JULY 2021

mourant

UPDATE

Data protection regime introduced in the BVI

Update prepared by Sara Galletly (Cayman) and Ian Montgomery (BVI)

A new data protection regime has been established in the British Virgin Islands (**BVI**) providing a comprehensive framework for the protection of personal data which aims to meet UK and EU standards of data protection, as established by the EU's General Data Protection Regulation (**GDPR**).

The Data Protection Act, 2021 (**DPA**), which came into force on 9 July 2021, establishes a legal framework to ensure the protection of personal data collected and processed by public and private bodies. The definition of a **private body** includes any entity which carries on any trade, business or profession, but only in that capacity, or which has legal personality. The DPA will therefore apply to all BVI incorporated companies and limited partnerships with legal personality. Limited partnerships without legal personality should also prepare for the DPA as they may fall within scope by virtue of being 'established' in the BVI.

Who will it apply to?

The DPA aims to protect **data subjects**, being the natural person (whether living or deceased) whose data is being processed.

The public or private body processing the data will either be a:

- **data controller**, meaning the person who either alone or jointly processes any personal data, or has control over, or authorises the processing of any personal data; or
- **data processor**, meaning the person processing personal data on behalf of the data controller (but not including an employee of the data controller).

What data will it apply to?

Personal data includes any information in respect of commercial transactions[1], which:

- is being processed wholly or partly by automatic means;
- is recorded with the intention that it should be wholly or partly processed by such means; or
- is recorded as 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 controller (including any sensitive personal data and expression of opinion about the data subject).

[1] **Commercial transactions** means 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.

Sensitive personal data means any personal data about a data subject's physical or mental health, sexual orientation, political opinions, religious beliefs, criminal convictions, commission or alleged commission of any offence or any other personal data as may be prescribed.

When will it apply?

The DPA will apply to a person:

- established in the BVI that processes personal data whether or not in the context of that establishment; and
- not established in the BVI that uses equipment in the BVI for processing personal data, otherwise than for the purpose of transit of data through the BVI.[2]

Key principles

General principle

The general principle of the DPA provides that a data controller shall not:

- process personal data (other than sensitive personal data[3]) without the express consent of the data subject[4];
- transfer personal data outside of the BVI without proof of adequate data protection safeguards or consent from the data subject.

Notwithstanding the above, processing will be permitted if:

- it is for a **lawful purpose** directly related to an activity of the data controller;
- it is **necessary** for, or directly related to, that purpose; and
- the personal data is **adequate but not excessive** in relation to that purpose.

Lawful purposes for processing

The lawful purposes for which processing of personal data will be permitted include where it is necessary:

- for the performance of a **contract** to which the data subject is a party or for 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 one imposed by a contract);
- to protect the **vital interests** of the data subject;
- for the **administration of justice**; or
- for the **exercise of any functions conferred on a person by law**.

Note that the lawful purposes above do not include the 'legitimate interests' basis contained in GDPR.

Additional principles

The DPA also contains the following principles:

- **Notice and choice principle** - data controllers must inform a data subject of:
  - the purposes for processing;
  - information as to the source of the personal data;
  - the rights to request access to and correction of personal data;
  - how to contact the data controller with any inquiries or complaints;

---

[2] In such cases a local representative must be nominated.

[3] In the case of sensitive personal data, a data controller must comply with section 20 of the DPA.

[4] A data subject may withdraw their consent at any time. The withdrawal of consent by a data subject will not affect the lawfulness of processing based on consent before its withdrawal.

- the class of third parties to whom the personal data will be disclosed; and
- whether the data subject is obliged to supply the personal data and, if so, the consequences of non-compliance.

- Disclosure principle - no personal data shall be disclosed without the consent of the data subject for any purpose other than the purpose for which the personal data was to be disclosed at the time of collection (or a directly related purpose) or to any party other than a third party of the class of third parties specified above.
- Security principle - data controllers must take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to:
  - the nature of the personal data and the harm that would result from the same;
  - the place or location where the personal data is stored;
  - any security measures incorporated into any storage equipment;
  - the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
  - the measures taken for ensuring the secure transfer of the personal data.
- Retention principle - personal data shall not be kept longer than is necessary for the fulfilment of the purpose for processing and data controllers must take all reasonable steps to ensure that personal data is destroyed or permanently deleted if no longer required for the purpose for which it was to be processed.
- Data integrity principle - a data controller shall take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up-to-date.
- Access principle - data subjects shall be given access to their personal data and be able to request corrections where the personal data is inaccurate, incomplete, misleading or not up-to-date.

What rights will the DPA give individuals?

A data subject may make a written request to the data controller under the following rights:

- to be informed of processing and be given a description of the data and purposes for processing within 30 days of such request (the right of access);
- for the data controller to rectify any data which is incomplete, incorrect, misleading, excessive or which is not relevant to the purpose for which it is held (the right to apply for rectification); and
- that the data controller stop or not begin processing for the purposes of direct marketing (the right to prevent processing for direct marketing).

Will there be any exemptions?

The DPA will not apply to personal data processed by individuals for personal reasons. There may also be potential exemptions for data controllers where personal data is processed for:

- the prevention or detection of crime or for the purpose of investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of any tax or duty;
- preparing statistics or carrying out research (provided it is not processed for any other purpose and the results are not in a form which identifies the data subject);
- necessary compliance with any order or judgment of a court; or
- the discharge of regulatory functions.

Information Commissioner

The DPA will establish the Office of the Information Commissioner as supervising authority with powers to:

- monitor compliance with the DPA by public and private bodies
- provide advice to public and private bodies regarding their obligations under the DPA;

- investigate complaints about alleged violations of the data protection principles; and
- manage technical co-operation and exchange of information with foreign data protection authorities

The Information Commissioner will have various enforcement powers available to it, such as issuing information notices and enforcement notices and requesting that a Magistrate issue a search warrant.

Offences

Offences by bodies corporate under the DPA will give rise to liability on summary conviction to a fine of US$250,000 or on indictment to a fine of US$500,000. The directors and officers of a body corporate may also be held liable if the offence was committed with their consent or connivance, or was attributable to their neglect.

Next steps

Businesses that process personal data will need to ensure that their data processes and procedures are compliant. Mourant can advise you on what changes may be required depending on the nature of your business.

Contacts

Paul Christopher
Managing Partner, Mourant Ozannes
Hong Kong
+852 3995 5700
paul.christopher@mourant.com

Ian Montgomery
Partner, Mourant Ozannes
British Virgin Islands
+1 284 852 1730
ian.montgomery@mourant.com

John Rochester
Solicitor (BVI) (England & Wales) non practising
Mourant Ozannes (Guernsey) LLP
+44 1481 739 359
john.rochester@mourant.com

Sara Galletly
Partner, Mourant Ozannes
Cayman Islands
+1 345 814 9233
sara.galletly@mourant.com

Simon Lawrenson
Partner, Mourant Ozannes
Hong Kong
+852 3995 5707
simon.lawrenson@mourant.com

2021934/812 83 25 4/1