

# DATA PROTECTION

## in the BVI

---

A Legal Guide



George Henry Partners LP

[www.ghpbvi.com](http://www.ghpbvi.com)

## Data Protection in the British Virgin Islands

### Overview

The Data Protection Act, 2021 (the **DPA**) is now of some vintage, having come into force in the British Virgin Islands (the **Virgin Islands**) on 9 July 2021.

The DPA was designed to:

- safeguard **personal data** (defined below) processed by public and private bodies (**Relevant Persons**) by balancing the necessity of processing the personal data with the need to protect personal data from unlawful processing; and
- promote transparency and accountability in the processing of personal data.

### 1. To whom does the DPA apply?

The DPA applies to **data processors** and **data controllers** (defined below).

For data processors and data controllers who are private bodies, the DPA will apply only if the private body is:

- established in the Virgin Islands and processes personal data, or employs or engages any other person to process personal data on its behalf in any way; or
- not established in the Virgin Islands but uses equipment in the Virgin Islands for processing personal data otherwise than for the purposes of transit through the Virgin Islands (**Non-BVI Persons**).

Non-BVI Persons are required to nominate a representative established in the Virgin Islands for purposes of the DPA.

The DPA also binds the Government of the Virgin Islands.

### 2. Who are data controllers and data processors?

A “**data controller**” is any person who either individually or collectively processes or authorises the processing of any personal data, but *does not* include a data processor. BVI business companies and limited partnerships, including investment funds, investment administrators, financial services licences including banks and trust companies, charities and government ministries, departments and agencies would all be data controllers to the extent that they process personal data.

A “**data processor**” is any person who processes data on behalf of a data controller. The data processor is typically a separate person from the data controller but *does not* include an employee of the data controller.

Although the DPA applies to data processors, data controllers bear the brunt of the obligations under the DPA as they are typically the users and ultimate controllers of the personal data. Even where processing of personal data is carried out by a data processor on behalf of a data controller, it is the data controller's obligation to ensure that the data processor provides sufficient guarantees regarding the security and integrity of the personal data being processed. A data processor would include, for example, cloud providers that store personal data and other service providers acting on behalf of an organisation with access to customer or employee personal data.

### 3. What are personal data and sensitive personal data?

The DPA defines "**personal data**" 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; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

all of which relate 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 DPA defines "**commercial transactions**" 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.

The definition of "**personal data**" is fairly broad. Personal data includes traditional data that may directly identify a data subject, such as their names, identification numbers, location data and online identifiers. It also includes other data which, when scrutinised in context, could indirectly relate to the data subject. Accordingly, the DPA will not likely apply to completely anonymised data.

The DPA defines "**sensitive personal data**" as 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 any offence; or
- any other personal data that the Minister may by Order prescribe.

A "**data subject**", in relation to personal data, means any natural person whether living or deceased. Accordingly, information about companies and public bodies as such is not personal data under the DPA.

### 4. When is a data controller considered to be "processing" personal data?

Any activity which affects personal data in any way may constitute processing. The DPA defines “**processing**” as the collecting, recording, holding or storing of personal data or the carrying out of any operation or set of operations on the personal data, including the:

- organisation, adaptation or alteration of personal data;
- retrieval, consultation or use of personal data;
- disclosure of personal data by transmission, transfer, dissemination or otherwise making personal data available; or
- alignment, combination, correction, erasure or destruction of personal data;

## 5. What are my obligations as a data controller?

Data controllers are responsible for applying the requirements of the DPA including the data protection principles. The data protection principles may be categorised as follows:

- General principle
- Notice and choice principle
- Disclosure principle
- Security principle
- Retention principle
- Data integrity principle
- Access principle

In very broad summary, the data protection principles provide that a data controller shall not:

- process personal data about a data subject unless the data subject has given his or her *express* consent; or
- transfer personal data outside the Virgin Islands without proof of adequate protection, safeguards or consent from the data subject.

Where personal data is processed with the consent of the data subject, the data subject may at any time withdraw his or her consent. Additionally, a data controller cannot process sensitive personal data except in accordance with the DPA.

Data controllers are also subject to the overarching purpose limitation and data minimisation requirements which state that personal data shall not be processed unless:

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

A data controller must inform a data subject upon a request for personal data of the purpose for which the personal data is being collected and of the data subject’s right to request access to and correction of personal data. When processing data, a data controller must also take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure or any alteration or destruction.

Personal data processed for any purpose cannot be kept longer than is necessary for the fulfilment of that purpose and must be destroyed or permanently deleted if it is no longer required for that purpose. Data controllers are required to take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date having regard to the purpose for which the personal data was collected and further processed.

A data controller must also cooperate with the Information Commissioner (the **Commissioner**) in relation to any investigation being carried out under the DPA.

## 6. Can I process personal data without consent?

The main basis for the processing of personal data under the DPA is consent. Accordingly, there are only very limited circumstances in which personal data may be processed without express consent. These include where such processing is necessary for:

- 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;
- compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
- the protection of the vital interests of the data subject;
- the administration of justice; or
- the exercise of any legally conferred functions.

## 7. What additional rights do data subjects have?

**Right of access to personal data:** All data subjects have a right to access their own personal data.

**Right of rectification of personal data:** A data subject has a right to rectification of any personal data held by a Relevant Person that is incomplete, incorrect, misleading, excessive, or irrelevant to the purpose for which the personal data is held.

**Right to prevent processing for purposes of direct marketing:** A person may require the data controller within a reasonable period to stop processing or to not begin processing of personal data for the purposes of direct marketing. For these purposes, direct marketing means the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals. By way of example, an organisation sending promotional emails directly to existing clients (often unsolicited) would be considered to be participating in direct marketing.

## 8. What exemptions under the DPA should I be aware of?

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.

Additionally, specified data protection principles and provisions of the DPA will not apply where personal data is processed for the following reasons:

- Prevention or detection of crime or for the purpose of investigations

- Apprehension or prosecution of offenders
- Assessment or collection of any tax or duty or other imposition of a similar nature
- Physical or mental health of a data subject
- Preparation of statistics or carrying out research
- Processing relating to any order or judgment of the Court
- Discharging regulatory functions
- Journalistic, literary or artistic purposes.

## 9. The Information Commissioner

The DPA establishes the Office of the Information Commissioner which is to be headed by a Commissioner. The functions of the Commissioner include:

- monitoring compliance by public and private bodies with the requirements of the DPA;
- receiving and investigating complaints about alleged violations of the data protection principles;
- making reports to complainants about investigations into any complaint;
- managing technical co-operation and exchange of information with foreign data protection authorities as is necessary.

As of the date of writing this article, no Commissioner has been appointed under the DPA.

## 10. Enforcement

There are various enforcement mechanisms under the DPA. These are set out and briefly explained below.

**Investigation of complaints:** The Commissioner may investigate or cause to be investigated any complaint by a data subject that a Relevant Person has breached, is breaching or is likely to breach any provision of the DPA.

**Information notice:** The Commissioner may, by way of information notice, request that a person provide access to personal data and furnish:

- information about and documentation of the processing of personal data;
- information related to the security of processing of personal data; and
- any other information in relation to matters specified in the notice that the Commissioner considers necessary or expedient for the performance of his or her functions and the exercise of his or her powers under the DPA.

**Warrant to search and enter:** A Magistrate may issue a warrant to enter and search any premises with respect to which there are reasonable grounds for suspecting that an offence under the DPA has been or is being committed and that evidence of the contravention or commission of the offence may be found on such premises.

**Enforcement notice:** Where the Commissioner is satisfied that a Relevant Person is contravening or has contravened any provision of the DPA, the Commissioner may serve an enforcement notice on the Relevant Person. The enforcement notice may require the relevant body to:

- rectify or erase personal data; or
- supplement the personal data with statements concerning the matters dealt with by the personal data as the Commissioner may approve.

**Assessment of processing:** The Commissioner may also carry out an assessment of the processing of personal data to determine compliance with the DPA.

## 11. What remedies and protections do I have as a data subject or complainant?

**Damages:** If a data subject suffers damage or distress by reason of a Relevant Person's contravention of the DPA, the data subject can institute civil proceedings in the High Court to request compensatory damages or any other appropriate relief.

**Whistleblower's protection:** A Relevant Person is barred from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee or denying an employee any benefit because the employee, acting in good faith and based on reasonable belief:

- notifies the Commissioner that his or her employer or any other person has contravened or is about to contravene the DPA;
- has done or stated his or her intention to do anything that is required to be done to avoid any contravention of the DPA;
- refused to do or stated the intention of refusing to do anything that is in contravention of the DPA,

or because the employer believes that the employee will do any of the above action.

**Judicial review:** Any person who is aggrieved by any decision of the Commissioner may seek judicial review of the decision.

## 12. Offences

The DPA sets out various offences and their corresponding penalties. The penalties, particularly as regards the breach of confidentiality and offences committed by bodies corporate, are quite significant.

The offences include:

- Obstruction
- Wilful disclosure of information
- Processing sensitive personal data, otherwise than in accordance with the DPA
- Breach of confidentiality

### *Offence by bodies corporate*

If a body corporate commits an offence with the consent or connivance of or due to the neglect on the part of any director, manager, secretary or other similar officer or any other person purporting to act in that capacity, that person as well the corporate body commits the offence and may be punished accordingly.

A body corporate that commits an offence under the DPA is liable on:

- summary conviction to a fine not exceeding US\$250,000;
- conviction on indictment, to a fine not exceeding US\$500,000.

### 13. What should I be doing now?

Every organisation in the BVI should be continually reviewing their business operations to determine whether they are data controllers within the meaning of the DPA. If an organisation is a data controller, it should consult with its BVI counsel to determine what measures it may need to implement to comply and stay compliant with the ongoing requirements of the DPA.

### 14. How can GHP help?

At GHP, we understand the complexity of data protection compliance and can assist with the following:

- Providing legal advice on the application of the DPA
- Conducting a data mapping exercise to determine how information and data flows into your organisation and how it is processed, used, protected, stored and deleted
- Drafting or updating privacy notices
- Drafting or reviewing data transfer agreements
- Drafting or reviewing written procedures for handling data subject requests
- Drafting or reviewing internal data protection policies and procedures
- Updating offering and subscription documents and other third-party agreements for investment funds
- Training relevant staff.

If you have any further queries on or need any assistance with compliance with the DPA, please reach out to your usual GHP contact.

## Contact Us

---

JERMAINE O CASE  
Senior Associate | George Henry Partners LP  
☎ + 1 284 393 7004 | + 1 284 346 4422  
✉ [jermaine.case@ghpbvi.com](mailto:jermaine.case@ghpbvi.com)

---

Copyright © George Henry Partners LP

*The content of this guide is intended for general information purposes only and is current as at the date of publication indicated. This guide does not constitute legal advice and should not be relied upon as such. You should always seek specific legal advice that takes into account your individual circumstances.*