Data Protection in Bermuda: overview

STEVEN REES DAVIES, TIFFANY BOYS, SHANNON CANN, APPLEBY (BERMUDA) LIMITED, WITH PRACTICAL LAW

A Q&A guide to data protection in Bermuda. This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.
To compare answers across multiple jurisdictions, visit the Data protection Country Q&A (2-502-1510) tool.

REGULATION

LEGISLATION

1. What national laws regulate the collection and use of personal data?

GENERAL LAWS

The Personal Information Protection Act 2016 (*PIPA*) is the principal piece of Bermuda legislation regarding the right to personal informational privacy. Provisions relating to the supervision under the PIPA came into force on 2 December 2016. The majority of the PIPA will come into force in increments over a period of two years, but PIPA's regulations will not become mandatory until it is fully implemented at the end of 2018.

In Bermuda, European Union (*EU*) Regulations are not directly applicable and EU Directives are not automatically implemented into Bermuda law. The government of Bermuda, however, has drawn on legislation from a number of jurisdictions including the EU General Data Protection Regulation as well as recent international developments, such as the EU-US Privacy Shield, to produce the PIPA, with the goal to enable the unhindered transfer of personal information between Bermuda and any EU member state, together with the increasing number of countries that have been or will also be deemed adequate by the EU Commission.

SECTORAL LAWS

Bermuda currently boasts a series of sectorial-specific areas of data control which are implemented via both legislative and regulatory mechanisms. These sectoral laws are significantly older than the above-mentioned overarching data protection framework and include the following industry-specific areas:

- Banking: Banks and Deposit Companies Act 1999.
- Electronic Transactions: Electronic Transactions Act 1999.
- Public authorities: Public Access to Information Act 2010.

All legislation in this area is and will continue to be subject to Bermuda's constitution, which overrides both domestic legislation and the principles of common law, as well as the Human Rights Act 1981 (*HRA*), which also cannot be derogated from unless specifically stated therein.

When the PIPA is fully implemented, the sectoral data protection laws will remain in force, but the PIPA will become the overriding legislation. Section 4(5) of the PIPA states that the PIPA will prevail over any inconsistent legislation unless the PIPA is inconsistent with or in conflict with a provision of the HRA, in which case the HRA prevails.

SCOPE OF LEGISLATION

2. To whom do the laws apply?

Sectoral laws (*see* Question 1) apply to all persons (which include individuals, companies or associations, or bodies of persons, whether corporate or unincorporated, unless otherwise stated) who are subject to Bermuda law and are carrying on the sectoral specific activities governed by applicable legislation.

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 (*Banks Act*) regulates deposit-taking businesses. A person carries out a deposit-taking business for the purposes of the Banks Act if in the course of the business the person either:

- Lends money received by way of deposit to others.
- Finances any other activity of the business wholly or to any material extent, out of the capital of or the interest on money received by way of deposit.

ELECTRONIC TRANSACTIONS ACT 1999

The Electronic Transactions Act 1999 (*ETA*) protects the personal data of identifiable natural persons, who are individuals who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person's physiological, mental, economic, cultural, or social identity.

The ETA regulates

- E-commerce service providers, who are persons who use electronic means to provide goods, services, or information.
- Intermediaries, who are persons who, with respect to an electronic record and on behalf of another person:
  - send, receive, or store that electronic record; or
  - provide other services with respect to that electronic record.
- Data controllers, who are persons who, either alone or jointly or in common with other persons, determine the purposes for which and the manner in which any personal data is, or is to be, processed.
- Data processors, who are persons who process personal data on behalf of a data controller.

PERSONAL INFORMATION PROTECTION ACT 2016

Once the Personal Information Protection Act 2016 (*PIPA*) has been fully implemented (*see* Question 1), it will be applicable to all organisations, with certain exceptions that use personal information in Bermuda, wholly or partly by automated means or which form or are intended to form, part of a structured filing system.

Relevant definitions from the PIPA are as follows:

- Individual is defined as a natural person.
- Organisation is defined as any individual, entity, or public authority that uses personal information.
- Overseas third party is defined as an organisation not domiciled in Bermuda.

For more on the definition of personal data, see Question 3. For more on data processing operations, see Question 4.

3. What data is regulated?

There are currently two main legislative acts in force which govern the use of personal data or personal information:

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 governs the disclosure of information relating to any person's business or other affairs that a bank or financial institution receives.

STANDARD FOR ELECTRONIC TRANSACTIONS

Established in accordance with subsections 29(3) and 29(5) of the Electronic Transactions Act 1999 (*ETA*), the Standard for Electronic Transactions dated 18 May 2000 regulates the use and disclosure of personal data by e-commerce businesses, particularly intermediaries and e-commerce service providers.

The ETA defines personal data as any information relating to an identified or identifiable natural person, which includes a person who can be identified, directly or indirectly, by physiological, mental, economic, cultural, or social identity.

The ETA defines an identifiable natural person an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person's physiological, mental, economic, cultural or social identity.

PERSONAL INFORMATION PROTECTION ACT 2016

Once the Personal Information Protection Act 2016 (*PIPA*) has been fully implemented (*see* Question 1), it will regulate the following:

- Personal information, which is any information about an identified or identifiable individual.
- Sensitive personal information, which is any personal information relating to an individual's:
  - place of origin, race, colour, national or ethnic origin;
  - sex, sexual orientation, or 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.

Additional conditions apply to organisations using sensitive personal information.

For information regarding the processing of personal data, see Question 4. For information regarding the processing of sensitive personal data, see Question 11.

4. What acts are regulated?

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 regulates the disclosure of personal information by a bank or financial institution relating to any individual's business or other affairs.

ELECTRONIC TRANSACTIONS ACT 1999

The Electronic Transactions Act 1999 regulates the use and disclosure of personal data by e-commerce businesses, particularly intermediaries and e-commerce service providers.

PERSONAL INFORMATION PROTECTION ACT 2016

The Personal Information Protection Act 2016 regulates the processing of personal information, which is any operation on personal information, including the following:

- Collecting, obtaining, or recording.
- Holding, storing, or organising.
- Adapting or altering.
- Retrieving, transferring, or disclosing.
- Combining, blocking, erasing, or destroying.

5. What is the jurisdictional scope of the rules?

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 applies to organizations carrying on deposit-taking business in or from within Bermuda.

ELECTRONIC TRANSACTIONS ACT 1999

The Electronic Transactions Act 1999 regulates the use and disclosure of personal data by e-commerce businesses, particularly intermediaries and e-commerce service providers.

PERSONAL INFORMATION PROTECTION ACT 2016

Once the Personal Information Protection Act 2016 (*PIPA*) has been fully implemented (*see* Question 1), it will apply to every organisation that uses personal information in Bermuda. The PIPA currently does not distinguish between organisations that are incorporated under Bermuda law and overseas entities that have a business presence, such as an office, in Bermuda for the purposes of compliance with the data protection afforded to individuals.

6. What are the main exemptions (if any)?

BANKS AND DEPOSIT COMPANIES ACT 1999

The following are exempt from all provisions of the Banks and Deposit Companies Act 1999:

- The government of Bermuda.
- Bermuda Monetary Authority.
- Every public authority in Bermuda.
- A credit union licensed under the Credit Unions Act 2010.
- Any person carrying on deposit-taking business who is for the time being registered under the Insurance Act 1978. This paragraph applies only to persons who accept deposits in the course of carrying on the insurance business for which they are registered.
- Any person carrying on deposit-taking business who is for the time being licensed under the Investment Business Act 1998. This paragraph applies only to persons who accept deposits in the course of carrying on the investment business for which they are licensed.

STANDARD FOR ELECTRONIC TRANSACTIONS AND THE ELECTRONIC TRANSACTIONS ACT 1999

The Electronic Transactions Act 1999 and the Standard for Electronic Transactions do not provide any relevant exclusion from their requirements.

PERSONAL INFORMATION PROTECTION ACT 2016

The PIPA contains both exclusions from the definition of personal information and general exemptions from its regulation.

When fully implemented (*see* Question 1), the PIPA will exclude from personal information any information used for the following purposes:

- Crime and taxation.
- The exercise of political function by a member of the House of Assembly or the Senate if the personal information is covered by parliamentary privilege.
- Legal privilege.
- Personal or domestic purposes.
- Journalistic, literary, and artistic purposes.
- A transfer 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 before the PIPA comes into operation.
- Business contact information only, for contacting an individual in the individual's capacity as an employee or official of an organisation.
- Natural security.
- For regulatory activity and honours, and for:
  - the prevention or detection of crime and international obligations;
  - the assessment or collection of any tax or duty;
  - the prevention, investigation, detection, and prosecution of breaches of ethics for regulated professionals; and
  - the economic or financial interests of Bermuda;
- By communications providers.

The PIPA also excludes personal information about an individual who has been dead for at least 20 years and personal information about an individual that has been in existence for at least 150 years.

NOTIFICATION

7. Is notification or registration required before processing data?

Bermuda law does not require notification or registration before processing data.

MAIN DATA PROTECTION RULES AND PRINCIPLES

MAIN OBLIGATIONS AND PROCESSING REQUIREMENTS

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 does not impose any obligations on data controllers to ensure that data is processed properly.

STANDARD FOR ELECTRONIC TRANSACTIONS AND THE ELECTRONIC TRANSACTIONS ACT 1999

The Standard for Electronic Transactions that are established in accordance with the Electronic Transactions Act 1999 sets out the following safe harbour guidelines for service providers and data controllers:

- Maintenance of effective monitoring systems.
- Establishment of effective contracts.
- "Know Your Customer" practices.
- Systems to protect privacy.
- Practices to avoid abusive usage.
- Complaints and disputes systems.
- Establishing transparent business practices.
- Systems to avoid misleading statements or omissions.

Intermediaries and e-commerce service providers should collect personal data of customers only if it is:

- Relevant for the provision of goods, services, or information as agreed with the customer.
- Otherwise disclosed to the customer before the collection of the information.

Intermediaries and e-commerce service providers should also use personal data and business records of customers only for:

- Internal marketing, billing, or other purposes necessary for the provision of services.
- Other purposes made known to the customer before the time the personal data or business records are collected.
- Other purposes with the prior consent of the customer, and should endeavour to ensure that the personal data or business records are:
  - accurate, and if necessary, kept up to date;
  - if inaccurate, are erased or rectified; and
  - are erased when no longer reasonably required.

Providers should endeavour to:

- Ensure the confidentiality of personal data and business records of customers.
- Prevent the sale or transfer of the personal data and business records of customers other than as part of the sale of the intermediaries' or e-commerce service providers' business.
- Prevent the examination of or tampering with personal data or business records other than for the purposes of maintenance or security of the relevant information processing system or data integrity.

PERSONAL INFORMATION PROTECTION ACT 2016

The Personal Information Protection Act 2016 has eight Data Protection Principles, which mandate that personal information should:

- Be used fairly and lawfully.
- Be used for limited specified purposes.
- Be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is used.
- Be accurate and, where necessary, kept up to date.
- Not be kept for longer than is necessary for that use.
- Be used in accordance with the rights of individuals.
- Be kept securely.
- Only be transferred to third parties (including international transfers) where there is a comparable level of protection.

9. Is the consent of data subjects required before processing personal data?

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 requires the consent of the data subject before the disclosure of personal information.

STANDARD FOR ELECTRONIC TRANSACTIONS AND THE ELECTRONIC TRANSACTIONS ACT 1999

The Standard for Electronic Transactions and the Electronic Transactions Act 1999 do not impose a requirement to obtain consent to process data.

PERSONAL INFORMATION PROTECTION ACT 2016

Under the Personal Information Protection Act 2016 (*PIPA*), an organisation must obtain the consent of the individual before processing personal data, unless another condition for processing personal data applies (*see* Question 10).

When seeking consent, organisations must provide clear, prominent, easily understandable, and accessible mechanisms by which the individual can grant consent. An organisation is not obliged to provide these mechanisms where it can be reasonably implied from the individual's conduct that the individual consents to the use of its personal information for all intended purposes, unless the information is sensitive personal information. The PIPA does not define consent and is further silent as to the form that the mechanisms must take (whether it should be written versus electronic online consent).

In most cases, when it is known or reasonably likely that an organisation will use the personal information of a minor under the age of 14, for services delivered by means of digital or electronic communications, a parent or guardian must provide consent before the personal information is collected or otherwise used. In addition, organisations must provide a privacy notice that is easily understandable and appropriate to the age of the child.

10. If consent is not given, on what other grounds (if any) can processing be justified?

BANKS AND DEPOSIT COMPANIES ACT 1999

The Banks and Deposit Companies Act 1999 provides that the requirement to obtain consent does not apply to information:

- Which at the time of the disclosure is or has already been made available to the public from other sources.
- In the form of a summary or collection of information so framed as not to enable information relating to any particular person to be ascertained from it.

PERSONAL INFORMATION PROTECTION ACT 2016

Under the Personal Information Protection Act 2016 (*PIPA*), an organisation may process personal information without consent where:

- It is necessary for the performance of a contract to which the individual is a party or for the taking of steps at the request of the individual with a view of entering into a contract.
- The use of the personal information is pursuant to a provision of law that authorises or requires the use.
- The personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability.
- The use of the personal information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public.
- The use of the personal information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organisation or in a third party to whom the personal information is disclosed.
- The use of the personal information is necessary in the context of an individual's present, past, or potential employment relationship with the organisation.

Where an organisation is unable to meet any of the above conditions, then it may use personal information only if:

- It was collected from, or is disclosed to, a public authority which is authorised or required by statutory provision to provide the personal information to, or collect it from, the organisation.
- It is used for the purpose of complying with an order made by a court, individual, or body having jurisdiction over the organisation.
- It is used for the purpose of contacting the next of kin or a friend of an injured, ill, or deceased individual.
- Its use is necessary to collect a debt owed to the organisation or for the organisation to repay to the individual money owed by the organisation.
- Its use is in connection with disclosure to the surviving spouse or a relative of a deceased individual if, in the reasonable opinion of the organisation, the disclosure is appropriate.
- Its use is reasonable to protect or defend the organisation in any legal proceedings.

SPECIAL RULES

11. Do special rules apply for certain types of personal data, such as sensitive data?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will limit the use of sensitive personal information (*see* Question 3) to organisations with lawful authority to do so. Sensitive personal information is used with lawful authority if and only to the extent that it is used:

- With the consent of any individual to whom the information relates.
- In accordance with an order made by either the court or the Privacy Commissioner.
- For the purpose of any criminal or civil proceeding.
- In the context of recruitment or employment where the nature of the role justifies the use.

Special rules do not apply for certain types of personal data under the Banks Act, the Standard for Electronic Transactions, or the Electronic Transactions Act 1999.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will require an organisation collecting an individual's personal information to provide the individual with a clear and easily accessible Privacy Notice, which must include:

- The fact that personal information is being used.
- The purposes for which personal information is or might be used.
- The identity and types of individuals or organisations to whom personal information might be disclosed.
- The identity and location of the organisation, including information on how to contact it about its handling of personal information.
- The name of the privacy officer.
- The choices and means the organisation provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing, and destroying, the individual's personal information.

Organisations must take all reasonably practicable steps to ensure that the Privacy Notice is provided either before or at the time of the collection of personal information, or, where that is not possible, as soon thereafter as is reasonably practicable.

An organisation will not be obliged to provide a Privacy Notice if:

- All of the personal information it holds is publicly available information.
- The organisation can reasonably determine that all uses made, or to be made, of the personal information are within the reasonable expectations of the individual to whom the personal information relates.

There are no information disclosure requirements under the Banks Act, the Standard for Electronic Transactions, or the Electronic Transactions Act 1999.

13. What other specific rights are granted to data subjects?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will provide an individual with the following specific rights in relation to the individual's personal information:

- The right to access the information in the custody or control of an organisation.
- The right to access the purpose for which the information is being used.

- The name of any person the information was or will be disclosed to and the circumstances regarding the disclosure.

In addition, the PIPA will afford individuals with the right to require an organisation to refrain from or cease using their personal information:

- For the purposes of advertising, marketing, or public relations.
- Where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to the individual or another individual.

Individuals will further have rights relating to the rectification, blocking, erasure, and destruction of personal information. An organisation however is not required to comply with the request if the request is manifestly unreasonable.

These rights are not provided under the Banks Act, the Standard for Electronic Transactions, or the Electronic Transactions Act 1999.

14. Do data subjects have a right to request the deletion of their data?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will provide individuals with the right to request the erasure or destruction of their personal information when that personal information is no longer relevant for the purposes of its use.

On receipt of the request, the organisation must either erase or destroy the information identified in the request or provide the individual with written reasons as to why the continued use of such information is justified.

There are no such rights provided under the Banks Act, the Standard for Electronic Transactions, or the Electronic Transactions Act 1999.

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will require an organisation to safeguard all personal information that it holds against risk, including the risk of:

- Loss.
- Unauthorised access.
- Use.
- Modification.
- Disclosure.
- Any other misuse.

These safeguards must be subject to periodic review and reassessment and be proportional to:

- The likelihood and severity of the harm threatened by the loss, access, or misuse of the personal information.
- The sensitivity of the personal information (including in particular whether it is sensitive personal information).
- The context in which it is held.

STANDARD FOR ELECTRONIC TRANSACTIONS

The Standard for Electronic Transactions dated 18 May 2000 (*Standard*) provides that intermediaries and e-commerce service providers should endeavour to:

- Ensure the confidentiality of personal data and business records of customers.
- Prevent the sale or transfer of the personal data and business records of customers other than as part of the sale of the intermediaries' or e-commerce service providers' business.
- Prevent the examination of or tampering with personal data or business records other than for the purposes of maintenance or security of the relevant information processing system or data integrity.

There are no security requirements imposed in relation to personal data under the Banks Act, the Standard, or the Electronic Transactions Act 1999.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), it will require organisations to notify without undue delay the Privacy Commissioner and any individual affected of any breach of security leading to loss or unlawful destruction or unauthorised disclosure of or access to personal information likely to adversely affect any individual.

The notification to the Privacy Commissioner must describe:

- The nature of the breach.
- Its likely consequences for that individual concerned.
- The measures taken or to be taken to address the breach.

On notification, the Privacy Commissioner may determine whether to order the organisation to take further steps and for maintenance of a record of the breach and the remedial measures taken.

There are no requirements to notify personal security breaches to data subjects under the Banks Act, the Standard for Electronic Transactions, or the Electronic Transactions Act 1999.

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), an organisation engaging (by contract or otherwise) the services of a third party in connection with the use of personal information remains responsible for ensuring compliance with the PIPA at all times.

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Bermuda legislature has not adopted any regulations under the Personal Information Protection Act 2016 governing or regulating the storage of cookies or equivalent devices on an individual's terminal equipment.

Intermediaries and e-commerce service providers should observe the principles of the Standard for Electronic Transactions dated 18 May 2000 (*see* Question 8).

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

There are no requirements in place under the Personal Information Protection Act 2016 (*PIPA*) regarding the sending of unsolicited electronic commercial communications (spam).

Under the PIPA, after a request from an individual, an organisation must cease or refrain from beginning the use of the individual's personal information for the purposes of marketing advertising or public relations.

The Standard for Electronic Transactions dated 18 May 2000 (*Standard*) provides that intermediaries and e-commerce service providers must:

- Refrain from sending bulk, unsolicited electronic records to persons:
  - with whom they do not have a relationship (either contractual or personal); or
  - who have not otherwise consented to receive the records.
- Establish reasonable practices to prevent their services from being used for the sending of bulk, unsolicited electronic records.
- Endeavour to cease providing services to persons who engage in this conduct.

There are no requirements under the Banks Act.

INTERNATIONAL TRANSFER OF DATA

TRANSFER OF DATA OUTSIDE THE JURISDICTION

20. What rules regulate the transfer of data outside your jurisdiction?

Once the Personal Information Protection Act 2016 (*PIPA*) is fully implemented (*see* Question 1), an organisation transferring personal information to an overseas third party for use by the third party, either on behalf of the organisation or for its own business purposes:

- Is responsible for compliance with the PIPA in relation to the personal information transferred, which includes assessing whether the level of protection of personal information provided by the overseas third party is comparable to the level of protection required by the PIPA.
- Must employ mechanisms, corporate codes of conduct, or other means to ensure the level of protection provided is a comparable level, if the organisation is not satisfied that the level of protection being provided by the overseas third party is comparable to the level the PIPA requires.

An organisation is not required to comply with these rules if the transfer of personal information to an overseas third party:

- Is necessary for the establishment, exercise, or defence of legal rights.
- Follows the organisation's assessment that the transfer is reasonably considered to be small-scale, occasional, and unlikely to prejudice the rights of an individual.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

There is no requirement to store any type of personal information inside Bermud a.

DATA TRANSFER AGREEMENTS

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

No.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

See Question 22.

24. Does the relevant national regulator need to approve the data transfer agreement?

See Question 22.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

Once appointed in accordance with the Personal Information Protection Act 2016 (*PIPA*), the Privacy Commissioner, following notification, a complaint, an investigation, or an inquiry, may utilise any one or more of the following enforcement powers:

- Make an order that an organisation commence or cease the performance of an activity.
- Issue formal warnings, admonish an organisation, and bring to the organisation's attention any failure to comply with the PIPA.
- Provide guidance and recommendations on the application of an organisation's rights and obligations under the PIPA.
- Attempt to resolve any matter under application for review or following a complaint by negotiation, conciliation, mediation, or other methods.

The Bermuda Monetary Authority (*Authority*) may impose a civil penalty to a person who fails to comply with any requirement or contravenes any prohibition imposed by or under the Banks Act, following notice to the person concerned (*see* Question 26).

Where an intermediary or e-commerce service provider has failed to comply with the Standard for Electronic Transactions, the Minister of Economic Development must give a written warning and may direct that person to cease and desist or otherwise to correct its practices, pursuant to the Electronic Transactions Act 1999.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The Personal Information Protection Act 2016 establishes the following sanctions for non-compliance with its provisions:

- For summary convictions of individuals, a fine not exceeding BD25,000, imprisonment not exceeding two years, or both.
- For convictions on indictment of persons other than individuals, a fine not exceeding BD250,000.

There is a defence available to both individuals and organisations if they can provide, to the satisfaction of the court, that they acted reasonably in the circumstances that gave rise to the offence.

It is possible that liability and punishment can be extended to any director, manager, secretary, or similar officer, or any person purporting to act in this capacity, if it can be proven that the offence was committed with the consent or connivance of, or was attributable to, any neglect on the part of the person.

Every person who fails to comply with any requirement or contravenes any prohibition imposed by or under the Banks Act is liable to a penalty not exceeding BD500,000, as the Bermuda Monetary Authority (*BMA*) considers appropriate, for each failure or contravention. The BMA does not impose this penalty if it is satisfied that the person concerned took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.

A data controller or data processor must comply with the Standard for Electronic Transactions (*Standard*) in respect to any personal data that is collected by the data controller. Failure to comply with the Standard may result in summary conviction and imprisonment for six months or a fine of BD50,000, or both.

An intermediary or e-commerce service provider who fails to comply with the Standard, must in the first instance be given a written warning by the Minister of Economic Development. The minister may direct that person to cease and desist or otherwise to correct its practices, and, if that person fails to do so within a period as may be specified in the direction, the person is guilty of an offence and may be liable on summary conviction to a fine of BD5,000 for each day on which the contravention continues.

REGULATOR DETAILS

A Privacy Commissioner will be appointed to office by the Governor of Bermuda, following consultation with the Premier and Opposition Leader in accordance with the Personal Information Protection Act 2016 (*PIPA*). The term of office will be five years with the ability to be re-appointed for a further five-year term. For greater objectivity, the commissioner, while exercising official functions, will not be subject to the direction or control of any person or authority.

The Minister of Finance and the Bermuda Monetary Authority (*BMA*) are responsible for matters relating to the Banks Act

At the time of drafting, the Minister of Economic Development is responsible for matters relating to the Electronic Transactions Act 1999 (*ETA*).

Main areas of responsibility. Once appointed, the Privacy Commissioner will be responsible for monitoring how the PIPA is administered.

The Minister of Economic Development is responsible under the ETA for making regulations prescribing standards for the processing of personal data whether or not the personal data originates inside Bermuda.

The Minister of Finance is responsible for making regulations under the Banks Act, acting on the advice from the BMA. The BMA is responsible for supervising the institutions licensed to undertake deposit-taking business under the Banks Act.

ONLINE RESOURCES

W www.bermudalaws.bm

Description. Bermuda Laws Online is a database of Bermuda's statutes and statutory instruments. It contains both consolidated laws as amended up to 16 February 2016 and annual laws from 1993. The Ministry of Legal Affairs and the Attorney-General's Chambers of Bermuda provide the content.

CONTRIBUTOR PROFILES

STEVEN REES DAVIES, PARTNER

Appleby (Bermuda) Limited

T + 441 298 3296
F + 441 298 3478
E sreesdavies@applebyglobaltrinidadlaw.com
W www.applebyglobal.com

Professional qualifications. New York, US, Attorney, 2002; England and Wales, Solicitor (non-practising) 2003; Bermuda, Attorney, 2008

Areas of practice. Corporate regulation.

Languages. English

Professional associations/memberships. Bermuda Bar Association; the Law Society of England and Wales; and the New York Bar Association.

TIFFANY BOYS, ASSOCIATE

Appleby (Bermuda) Limited

T + 441 298 3596
F + 441 298 3430
E tboys@applebyglobal.com
W www.applebyglobal.com

Professional qualifications. Bermuda, Attorney, 2011

Areas of practice. Banking; asset finance.

SHANNON CANN, ASSOCIATE

Appleby (Bermuda) Limited

T + 441 298 3230
E scann@applebyglobal.com
W www.applebyglobal.com

Professional qualifications. Bermuda, Attorney, 2011

Areas of practice. Corporate regulation

Professional associations/memberships. Bermuda Bar Association