ADVISORY | INDUSTRY INFORMATION

Data Protection in the British Virgin Islands

Introduction

The British Virgin Islands ("**BVI**") Data Protection Act, 2021 ("**DPA**") came into force on 9 July 2021. It was introduced so the BVI would have a data protection framework which is broadly similar to EU and UK standards. To date, no accompanying regulations or codes of practice have been published. This advisory provides an overview of the DPA.

Overview of the DPA

One of the main drivers behind the DPA is to enable the EU and the UK to adopt adequacy decisions in respect of the BVI, which would allow for international transfers of personal data without the requirement for further safeguards.

The DPA requires a data controller to comply with seven data protection principles when processing personal data and to ensure that any data processor it appoints has sufficient safeguards in place to protect the personal data.

The DPA applies to "personal data" processed by a "data controller" or by a "data processor" on its behalf that is:

- established in the BVI; or
- established outside the BVI, but uses equipment in the BVI for processing personal data, other than for transit purposes.

The latter category of persons must nominate for the purposes of the DPA a representative established in the BVI.

In addition, the DPA gives "data subjects" rights to access and rectify their personal data.

BVI businesses and foreign businesses that process personal data in the BVI are likely to fall within the definition of "data controller", which is a person who processes, has control over or authorises the processing of personal data.

A "data processor" is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller.

The term "personal data" means any information in respect of commercial transactions relating to an identifiable natural person, whether living or deceased – referred to as a "data subject". The data subject does not need to be in the BVI.

The term "processing", in relation to personal data, means collecting, recording, holding or storing personal data, or carrying out any operation or set of operations on personal data.

A business that receives personal data from another business and processes that data on behalf of that business is a data processor. Examples include software platform providers, fund administrators and marketing agencies.

Data controllers and data processors in practice

Financial services businesses could be data controllers for some purposes, and data processors for others, depending on the extent of their control over the personal data processed. For example, in their capacity as employers, they would be data controllers with respect to employee personal data, whereas they would be data processors of any client or counterparty personal data.

The DPA has direct application to data controllers, with whom the responsibility for compliance rests, and indirect application to data processors, who will – in practice – be subject to the contractual push down of DPA obligations by data controllers. Data processors that breach their contractual obligations may be liable for damages to the data controller.

While there is no explicit requirement in the DPA for there to be a written agreement between a data controller and a data processor, this would be the industry expectation and assists the data controller with meeting its DPA requirements in respect of the data processor. These are to ensure that the data processor provides sufficient guarantees as to security

measures and takes reasonable steps to comply with the same in relation to personal data processed on the data controller's behalf.

The seven data protection principles

A data controller must comply with the following seven data protection principles, which are summarised below.

1. **General** – No processing of personal data (including sensitive personal data) is allowed without express consent from the data subject or on the meeting of certain other conditions for lawful processing discussed below. Data subject consent or proof of adequate data protection safeguards is required for the transfer of personal data outside the BVI.
2. **Notice and choice** – Upon request to a data subject for personal data, inform the data subject of certain prescribed information discussed below by way of a data privacy notice.
3. **Disclosure** – Limit disclosure of personal data without data subject consent, including such disclosure being necessary to prevent or detect a crime or for the purpose of investigations, or required by law or the order of a court.
4. **Security** – Take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.
5. **Retention** – Personal data must not be kept longer than necessary for the fulfilment of its purpose. No prescribed data retention periods are provided, but should be considered by businesses as part of their internal data protection policies. All reasonable steps must be taken to destroy or permanently delete personal data once it is no longer required for the relevant purpose, and accompanying regulations are expected on this point.
6. **Data integrity** – Take reasonable steps to ensure personal data is accurate, complete, not misleading and up-to-date by having regard to the purpose for which it was collected and processed.
7. **Access** – A data subject must be given access to their personal data and be able to correct it where it is inaccurate, incomplete, misleading or not up-to-date, except where compliance will be in contravention of the exemptions discussed below or any legal duty of confidentiality.

Conditions for lawful processing of personal data

Personal data cannot be processed unless 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 not excessive.

Express consent of the data subject is required, but no definition is provided of the same, although the DPA states that regulations may be made in due course on the conditions for consent. Noting the UK and EU General Data Protection Regulation ("**GDPR**") requirements, best practice would require some form of affirmative action on behalf of the data subject. Consent may also be withdrawn at any time, which could be problematic in practice, especially in a financial services context.

In the absence of express consent, processing is allowed if necessary for one of the following conditions to be met.

1. **Contract** – For the performance of a contract to which the data subject is a party, or the taking of steps at the request of the data subject with a view to entering into a contract.
2. **Legal obligation** –To enable compliance with any noncontractual legal obligation to which the data user is subject.
3. **Vital interests** – Protection of the vital interests of the data subject (generally considered to mean the protection of life).
4. **Administration of justice and legal functions** – To provide for administration of justice and the exercise of any functions conferred on a person by or under any law.

Note that, unlike under the EU and UK GDPR, there is no legitimate interest condition, which allows a data controller to process personal data where, on balance, its legitimate interest does not override the fundamental rights and freedoms of the data subject.

Cross-border transfer

In accordance with the general principle, personal data must not be transferred outside the BVI without data subject consent or proof of adequate data protection safeguards in the recipient jurisdiction. No further exceptions are provided for.

The DPA does not reference a mechanism for ensuring adequate safeguards. We expect accompanying regulations will provide for this, e.g. the use of EU standard contractual clauses pursuant to the GDPR. In the interim, businesses will need to seek consent from data subjects for cross-border transfers.

The BVI has not yet achieved adequacy status from the EU or the UK. However, by implementing the DPA, the BVI has taken steps towards the process of achieving a positive adequacy determination.

Rights of data subjects

The DPA provides for a number of rights of data subjects, summarised below.

- Data subjects are able to request access to their personal data, with further detail on access procedures expected in accompanying regulations. This request has to be made in writing to a BVI public body or a private body, which then has thirty days (extendable in certain circumstances) to respond. There is reference to payment of a prescribed fee in order to provide access, but the amount is not specified. Access can be denied if compliance would contravene the exemptions discussed below or any legal duty of confidentiality. However, data controllers should be prepared for the possibility that personal data may need to be disclosed and ensure there are sufficient systems in place to do so.
- Data subjects can request that incomplete, incorrect, misleading, excessive or irrelevant personal data be amended by the relevant body. Note that this is only a rectification right, is not absolute and does not extend to the personal data being blocked, erased or destroyed. The DPA also states that the personal data as it existed prior to the amendment should not be obliterated.
- There is no explicit right for data subjects to demand that processing cease. However, if processing is based on consent, which is subsequently withdrawn, and the data controller has no other grounds under which it can justify the processing, it would need to cease.
- The DPA introduces an absolute right for individuals to require that processing for the purposes of "direct marketing" cease or not begin. "Direct marketing" means the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.
- A data subject is able to complain to the BVI Information Commissioner (not yet appointed) about alleged violations of the DPA, and to institute civil proceedings for damages in the High Court.

Data subjects also have the right to be informed by way of a data privacy notice, as discussed further below.

Data privacy notice

Under the notice and choice principle, a data controller must inform a data subject of the following upon a request for personal data.

- The purposes for which the personal data is being collected and processed.
- Any information available as to the source of the personal data.
- The data subject's right to request access to, and correction of, the personal data, along with the data controller's contact details (including those of its representative, where relevant).
- The class of third parties to whom the data controller may disclose the personal data.
- Whether it is obligatory or voluntary to supply the personal data and, where the former, the consequences for the data subject in failing to do so.

Although not specified, in accordance with other data protection regimes, we would expect this information to be provided in the form of a data privacy notice. While there is no timeframe specified under the DPA, best practice would be to provide the privacy notice at each point of personal data capture, e.g. an investment fund would likely include it within its subscription agreement or equivalent.

Data security, integrity and confidentiality

Data controllers are required to take practical steps to protect personal data, taking into account its nature and the harm that would result from its loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. In this respect, data controllers should have regard to the following factors.

- The physical location of personal data storage.
- Technological means by which security measures are incorporated into personal data storage equipment.
- Sufficient staff competence and training where they have access to personal data.
- Systems and processes for ensuring the secure transfer of personal data.

On the wider cybercrime front, businesses should also be aware of the BVI Computer Misuse and Cybercrime Act, 2014, which prohibits the unauthorised access, modification and use of data held on a computer or any computer service, and the knowing disclosure of passwords or other means of access to a computer, with a view to cause loss, gain or for any unlawful purposes.

Personal data breaches

There is no requirement for data controllers to register with the BVI authorities and the DPA does not provide for the notification by data controllers of personal data breaches to the relevant data subject or the BVI Information Commissioner.

Businesses should still have processes in place to deal with the identification and handling of a personal data breach as part of their wider business continuity planning, noting also that breach notification elsewhere may be a requirement for those with cross-border operations.

Data controllers may also wish to consider courtesy notifications to data subjects and the BVI Information Commissioner (once appointed) as a matter of best practice in the case of a serious breach.

Internal data protection policy

There is no specific requirement under the DPA for a data controller to have an internal data protection policy, but it is a general industry expectation and, from a practical perspective, having documented policies and procedures in place will assist businesses with handling any data subject requests, personal data breaches or complaints received.

Businesses are not required to appoint data protection officers under the DPA, but it would be best practice to do so, and aid in the robustness of internal data protection policies.

Exemptions

The DPA provides for an absolute exemption for personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

There are a number of partial exemptions provided for under the DPA, which exempt personal data processed for the following reasons from the application of certain data protection principles (commonly, the general, notice and choice, disclosure and access principles).

- Crime prevention and prosecution.
- Tax assessment or collection.
- Physical or mental health data likely to cause serious harm to the data subject.
- Preparation of statistics or carrying out research that does not identify the data subject.
- Order or judgment of a court.
- The proper discharge of regulatory functions.
- Journalistic, literary or artistic purposes.

In the majority of cases, the security, retention and data integrity principles continue to apply in the case of a partial exemption, along with the wider DPA provisions.

Enforcement

The DPA bestows power on the BVI Information Commissioner to investigate complaints, serve information and enforcement notices, carry out an assessment of the processing of personal data, and request a warrant to enter and search premises. A data subject that is aggrieved by the decision of the BVI Information Commissioner may appeal to the High Court against the decision.

Obstruction, willful disclosure of information, breach of confidentiality and body corporate offences are all punishable under the DPA by way of fines of up to USD 500,000 and/or prison sentences of up to 5 years on conviction on indictment.

For body corporate offences, where committed with the consent or connivance, or attributable to the neglect, of any director, manager, secretary or similar officer (or purporting to act in that capacity), the individual is also deemed to have committed the offence.

Practical measures

To demonstrate compliance with the DPA, BVI businesses or those with data processing equipment in the BVI, will need to have taken the following practical measures.

- Consider the application of the DPA to the business, including whether, and in what circumstances, the business would be considered a data controller or data processor, and the extent of any exemptions that may apply.
- Analyse how and when personal data is currently processed.
- Determine whether there is a lawful basis for the processing of personal data.
- If personal data is transferred out of the BVI, determine whether subject data consent has been obtained or if there is a case to rely on adequate safeguards.
- Prepare, review and update, where necessary, documentation where personal data is being processed as a result of a business relationship, e.g. client and service provider agreements, offering and transactional documents and employment contracts.
- Prepare a data privacy notice.

- Prepare or update an internal data protection policy, providing for sufficient procedures to allow staff to recognise and promptly respond to data subject requests and react to data breaches.
- Establish and maintain a plan to deal with a potential data breach.
- Train relevant staff.

Next steps

This advisory provides an overview of the DPA, which provides for similar, but lighter touch, data protection regulation than the EU and UK GDPR, and other jurisdictions in the region. At present, there are no accompanying regulations or codes of practice published alongside the DPA, but we expect these in due course.

Given the cross-border nature of many BVI businesses, careful consideration will also need to be given to the potential extra-territorial effect of other data protection regimes. The application of data protection requirements will need to be considered on the facts in each case.

Walkers' Regulatory & Risk Advisory practice group comprises a team of dedicated specialist lawyers who will be happy to advise on all aspects of data protection requirements, as well as reviewing and preparing data privacy notices, internal data protection policies and agreements between data controllers and data processors.

Key Contacts

Lucy Frew
Partner
lucy.frew@walkersglobal.com
+1 345 814 4676

Sara Hall
Partner
sara.hall@walkersglobal.com
+44 (0)20 7220 4975

Colm Dawson
Partner
colm.dawson@walkersglobal.com
+852 2596 3357

Daniel Wood
Managing Partner
daniel.wood@walkersglobal.com
+971 4 363 7912

Iona Wright
Senior Counsel
iona.wright@walkersglobal.com
+1 345 914 6356

John Rogers
Managing Partner
john.rogers@walkersglobal.com
+65 6595 4673

© 2023 Walkers | Disclaimer: The information contained in this advisory is necessarily brief and general in nature and does not constitute legal or taxation advice. Appropriate legal or other professional advice should be sought for any specific matter.