DATA PROTECTION LAWS OF THE WORLD

British Virgin Islands

DLA PIPER

BRITISH VIRGIN ISLANDS

Last modified 28 January 2024

LAW

The British Virgin Islands' Data Protection Act, 2021 (DPA) came into force on 9 July 2021.

The DPA is the primary legislation and the first legislative framework of its kind in the British Virgin Islands to govern how public and private bodies may process personal data. The law strives to promote transparency and accountability, bringing the British Virgin Islands in line with the UK and EU data protection standards.

DEFINITIONS

Definition of personal data

Personal data means any information in respect of commercial transactions which: (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention, and in each case, 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 or other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject

Definition of sensitive personal data

Sensitive personal data means any personal data about a data subject’s:

- physical or mental health;
- sexual orientation;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- criminal convictions, the commission or alleged commission of, an offence; or
- any other personal data that may be prescribed as such under the DPA, from time to time.

Other key definitions

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

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

data subject means a natural person, whether living or deceased

data controller means a person who, 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, in relation to personal data, means collecting, recording, holding, or storing the personal data or carrying out any operation or set of operations on the personal data, including the: (i) organisation, adaptation, or alteration of personal data; (ii) retrieval, consultation or use of personal data; (iii) disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (iv) alignment, combination, correction, erasure or destruction of personal data, and

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority under the DPA is the Office of the Information Commissioner.

Given the recent enactment of the DPA, the Office of the Information Commissioner has not yet been staffed.

REGISTRATION

There is currently no requirement for a data controller or a data processor to notify the Information Commissioner of their role or complete any registration.

DATA PROTECTION OFFICERS

There is no requirement under the DPA for a data protection officer to be appointed.

COLLECTION & PROCESSING

Data controllers are responsible for compliance with certain privacy and data protection principles applicable to the personal data it processes. Data controllers are also responsible for ensuring that the principles are complied with, where personal data is processed on the data controller’s behalf (e.g., by its vendors).

Under these principles:

- a data controller shall not process personal data (other than sensitive personal data) without the express consent of the data subject, or transfer personal data outside of the British Virgin Islands without proof of adequate data protection safeguards or consent from the data subject, unless either of the Exceptions defined under the heading “ Transfer” exists (the **General Principle**)
- a data controller must inform a data subject of: (a) the purposes for processing; (b) information as to the source of the personal data; (c) the rights to request access to and correction of the personal data; (d) how to contact the data controller; (e) the class of third parties to whom the personal data will be disclosed; and (f) whether the data is obligated to supply the personal data, and if so, the consequences of not supplying same (the **Notice and Choice Principle**)
- no personal data shall be disclosed without the consent of the data subject for any purposes other than the purpose for which the personal data was to be disclosed at the time of collection or to any party other than a third party of the class of third parties noted above (the **Disclosure Principle**)
- a data controller 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 (a) the nature of the personal data and the harm that would result from any loss, misuse, etc.; (b) the place or location where the personal data is stored; (c) any security measures incorporated into any storage equipment; (d) the measures taken for ensuring the reliability, integrity, and competence of personnel having access to the personal data; and (e) the measures taken for ensuring the secure transfer of the personal data (the **Security Principle**)
- personal data shall not be kept longer than is necessary for the fulfillment of the purpose of 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 (the **Retention Principle**)
- a data controller shall take reasonable steps to ensure that personal data is accurate, complete, not misleading, and kept current (the **Data Integrity Principle**), and
- 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 current (the “**Access Principle**”)

TRANSFER

As set out under the **General Principle**, transfers of personal data by a data controller or a data processor to countries or territories outside the British Virgin Islands are only permitted where that country or territory ensures an adequate level of protection of data protection safeguards in relation to the processing of personal data. This transfer restriction endeavors to ensure that the level of protection provided by the DPA is not circumvented by transferring personal data abroad.

The DPA also includes the following exceptions where the General Principle will not apply to a transfer:

- if the data subject has consented to the transfer (where consent must be freely given, specific, informed, and unambiguous and must be capable of being withdrawn at any time)
- where the transfer is necessary for the performance of a contract between the data subject and the data controller, or the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller
- the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject, or for the performance of such a contract;
- the transfer is necessary for reasons of substantial public interest
- the transfer is for a lawful purpose directly related to an activity of the data controller, is necessary for, or directly related to, that purpose, and the personal data is adequate but not excessive in relation to that purchase
- the transfer is necessary in order to protect the vital interests of the data subject
- the transfer is necessary for the administration of justice, or
- the transfer is required for the exercise of any functions conferred on a person by law.

SECURITY

While the DPA does not specify any technical standards for data controllers to implement, the DPA requires a data controller, when processing personal data, to take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access, or disclosure, alteration or destruction (together, '**Security Breach**') by having regard to the following matters:

- the nature of the personal data and the harm that would result from a Security Breach
- the place or location where the personal data is stored
- any security measures incorporated into any equipment in which the personal data is stored
- 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

The DPA also requires, where a data processor carries out the processing of personal data on behalf of the data controller, the data controller (for the purpose of protecting the personal data from Security Breach) to ensure that the data processor:

- provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
- take reasonable steps to ensure compliance with the above measures

BREACH NOTIFICATION

The DPA does not require data controllers to notify the Information Commissioner or the data subjects of personal data breaches.

However, notice requirements apply to data controllers that receive enforcement notices from the Information Commissioner. The DPA requires a public or private body to, as soon as practicable, and in any event within 30 days of complying with an

enforcement notice from the Information Commissioner: (i) notify the data subject(s) concerned; and (ii) any person to whom the personal data was disclosed within the twelve months preceding the date of service of the enforcement notice (as determined by the Information Commissioner).

ENFORCEMENT

A breach of the DPA constitutes a criminal offence. Upon conviction, violators may be subject to a fine of up to US$100,000, imprisonment of up to five years, or both. A body corporate is punishable on conviction to a fine of up to US$500,000.

The Information Commissioner has broad investigative and corrective powers under the DPA, including the power to request and obtain information from parties subject to the law and to issue orders to carry out specific remediation activities.

The DPA provides for a private right of action where data subjects suffer damage or distress due to a breach of the DPA by a public or private body.

In addition, the DPA explicitly provides for personal liability in respect of offences committed by a body corporate where the offence is proven to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, any director, secretary, or similar officer, or any person purporting to act in such capacity. Where the affairs of a body corporate are managed by its members, this personal liability also applies to the acts and defaults of a member in connection with the member’s function of management.

ELECTRONIC MARKETING

The DPA applies to “direct marketing”, which is the communication, by whatever means, of any advertising or marketing material that is directed to particular individuals and therefore includes electronic marketing.

Prior express consent is not required for the purposes of direct marketing. However, a data subject has an unconditional right to require the date controller to stop, or not to commence, the processing of any of their personal data for the purposes of direct marketing (i.e., an “opt-out” right).

ONLINE PRIVACY

There are no specific restrictions on online privacy in the DPA. However, the provisions of the DPA apply where a private body is a website operator that collects personal data.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Clinton Hempel
Partner
Carey Olsen
T +27 76 412 6091
clinton.hempel@careyolsen.com

Jude Hodge
Counsel
Carey Olsen
T +1 284 394 4034
jude.hodge@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.