF processes about them;

C. the right to request that the MOF rectify their personal information if it is inaccurate or incomplete;

D. the right to request that the MOF erase their personal information in certain circumstances. This may include, but is not limited to, circumstances in which:

    i. it is no longer necessary for the MOF to retain their personal information for the purposes for which it was collected; or

    ii. the MOF is only entitled to process the individual's personal information with their consent (i.e. because no other lawful ground for use the personal information applies), and the individual withdraws their consent; and

E. the right to lodge a complaint with the Privacy Commissioner if the individual thinks their rights have been infringed by the MOF.

Requests to exercise these rights should be sent to the MOF's Privacy Officer.

Record keeping

Accurate and up to date records of personal information use carried out by the MOF must be maintained. These records must include:

A. details of the Personnel using the personal information;

B. the purposes of using the personal information;

C. the categories of individual;

D. the categories of recipients of personal information;

E. the categories of transfers of personal information overseas;

F. the envisaged time limits for erasure of the personal information (where possible); and

G. a general description of the technical and organisational security measures adopted by the MOF.

The Privacy Officer will keep a central record of the MOF's personal information use activities or material changes to existing activities. Changes made by Personnel must be notified to the Privacy Officer.

Privacy Officer

The MOF's Privacy Officer is ultimately responsible for ensuring that the MOF meets its legal obligations under the Act.

The Privacy Officer is responsible for:

A. keeping all Personnel updated about their responsibilities, risks and issues in connection with personal information protection;

B. reviewing and recommending the revision, if necessary, of all personal information protection procedures and related policies;

C. arranging appropriate training, advice and instruction for Personnel;

D. handling all personal information protection queries from or on behalf of Personnel or third parties;

E. dealing with all requests from individuals relating to access, use, storage and destruction of personal information;

F. reviewing and approving any contracts or agreements with information processors;

G. ensuring all systems, services and equipment for storing personal information by the MOF or on the MOF's behalf meets acceptable security standards;

H. ensuring that regular checks are carried out on computer hardware and software to ensure they are functioning properly, and personal information is being stored securely;

I. ensuring that in the event the Privacy Officer is unable to carry out their responsibilities, their duties are delegated to one or more appropriate individuals; and

J. communicating with the Privacy Commissioner on all personal information matters in connection with the MOF and dealing with any requests from the Office of the Privacy Commissioner.