COLLAS CRILL

The BVI's new data protection law explained

AUGUST 2021

The BVI has introduced data protection legislation, the Data Protection Act, 2021 (the **DPA**), which came into force on 9 July 2021.

This guide summarises the new law and what you need to do to comply with it. If you are a bond issuer or an investment fund, please consult the specific guidance in sections 5 and 6, below.

1. Why was the DPA introduced?

The DPA was introduced so that the BVI would have a framework for the protection of personal data which is broadly similar to the principles that apply in the UK and EU under the General Data Protection Regulation 2016/679 (**GDPR**).

The objectives of the DPA are expressed to be twofold:

- to safeguard personal data processed by public bodies and private bodies by balancing the necessity of processing personal data with protecting it from unlawful processing by public bodies and private bodies; and
- to promote transparency and accountability in the processing of personal data.

2. What do I need to do?

If you are a data controller or a data processor (see section 3 below), then you must **immediately ensure that you process personal data strictly in accordance with the DPA**. Read this guide to learn more about your obligations.

3. Who does the DPA apply to?

The DPA has *potential* impact for public bodies and private bodies:

- Public bodies include: the House of Assembly or any committee of the House of Assembly; the Cabinet of the Virgin Islands; any ministry or department or division of a ministry; local authorities; statutory bodies (for example, the National Parks Trust of the Virgin Islands) and any other body designated as such by the Minister for Information (as defined below);
- It binds the Crown; the BVI Government;
- Private bodies are basically all bodies ***excluding*** public bodies that carry on trade, business or a profession and extends to all persons established in the BVI, including natural persons resident for not less than 180 days per year, all bodies corporate, partnerships or unincorporated associations incorporated/registered and/or formed (as applicable) under BVI law and all persons maintaining an office, branch or agency or regular professional practice in the BVI. **This extends to all BVI companies and limited partnerships;**
- Persons not established in the BVI, but who use equipment in the BVI for processing personal data otherwise than for the purposes of transit through the BVI, are also subject to the DPA and will need to designate someone situated in the BVI for the purpose of compliance with the DPA.

The DPA will apply if you are a public or private body as above which (1) **is a data controller** and (2) **processes personal data** of (3) a **data subject**. If you are a data controller who outsources the processing of personal data of a data subject to a third party, you will also be responsible for ensuring that that third party (a **data processor**) complies with the DPA.

The data must be processed in respect of **commercial transactions**.

The DPA uses the following key definitions.

- **Commercial transaction** 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 controller** is a person who, either alone or jointly or in common with other persons, processes any personal data (including collecting, recording, holding or storing) or has control over, or authorises the processing of any personal data, excluding a data processor.
- A **data processor** in relation to any personal data is a person who processes data on behalf of a data controller, excluding an employee of the data controller. A key example of a data processor is an investment fund administrator.

- **Data subject** is a natural person (whether living or deceased) whose data is processed; a data subject may reside anywhere in the world and be of any nationality.
- **Personal data** includes any information in respect of a commercial transaction (ie any transaction of a commercial nature (whether contractual or not) which includes any matters relating to the supply or exchange of goods or services, investments, agency financing, banking and insurance) that is:
  - being processed (wholly or in part) by means of equipment operating automatically in response to instructions given for that purpose;
  - is recorded with the intention that it should be (wholly or in part) processed by means of that equipment; or
  - recorded as part of a relevant filing system,

and relates (directly or indirectly) to a data subject, who is *identified or identifiable from that information* or from that information and other information in the possession of the data controller (including any sensitive personal data and expression of opinion about the data subject).

- **Process** or **processing** means, in relation to personal data, collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including: (i) the organisation, adaption or alteration of personal data; (ii) the 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.
- **Sensitive personal data** is 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 prescribed as sensitive personal data. Sensitive personal data attracts a more onerous level of data protection compliance.
- 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. Other exemptions apply in respect of personal data processed:
  - for the prevention or detection of crime or for the purpose of investigation
  - in relation to information of the physical or mental health of a data subject;
  - for preparing statistics or carrying out research;
  - for the purpose of or in connection with any order or judgment of a court;
  - for carrying out a regulatory function; and
  - for journalistic, literary or artistic purposes.

4. If you are a general data controller or data processor

Policy formulation: the starting point is to formulate an in-house policy for the processing, protection, access and retention of personal data.

Policy review: if you already have a data protection policy, then you will simply need to make sure that they meet the requirements of the DPA (which are less prescriptive than the data protection requirements in other jurisdictions and significantly less onerous than GDPR).

Contract review: review any contracts under which any third party processes data on your behalf to ensure that the third party (the data processor) carries out its responsibilities in a manner that will satisfy your obligations as a data controller under the DPA. In particular, you should take steps to satisfy yourself that:

- there are adequate data protection safeguards in respect of any personal data held outside the BVI (note that 'adequate' is not defined in the DPA); and
- you obtain confirmation from any third party which processes personal data on your behalf that the third party has in place (and complies with) the necessary technical and organisational security measures governing the processing of personal data for the purposes of protecting the personal data from loss, misuse, modification, unauthorised or accidental access or disclosure alteration, or destruction.

Privacy notices: write and provide to natural persons a copy of your privacy notice, explaining how you will process, use and retain personal data of data subjects.

Access to data: be prepared to allow data subjects the opportunity to review the personal data and make any amendments if the data has not been correctly recorded.

5. If you are a bond issuer

The key question BVI bond issuing vehicles should ask is: **have we issued a bond to a natural person?** If the answer to this is yes, then you will be a data controller in respect of your register of bondholders and any data held on that register. Any third party maintaining the register will be a data processor for the purpose of the DPA.

In addition to the steps in section 4 of this guide, you should:

- update your offering memorandum or PPM, indenture and subscription agreements to include (i) a privacy notice in compliance with the DPA, and (ii) acknowledgments about how data has been collected;
- ensure that all data processors employed or engaged by you also agree to process the date in accordance with the DPA;
- formulate an in-house data protection policy; and

- put in place adequate protections and safeguards when passing data to a processor outside the BVI or a GDPR compliant jurisdiction.

6. If you are an investment fund

They key question that investment funds should ask is: **have we issued a limited partnership interest to a natural person?** If the answer to this is yes, then you will be a data controller in respect of your register of limited partners and any data held on that register. Any third party maintaining the register will be a data processor for the purpose of the DPA.

In addition to the steps in section 4 of this guide, above, you should:

- update your offering documents and subscription agreements to include (i) a privacy notice in compliance with the DPA and (ii) acknowledgments about how data has been collected;
- ensure that all data processors employed or engaged by you also agree to process the date in accordance with the DPA; and
- put in place adequate protections and safeguards when passing data to a processor outside the BVI or a GDPR-compliant jurisdiction.

7. Data protection principles

The DPA introduces a number of data protection principles with which a data controller must comply.

The most fundamental principle is the **General Principle**. Under the General Principle, a data controller shall not:

- process personal data (other than sensitive personal data) without the express consent of the data subject;
- process sensitive personal data without meeting the special conditions set out below; or
- transfer personal data outside of the BVI without proof of adequate data protection safeguards or consent from the data subject.

In each case, consent may be withdrawn at any time. Withdrawn consent does not retrospectively impact the legality of data already processed with consent.

However, a data control may process personal data about a data subject where such processing is necessary:

- for the performance of a contract to which the data subject is a party;
- 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 an obligation imposed by a contract;
- in order to protect the vital interests of the data controller;
- for the administration of justice; or
- for the exercise of any functions conferred on a person by or under any law

provided that

- 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.

Sensitive personal data is subject to additional controls. In addition to the above, before processing sensitive personal data of a data subject, the data controller must either (i) obtain the express consent of the data subject, or (ii) establish there are 'necessary grounds' for processing, or (iii) be satisfied that the data subject has deliberately made such sensitive personal data public. The necessary grounds are:

- for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, in order to protect the vital interests of the data subject or another person, in a case where (i) consent cannot be given by or on behalf of the data subject, or (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or (iii) consent by or on behalf of the data subject has been unreasonably withheld;
- to protect the vital interests of the data subject or another person where there are challenges obtaining consent;
- for medical purposes;
- for legal proceedings;
- for the purpose of obtaining legal advice;
- for the purpose of establishing, exercising or defending legal rights;
- for the administration of justice;
- for the exercise of any functions conferred on any person by or under any enactment; or

- for any other purpose as the Minister of Information thinks fit.

The other data protection principles are:

- **Notice and Choice Principle**. Briefly, this requires a data controller, upon requesting data, to inform a data subject of, *inter alia*, the purposes for which the personal data is being collected and the data subject's right to request access to and to request correction of the personal data. The request must also state whether it is voluntary or obligatory.
- **Disclosure Principle**. Personal data should not be disclosed without the consent of the data subject, for any purposes other than the purpose (or a related purpose) for which it was to be disclosed at the time of collection.
- **Security Principle**. This is the requirement to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. It also extends a data controller's obligations to ensuring any data processor also observes security principles.
- **Retention Principle**. Personal data that is processed is not to be kept for longer than is necessary for the fulfilment of the purpose for which it was processed. If no longer required, personal data must be destroyed or permanently deleted.
- **Data Integrity Principle**. Personal data must be accurate, complete, not misleading and up to date.
- **Access Principle**. The requirement to allow data subjects access to, and the opportunity to correct inaccuracies in, personal data.

8. What can data subjects do?

The DPA confers various rights on data subjects, which focus on the right of access to personal data and the right to rectify any incorrect personal data:

- specifically, a data subject may requested to be informed whether his personal date is being processed and is owed an intelligible explanation of how the data is processed, for what purposes, to whom it will be disclosed and any information available as to the source of the data;
- requests for access must be confirmed or denied within 30 days;
- if a data controller or data processor which is a private body receives such a request, it is not obliged to comply:
  - unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the personal data which that person seeks;
  - if compliance with the request will be in contravention of any duty of confidentiality recognised by law; or
  - where another person who can be identified from the personal data consents to the disclosure of his or her personal data to the person making the request;
- data controllers receiving access requests must be able to satisfy themselves of the identity of the person requesting it and further than access will be lawful;
- data subjects may apply in writing to correct any erroneous personal data held by the data controller.

Data subjects suffering damage or distress by reasons of the contravention by a public or private body of the DPA are entitled to institute civil proceedings and may be awarded damages or such other relief as the BVI courts deem fit.

9. Offences

The DPA provides for civil remedies and prescribes a number of criminal offences:

Offence	Punishment
Obstructing an officer of the Information Commission	On summary conviction, a fine not exceeding US$5,000 or imprisonment for a term not exceeding six months
Wilful disclosure in contravention of the DPA	On summary conviction, a fine not exceeding US$5,000 or imprisonment for a term not exceeding six months
Collecting, storing and disposing of personal data in contravention of the DPA	On summary conviction, a fine not exceeding US$5,000 or imprisonment for a term not exceeding six months

Persons breaching confidentiality obligations	On summary conviction, a fine not exceeding US$50,000 or imprisonment for a term not exceeding three years, or both; on conviction on indictment, a fine not exceeding US$100,000 or imprisonment for a term not exceeding five years, or both
A company that commits an offence under the DPA (where the consent or connivance of any human agents, such as directors of the company, is proved, those persons will also be liable to be proceeded against and punished accordingly)	On summary conviction, a fine not exceeding $250,000 and on conviction on indictment to a fine not exceeding $500,000

10. Regulation

The DPA creates the Office of the **Information Commissioner**, the BVI's first data protection regulator, who has responsibility, *inter alia*, for monitoring compliance with the DPA, investigating complaints related to violations of personal data use, advising public and private bodies on their obligations under the DPA.

Further assistance and advice

If you have any questions or require advice as a data controller, data processor or data subject, please contact a member of our dedicated data protection knowledge team or your usual contact at Collas Crill.

COLLAS CRILL

For more information please contact:

Ellie Crespi
BVI Managing Partner | BVI
t: +1 284 852 6335 | **e:** ellie.crespi@collascrill.com