BVI introduces data protection regime

On 6 April 2021, the BVI government passed the Data Protection Act (the ***DPA***). The DPA was published in the gazette on 13 April 2021 but has not yet come into force – it will come into force on a date to be determined by the government and this is expected imminently.

The background to this is of course the drive for the BVI to become equivalent with the UK and European Union in this area, in particular under the EU's General Data Protection Regulation (***GDPR***).

Data controllers and processors, take note

In brief, the DPA governs how a "data controller" may process, use and retain personal data and the objectives of the DPA are to:

- Safeguard personal data processed by public bodies and private bodies by balancing the necessity of processing personal data, protecting personal data from unlawful processing by public bodies and private bodies.
- Promote transparency and accountability in the processing of personal data.

Anyone in the BVI who falls within the definition of a "data controller" must now comply with the data protection principles in relation to any personal data processed by the data controller. Where a data controller engages a third party (a ***data processor***) to process personal data on its behalf, the data controller must ensure the third party complies with the data protection principles.

The DPA also sets out the rights of individuals to control their personal data and implements a system to protect against the misuse of personal data.

The BVI supervisory authority for the DPA, the Office of the Information Commissioner, will have responsibility for investigating complaints relating to violations of personal data use.

What are the data protection principles?

The data protection principles are the:

- General Principle
- Notice and Choice Principle
- Disclosure Principle
- Security Principle
- Retention Principle
- Data Integrity Principle
- Access Principle

These principles bear some similarity to comparable principles set out in the GDPR and in a future article we will be comparing and contrasting the regimes more closely.

Who must comply with the DPA?

The DPA applies to:

- A "private body" (being an entity that carries on any trade, business or profession, but only in that capacity; or has legal personality), a person who "processes" or a person who has control over or authorises the "processing" of any personal data in respect of commercial transactions (defined as any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance).

- A person established in the BVI and who processes personal data or employs or engages any other person to process personal data on his or her behalf, whether or not in the context of that establishment.

- Where the person is not established in the BVI but uses equipment in the BVI for processing personal data otherwise than for the purpose of transit through the BVI. Such persons are required under the Act to appoint a person established in the BVI for the purposes of the DPA.

The DPA also binds the Crown, ie the BVI government.

What about BVI business companies and other businesses?

Importantly, any data controller that is a BVI company or partnership; foreign company registered in the BVI; or business operating in the BVI, that processes personal data, in the context of being established in the BVI, must comply with the DPA.

Any data controller that processes personal data in the BVI, regardless of where it is established, must also comply with the DPA.

The individual to which the personal data relates does not need to be in the BVI nor a citizen (belonger) of the BVI.

Who is a data controller or processor?

A "data controller" is an entity that either alone or jointly or in common with other persons processes any personal data, or has control over, or authorises the processing of any personal data, but does not include a data processor. Processing includes collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data.

A "data processor" in relation to personal data, means a person who, processes data on behalf of a data controller (but does not include an employee of the data controller).

A business will be considered a data controller of the data it collects and processes for the purposes of its business.

A service provider which receives personal data from a business and processes that data on behalf of the business is a data processor. Examples of data processors will include fund administrators, cloud or other software platform providers or marketing firms with access to the business' client lists.

What is personal data?

A "data subject" is defined under the DPA to include both living and deceased persons.

"Personal data" is defined under the DPA as any information in respect of commercial transactions:

- Which is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose.

- Recorded with the intention that it should wholly or partly be processed by means of such equipment.

- Recorded as part of a relevant filing system with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information, or from that and other

information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject.

The data protection regime is therefore relevant only to the extent that the data in question can be used to identify a data subject.

Examples of personal data include items such as names, email, identity card numbers or telephone numbers – ie any information which allows the data subject to be identified.

Sensitive personal data is considered to be personal data revealing the data subject's physical or mental health, sexual orientation, political opinions, religious beliefs or other similar nature, criminal convictions, the commission or alleged commission of any offence or any other personal data that the Minister may by Order prescribe as sensitive personal data. Where sensitive personal data is being processed the data controller must adhere to additional conditions described below.

What must a data controller do to comply with the DPA?

Under the DPA, a data controller can process personal data about a data subject, if the processing is necessary for the following:

- The performance of a contract to which the data subject is a party
- The taking of steps at the request of the data subject with a view to entering into a contract
- For compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract
- In order to protect the vital interests of the data subject
- For the administration of justice
- For the exercise of any functions conferred on a person by or under any law

The DPA however, outlines certain overarching circumstances which must be met in order for personal data to be processed. Pursuant to the DPA, personal data cannot be processed unless:

- It is being processed for a lawful purpose directly related to an activity of the data controller
- Its processing is necessary for or directly related to that purpose
- It is adequate but not excessive in relation to that purpose

If a data controller is processing sensitive personal data then the data controller must have met one of the following conditions (in addition to the above):

- Received explicit consent from the data subject
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment

Considerations around consent

Under the Notice and Choice Principle, the data controller must inform a data subject following a request for personal data of:

- The purposes for which the personal data is being or is to be collected and further processed
- Any information available to the data controller as to the source of that personal data
- The data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data

- The class of third parties to whom the data controller discloses or may disclose the personal data
- Whether it is obligatory or voluntary for the data subject to supply the personal data
- Where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he or she fails to supply the personal data

Express consent is required to process personal data which can be withdrawn at any time.

Transfer of data outside the BVI

Personal data cannot be transferred outside the BVI unless there is proof of adequate data protection safeguards or consent from the data subject.

Adequate level of protection?

It is not clear at present what "adequate data protection safeguards" will entail however it should be noted that a similar concept exists under Article 46(2) of the GDPR.

Are there any exemptions from the DPA?

The DPA does not apply to personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

There are exemptions from the requirement to comply with some or all of the data protection principles such as for the purposes of the prevention or detection of crime or for the purpose of investigations; apprehension or prosecution of offenders; or assessment or collection of any tax or duty or any other imposition of a similar nature. There are also a number of other exemptions from certain of the data protection principles for specific classes of data processing.

What rights do data subjects have?

On written request, a data subject must be informed of the following by a data controller:

- Whether their personal data is being processed by or on behalf of the data controller
- Description of their personal data in an intelligible form
- The purpose for processing the personal data
- The recipients or classes of recipients to whom the personal data may be disclosed
- Where the personal data may be transferred to outside of the BVI
- How the data controller safeguards the integrity and confidentiality of the personal data
- Any other information required by the BVI Information Commissioner

A data subject may request details of the personal data held by a data controller. If it is a valid request the data controller must provide such information within 30 days. There are limited exceptions to providing this personal data to a data subject.

A data subject has the right to request that any inaccuracy or incompleteness in their personal data be corrected and the right to request that no automated decision making be made using their personal data.

At any time, a data subject may request a data controller to cease processing their personal data for any reason, including direct marketing. The DPA sets out various time limits for when such cessation must have happened.

A data subject has the right to lodge a complaint with the Office of the Information Commissioner.

What happens if there is misuse of personal data?

The Security Principle establishes that a data controller must take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of personal data.

Any person may make a complaint to the Information Commissioner that personal data is not processed in accordance with the DPA and the Information Commissioner must determine whether or not to conduct an investigation.

A data subject who suffers damage or distress by reason of the contravention by a public body or private body of any of the provisions of this Act may institute civil proceedings in the BVI Court.

What powers of enforcement does the Information Commissioner have?

The Information Commissioner has the power under the DPA to require any person to provide information to it in order to fulfil its functions under the DPA.

Where the Information Commissioner believes the data controller is, or may be, in contravention of the DPA, it may order a data controller to take, or refrain from, certain actions. It may also make monetary penalty orders.

Offences and penalties under the DPA

The DPA establishes the following offences:

- **Obstruction of an Information Officer:** A person who wilfully obstructs the Information Commissioner or an authorised officer commits an offence and is liable, on summary conviction, to a fine not exceeding US$5,000 or a term of imprisonment not exceeding six months, or both.

- **Wilful disclosure of information:** A person who wilfully discloses personal information in contravention of this DPA or collects, stores or disposes of personal information in a manner that contravenes the DPA commits an offence and is liable, on summary conviction, to a fine not exceeding US$5,000 or to imprisonment to a term not exceeding six months or both.

- **Breach of Confidentiality:** A person who wilfully breaches the confidentiality obligations established under the DPA commits an offence and is liable, on summary conviction, to a fine not exceeding US$50,000 or imprisonment for a term not exceeding three years, or both and on indictment to a fine not exceeding US$100,000 or to imprisonment not exceeding five years, or both.

Where it is proven that a body corporate commits an offence under the DPA and is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, any director, manager, secretary or other similar officer of that body corporate, or a person purporting to act in that capacity, the person as well as the body corporate each commits the offence and are liable to be proceeded against and punished accordingly , it is liable, on summary conviction, to a fine not exceeding US$250,000 and on indictment to a fine of US$500,000.

Other remedies under the DPA

- **Judicial Review:** A person aggrieved by a decision of the Information Commissioner may within 30 days of receiving the written notice of the decision, apply for judicial review of the decision.

- **Damages:** A data subject who suffers damage or distress by reason of the contravention of the provisions of this DPA may institute civil proceedings.

What are the next steps?

If your organisation is within scope of the DPA then you must:

- Prepare a privacy notice to give to individuals to explain how you will process, use and retain their personal data

- Review your procedures to ensure the manner in which you process and retain personal data complies with the DPA and that you are able to retrieve specific personal data if requested to do so by a data subject or a relevant authority

- You may need to adopt a data processing, protection and retention policy

- If you engage a third party to process data on your behalf you will need to ensure there is a written contract for such engagement that addresses your obligations under the DPA, including any transfer of data outside of the BVI

For investment funds this means they must:

- Send the privacy notice to existing investors
- Update subscription documents to include a privacy notice for new investors
- Update offering documents to reflect the new requirements under the DPA
- Update agreements with any third parties that process personal data on behalf of the fund to ensure such processing is undertaken in compliance with the DPA especially where there is transfer of data outside of the BVI

Harneys lawyers have advised on data protection legislation outside of the BVI for many years and would be delighted to assist in relation to the new DPA regime in the BVI.

For more information and key contacts please visit **harneys.com**