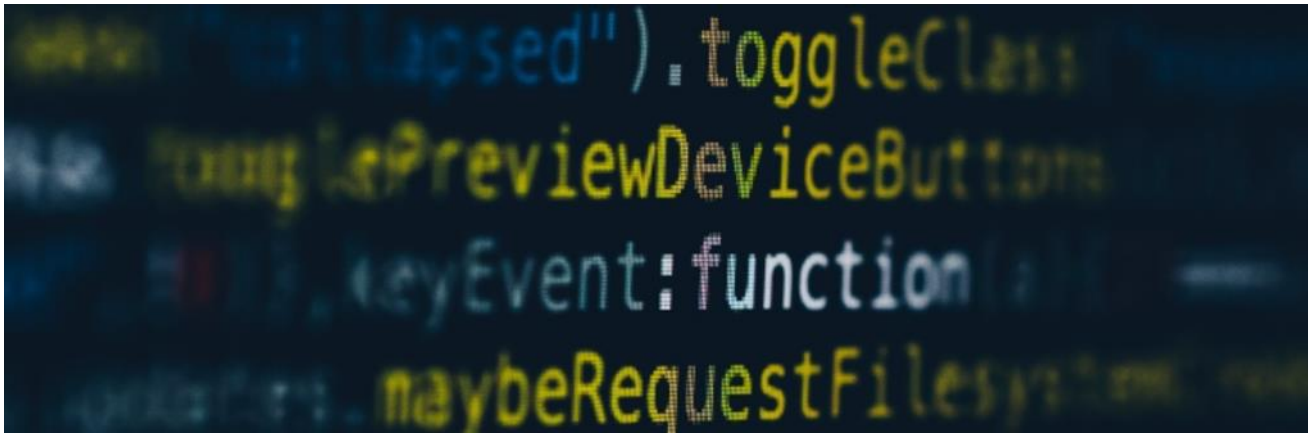
Why Data Privacy and Cybersecurity are Increasingly Important?

November 2020

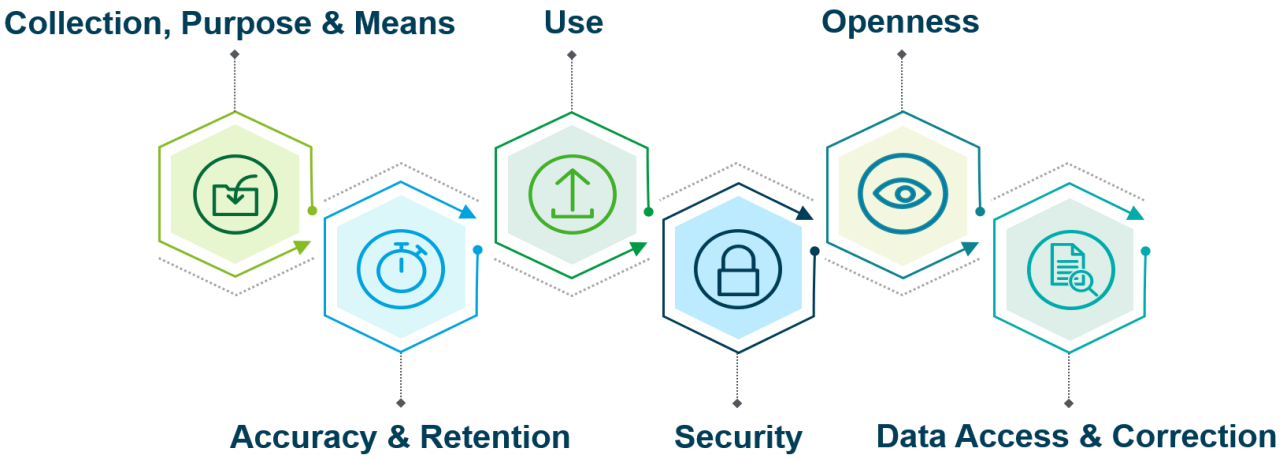


With the outbreak of COVID-19 around the world in early 2020, organizations have taken steps, including the most popular Work-from-Home ("WFH") arrangement, to mitigate its impact. However, though working from home is a solution to avoid frequent close human contacts, it brings up another issue – "data breaches" which occur now and then. Thus, cybersecurity comes into the picture and becomes the main focus of management. Meanwhile, organizations across different market sectors are subject to an increasing pressure from the community to strengthen their internal control mechanism as to how they collect, process, store and delete personal information, and how they manage data privacy. Moreover, along with the extensive use of telecommunication technology in the daily business operations to minimize physical travelling as much as possible, the pressure on each organization in monitoring its IT infrastructure, such as cloud computing storage, and remote dial-in access channel, etc., has been increasing. In this respect, it is essential for the organizations to ensure proper functionality and timely responsiveness of their data protection mechanism.

The concern of preserving data privacy is driven by the need to defend the cyber-attacks that can lead to massive breaches of personal data. As a result, regulations designed to strengthen consumer privacy protection have been developed in the countries around the world. For instance, the European Union ("EU") enacted the General Data Protection Regulation ("GDPR") in 2018 that sets guidelines for the collection and processing of personal information from those individuals who live in the EU. Locally in Hong Kong, the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486), which is similar to GDPR, was long enacted in 1995, and points out how individuals must be informed about the fact of data collection and the ways that their personal data can be used. Here is a summary of data privacy compliance requirements in the globe:

Hong Kong

In Hong Kong, the PDPO is to protect the privacy rights of a person in relation to the personal data (i.e. a "Data Subject"). In this respect, there are Six Data Protection Principles covering the life cycle of a piece of personal data:



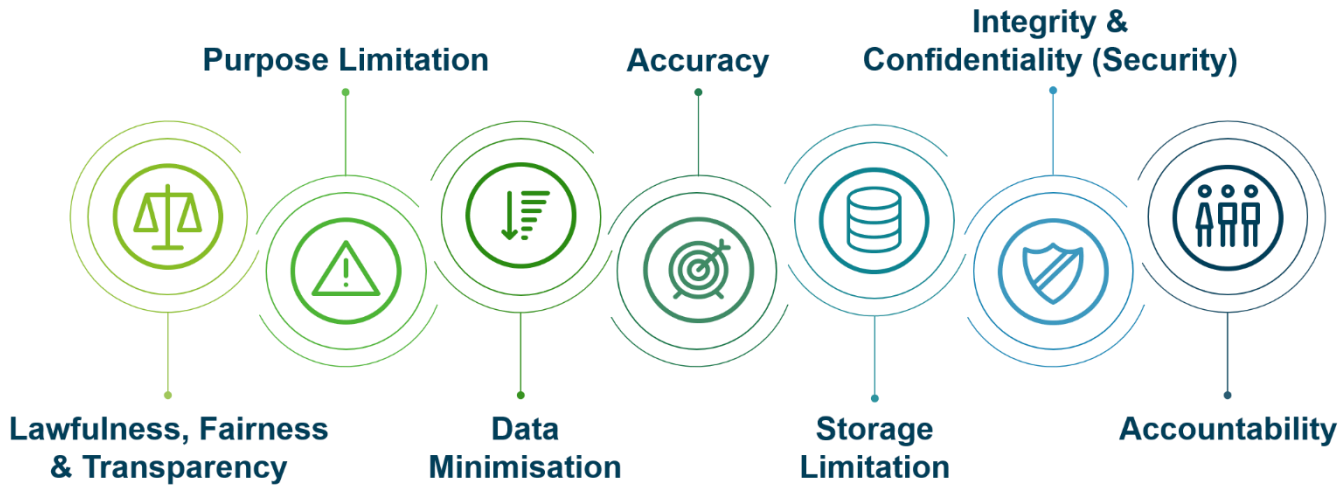
Penalty of data breaches:

- Breaches of the PDPO may lead to a variety of civil and criminal sanctions, including fines and imprisonment;
- The use of personal data in direct marketing without the data subject's consent is a criminal offence punishable by a fine of HK$500,000 and imprisonment for 3 years, or up to a fine of $1,000,000 and imprisonment for 5 years, if the data are provided to a third party for the purpose of gain.

European Union

GDPR is a piece of regulation in EU law specifically on data protection and data privacy throughout the countries of the EU. The primary aim of GDPR is to enable individuals to have some degree of control over the use of their personal data by any organizations who have the access to their personal data, and to simplify the regulatory environment for the international businesses by unifying the regulation of all countries within the EU.

There are Seven Data Protection Principles covering the life cycle of a piece of personal data:



Penalty of data breaches:

- Depending on the nature of the breach, the fine could be up to €20 million or 4% of the total worldwide annual turnover;
- Data protection authorities are empowered to impose administrative fines on data controllers and processors.

China

In the past, there was no data protection law in regard to individuals similar to the PDPO and the GDPR. The regulations concerning the protection of personal information are embedded in various laws, such as the Law on Protection of Consumer Rights and Interests (2nd Amendment, 2013), Criminal Law (9th Amendment, 2015), Cybersecurity Law (2017) and E-Commerce Law (2019), etc. In this regard, the Measures for Data Security Management (2019), to some extent, supplements the provisions under the Cybersecurity Law by providing more detailed requirements in respect of the protection of personal information and the administration of security over important data. In response to the data protection concerns, a draft of the Data Security Law was recently published on the National People's Congress official website in July 2020. It is expected that details of the regulatory requirements relating to data security will soon be announced in the new piece of Data Security Law in the near future.

In this respect, the following principles are covered in Chapter 4 of the draft of the Data Security Law in the area of personal data protection:

- Set-up of sound data security management system
- Promotion of economic growth, social morality and ethics in the process of data technological development
- Strengthening risk monitoring during the process of handling data
- Performing regular risk assessment in respect of data collection, storage, processing, and usage
- Ensuring lawful and proper collection and use of personal data
- Providers of data media services to understand data sources and verify the identity of the parties involved in a transaction
- On-line data service operators to obtain valid business licence
- Domestic law enforcement agencies to access data in accordance with the relevant national laws and regulations
- Overseas law enforcement agencies to access data in accordance with the relevant international treaties

Penalty of data breaches:

- Breaches of the Data Security Law may lead to a variety of civil and criminal sanctions;
- Depending on the nature of the breach, the fine could be up to 10 times of the illegal income, or up to RMB 1 million for an organization and up to RMB 100K for a data controller.

Management's Role in Data Privacy and Data Protection

Against the backdrop of the concerns of data privacy on the part of the various parties with the WFH landscape, community awareness and demand for the data privacy rights in the fear of leakage of personal data have been growing at a rapid pace. Although accountability is not explicitly stated under the regulatory requirements, the common view is that management (including the board of directors) is often the target to be held accountable, when there is a data breach and the necessary data security controls are not found to be in place.

In short, management needs to be aware of the risks relating to cybersecurity and data privacy matters, and should ensure that the organization has set up and maintains adequate and effective internal control system to tackle all cybersecurity and data privacy risks.

The Way Forward

Business information and technology are converging rapidly. With data protection becoming the key success factor of every business, it becomes the most important matter for an organization to have thorough understanding of the relevant cybersecurity risks so that the organization can adopt best practice in the area of information security with the set-up of a well-structured data security framework.

What Can BT Corporate Governance Limited ("BTCGL") Assist You?

BTCGL, an operating entity of Baker Tilly Hong Kong, is well prepared to lend you a hand in building up our internal control system in order to cope with the cybersecurity and data breach threats. If you are interested in our quality services, please don't hesitate to contact us. The following are the most popular services we offer to our clients:

Cybersecurity Risk Assessment

BTCGL's cybersecurity risk assessment will provide management with a snapshot of existing data protection measures in response to the cybersecurity risks, together with system improvement recommendations to address the system deficiencies identified.

Our cybersecurity risk assessment approach includes the following:

- **Classify** IT assets and infrastructure;
- **Identify** system vulnerabilities;
- **Evaluate** threats to the system vulnerabilities;
- **Determine** risk likelihood and impacts;
- **Analyse** the level of risks identified; and
- **Recommend** remediation plan for improvements.

ISO27001 ISMS Consultancy

ISO27001 is recognized as the international standard for securing business information assets. It provides a framework to minimize the threats to information and communication technology assets and the business. According to the International Organisation for Standardisation ("ISO"), ISMS is a systematic approach to managing sensitive company information and can be implemented in small, medium and large businesses in any industry sectors.

BTCGL will provide assistance to the organization in its implementation of ISO27001 framework. Our ISO27001 consultation approach includes the following:

- Perform gap analysis between current practice and ISO27001 standard;
- Assist organization to review the ISMS related policies and procedures;
- Support user information security awareness training;
- Conduct Internal audits and follow-up reviews; and
- Provide on-site support during the certification process.

BT Corporate Governance Limited

How can we help you reach new heights?

Contact Us

Doman Wong
Executive Director
D: +852 2152 2632
domanwong@btcgl.hk

Andrew Pang
Associate Director – IT Audit
D: +852 2152 2642
andrewpang@btcgl.hk