BEYOND LAW AND COMPLIANCE

DATA PROTECTION ACT 2021

BDO

Today, data has become one of the most valuable assets of any organisation and every person, and therefore the most desirable object for cybercriminals. Most cyberattacks are aimed at stealing information, damaging, and changing internal data, and destroying confidential information.

With the importance of data, cybercrime prevention is becoming increasingly necessary. This set of actions is aimed at ensuring an adequate level of data security and compliance with all cybersecurity measures that help organisations find, identify, and respond to cybercrime.

At an individual level, a cybersecurity threat can lead to identity theft, data loss, extortion, etc. At an organisation level, the consequences can be in the form of damage or destruction of a company's IT infrastructure. It is necessary for all companies and organisations that collect data to develop a cybersecurity plan. The stages of preparation and prevention of cyber-attacks are of key importance, since in case of a real attack, recovery can be time-consuming and costly, and sometimes even impossible.

The benefits of cybersecurity include:

- reduction of the risk of data corruption and security breaches;
- saving money that needs to be spent on repairing damage;
- protection customer privacy and increasing loyalty;
- maintenance of the integrity of the organisation;
- competitive advantage by improving, optimizing, and protecting business processes.

The field of cybersecurity spans a wide range of disciplines, behaviours, dangers, and concepts. Protecting people's digital lives and assets, though, is the common issue that runs through all of these sections. Protecting things like digital currency, data, is essential because they make lucrative targets for criminals.

Due to the prevalence of cybercrime, cybersecurity is crucial. In 2019, 32% of firms reported about cyberattacks or other security lapses.

Data management systems, sensitive data security tools, data loss prevention services, vulnerability scanners, and threat detection are all used in data protection software to protect your company against theft, loss, and unauthorised usage.

BEYOND LAW AND COMPLIANCE: OVERVIEW OF BVI'S DATA PROTECTION ACT, 2021

A number of laws and regulations affect businesses today. The topic of privacy is receiving extra attention from legislators and regulators. Businesses are motivated today, more than ever, to ensure compliance with these laws and regulations because they want to protect their brand name, reputation, and consumer/client trust.

In 2021, the Government of the Virgin Islands enacted its own privacy law called Data Protection Act, 2021 (the "Act"). The Act aims to safeguard personal data being processed by organisations, public bodies, and private bodies, from unlawful processing and to promote transparency and accountability in the processing of personal data. The Act contains seven privacy and data protection principles:

1. THE GENERAL PRINCIPLE
2. THE NOTICE AND CHOICE PRINCIPLE
3. THE DISCLOSURE PRINCIPLE
4. THE SECURITY PRINCIPLE
5. THE RETENTION PRINCIPLE
6. THE DATA INTEGRITY PRINCIPLE
7. THE ACCESS PRINCIPLE

It also sets out the rights an individual (data subjects), exemptions for personal data being processed, establishment of the Office of Information Commissioner, including IC's enforcement power, and offences. This paper focuses on the seven privacy and data protection principles.

BEYOND LAW AND COMPLIANCE: OVERVIEW OF BVI'S DATA PROTECTION ACT, 2021

What do we mean by personal data? The Act defines personal data as

> *"any information that identifies an individual, directly or indirectly, including any sensitive personal data and expression of opinion about the individual."*

Transparency and accountability are core principles in the Act. Individual has the right to know which personal data are collected and processed by organisations. Transparency is critically important, so it is crucial to provide individuals with information about privacy practices at the time of personal data is collected. This can be done through privacy notices. Accountable organisations have the proper policies and procedures to promote properly handling of personal data and can demonstrate they have the capacity to comply with applicable privacy laws. It is about not only saying the organisation is taking action, but actually being able to prove that it is. As Bob Siegel, the founder and president of Privacy Ref, Inc., explains:

> *"It is not enough for a business to create a privacy policy and place it on its website; a business must define policies and practices, verify that their employees are following the practices and complying with policies, and confirm that third-party service providers are adequately protecting any shared information as well. As customer demands and regulatory requirements change, the business' privacy practices and policies must be reviewed and revised to meet this changing business environment."*

PRIVACY AND DATA PROTECTION PRINCIPLES

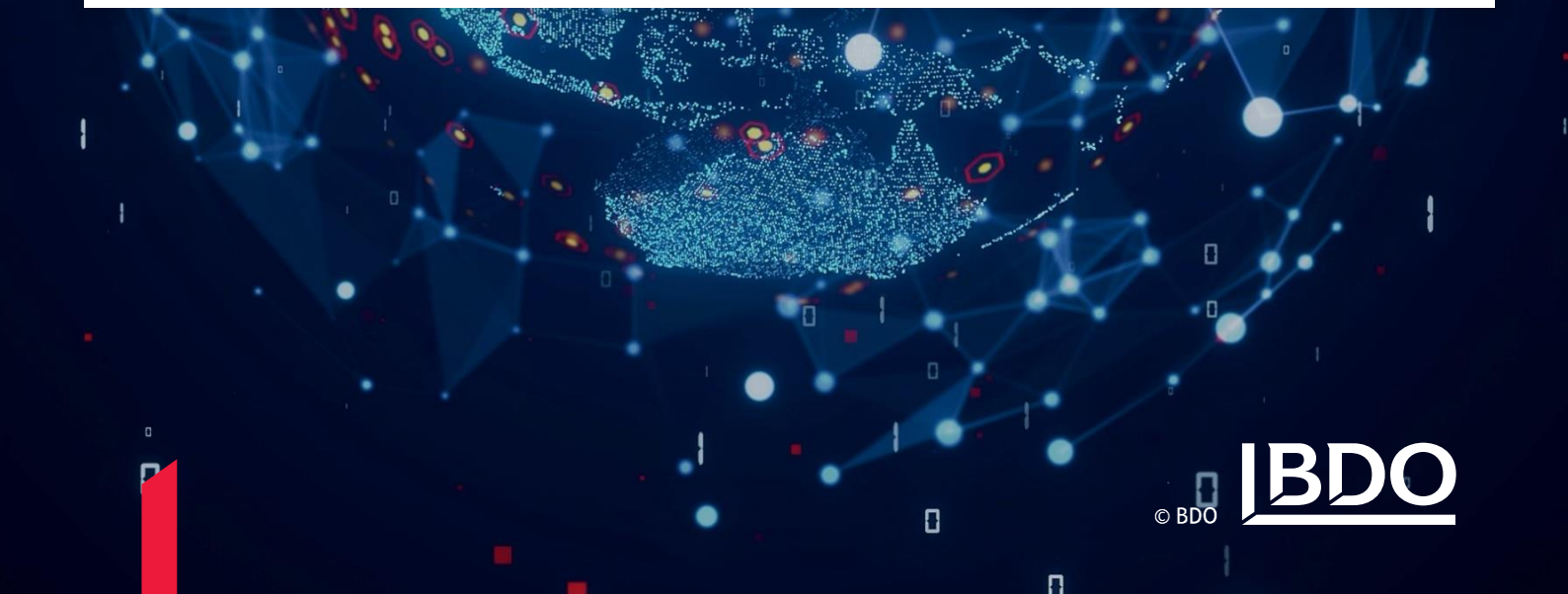
General principle requires a data user (in GDPR, this is equivalent to a data controller) to obtain a consent before processing personal data. An explicit consent is required by the Act if the processing involves sensitive personal data

If consent is required by a law or regulation, there must be a method for obtaining and recording it. Further, organisations should not process personal data in a manner incompatible with the consent.

Notice and choice principle requires a data user to inform individual,

i. upon request of personal data, of the purposes the personal data is being collected and further processed;
ii. of any information available to the data user as to the sources of the personal data;
iii. of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
iv. of the class of third parties to whom the data user discloses or may disclose the personal data;
v. whether it is obligatory or voluntary for the data subject to supply the personal data; and
vi. where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he or she fails to supply the personal data.

Privacy Notice, also known as Privacy Statement, is an external document directed to current or potential customers, clients, or users. A tool used to describe organisations privacy practices The goal of the privacy notice is to help recipients make informed privacy decisions. It can also be considered as a promise that organisation makes to data subjects. If the organisation breaks those promises, it may face regulation actions or litigation. European Data Protection Board including Fair Trade Commission of United States of America has endorsed layered approach in providing privacy notices. A layered approach provides a high-level summary of the various sections of the privacy notice. It also allows the users to read more about a section of the privacy notice by clicking a link to that section or scrolling below. Other ways to provide data subjects with notices is through just-in-time notice, by using icons or symbols, and privacy dashboard.



PRIVACY AND DATA PROTECTION PRINCIPLES

Disclosure principle states that no personal data shall be, without the consent of the data subject, disclosed for any purposes other the purpose for which the personal data was to be disclosed at the time of collection. In addition, disclosure shall not be to any party other than a third party of the class of third parties to whom the data user discloses of may disclose the personal data.

Organisations should only disclose personal data if consent or authorisation from the data subject has been obtained. Data subjects should always be informed from the time of the collection of the information, through a privacy notice, with whom your organisation will share the information. Organisations should ensure confidentiality of personal data being held by putting in controls and processes in place, for example access control policy should be established. This will minimise the risk of unauthorised disclosure of personal data.

Security principle requires a data user to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction. A data user should also ensure that the data processor processing personal data on his or her behalf provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and take reasonable steps to comply with measures in place.

Privacy requires security. Privacy addresses the rights of data subjects to control how and to what extent information about them is collected and further processed. Information security is about assuring confidentiality, integrity, and availability of information assets (CIA triad). Managing privacy within an organisation requires involvement and contribution of many members within an organisation. The information security group is strongly aligned to the privacy group than any other party in the organisation. The information security group ensures that appropriate controls (physical and technical) are in place. Information technology group supports privacy group by adding processes and controls that support privacy principles (i.e. creating processes to develop and test software and applications). For small to mid-sized organisations, information security group and information technology group roles and responsibilities might be assigned to one or two employees, sometimes outsourced to a service provider. This is where the involvement of those charged with governance becomes critical as they need to ensure that administrative controls (policies) are in place. On another note, data users who have entrusted data processors to process personal data should ensure that the same level of safeguards are being applied to personal data by the data processors. The concept of sufficient guarantees is much more than the creation of contracts. Data user should focus in obtaining proof of the data processor's competence.

PRIVACY AND DATA PROTECTION PRINCIPLES

Retention principle states that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The data user should also take all reasonable steps to ensure that personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

A key component of information management is appropriate destruction of data and/or information in any format or media. To protect personal data and ensure privacy, information should be destroyed when it is no longer needed. Privacy professional will need to work closely with those in-charge with data retention function, i.e. information security group, to ensure policies, procedures and guidelines are in place to properly handle personal information when it is intended to be destroyed.

Data integrity principle requires data users to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

Integrity is the assurance that data is authentic and complete. Integrity is to information security and accuracy is to privacy. This is one of the overlaps between the two practices. Information security's focus on data integrity overlaps with the privacy's accuracy requirement where in both wants to ensure that data is not altered without authorisation. The doctrines of information security and privacy requires data users and data processors to be responsible for protecting data.

Access Principle gives data subject access to his or her personal data being held by a data user and give the data subject the ability to correct that personal data when data is inaccurate, incomplete, misleading, or not up to date expect where access or correction is refused.

Privacy's access principle is supported by the information security's availability concept. If data is not available, it cannot be accessed. Availability means information is readily accessible to authorised users, in this case - user will be the data subject. Access requests from data subjects can pose substantial administrative burdens on organisations. At the earliest stage of designing a privacy program practice, organisations should consider what types of processes need to be in place to assist with this task.

Endnotes

Compliance to existing privacy laws and regulations, protecting personal data and building a program that drives privacy principles cannot be the left in the hand of just one employee or department. Key members across the organisation, specially those handling or have access to personal data, should work closely together to execute on a vision and making strategic decision to start up a privacy program.

BDO BRITISH VIRGIN ISLANDS

RYAN GELUK

Managing Director

BDO Limited

+1 284 541 0746 (mobile)

+1 284 852 6204 (direct)

ryan.geluk@bdo.vg

Follow on LinkedIn

REVA A. DAULO

CPA, CISA, CIPM, CIPP/E, DipBCM, BCRP

BDO Limited

+1 284 852 6229 (mobile)

reva.daulo@bdo.vg

Follow on LinkedIn

Contact address:

BDO Limited
PO Box 34
Sea Meadow House,Tobacco Wharf
Road Town
Tortola VG1110
BRITISH VIRGIN ISLANDS

+1 284 852 6200
+1 284 494 3783

www.bdo.vg