MARCH 2018
WWW.BDO.COM.HK

BDO NEWS

BE PREPARED FOR COMPLIANCE WITH THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

Following a lengthy adoption process that began in April 2016, the EU General Data Protection Regulation (GDPR) will take effect from 25 May 2018 throughout the countries of the European Union. The GDPR will replace existing data-protection laws throughout the EU, but it will have a significant impact on businesses around the world, regardless of where they operate. Time is running out: if Hong Kong businesses have not yet addressed the GDPR requirements, they should immediately assess how the GDPR will impact their business and update their data-protection policies and practices to comply with the requirements.

The GDPR aims to strengthen the laws on the protection of 'privacy data' that relates to an identified or identifiable 'natural person' (ie, one who has its own legal personality). Privacy data includes the following:

- basic information about a person's identity, such as their name, address and ID number;
- web data, such as location, IP address, cookie data and radio-frequency identification tags;
- health and genetic data;
- biometric data;
- racial or ethnic data;
- data about their political opinions; and
- data about their sexual orientation.

Any organisation that stores or processes personal information about EU citizens in EU states must comply with the GDPR, even if they do not have a business presence in the EU. An organisation must comply with the GDPR requirements if it:

- has a presence in an EU country;
- does not have a presence in an EU country but offers goods or services to individuals in the EU or monitors an identifiable natural person (data subject)'s behaviour in the EU (monitoring behaviour could include using cookies to track online activity and develop user profiles, even without knowing the users' names);
- has more than 250 employees; or
- has fewer than 250 employees but processes their personal information in a way that would affect the rights of data subjects repetitively.

To enforce the requirements of the GDPR, the European Parliament is introducing the following significant changes:

- GDPR defines three roles that are responsible for ensuring compliance: the data controller, the data processor* (see the note below) and the data protection officer (DPO). The data controller defines how personal data is processed and the purposes for which it is processed. The data controller is responsible for making sure that external contractors comply with the regulation. The GDPR requires organisations to appoint a DPO, and the data controller and data processor must assign the DPO to overseeing the organisation's data security strategy and GDPR compliance.

- The conditions for requesting permission to use personal data have been made stricter. Organisations must obtain permission separately from other permissions and ask for it in a way that is easy to access and understand, using clear and plain language. The consent for requesting the withdrawal of the use of personal data should also be the same as the request for consent to use it.

- The rights of data subjects have been strengthened and new rights have been introduced. These include the following:

  - the right to transfer their data to another processor (known as 'data portability');
  - the right to require the data controller to erase their personal data, to require them to stop sharing it with others, and, potentially, to have third parties stop processing the data (known as 'data forgotten'); and
  - the right to obtain confirmation from the data controller about whether or not their personal data is being processed, where it is being processed and for what purpose it is being processed (known as 'data access').

- Organisations must notify the regulatory authorities and the individuals concerned about any data breaches (eg, accidental or unlawful loss of, theft of, access to or disclosure of personal data) within 72 hours of noticing the breach.

- Data processors (ie, organisations that process personal data on behalf of other organisations) are now directly and legally responsible for complying with several obligations set out in the GDPR, including ensuring that the data is protected at the technical and organisational level.

- The GDPR does not require all personal data to be kept within the EU. However, if personal data is transferred outside the EU, data controllers should ensure that there is a similar level of technical and legal protection for the data. Therefore, the GDPR implements 'privacy by design', which calls for data controllers to protect personal data and consider the amount of personal data collected, how long it is kept for and how it can be accessed.

- For the most serious offences, the maximum fine that can be imposed for breaking the conditions of the GDPR is €20 million or four per cent of an organisation's worldwide turnover, whichever is highest.

In anticipation of the changes in the data-protection laws in EU countries, we have looked at the Personal Data (Privacy) Ordinance (Cap 486) (PDPO). The PDPO came into force in Hong Kong on 20 December 1996, just one year after the European Data Protection Directive of 1995, and certain aspects of the PDPO were developed based on the directive. The PDPO set out principles that data users must follow when handling personal data about individuals. The PDPO and the GDPR cover some of the same subjects. Their definitions of these subjects are set out below:

*Note: Data processors may be internal employees or an internal department that maintains and processes records of personal data, or any outsourcing vendor that performs all or some of those activities. The GDPR holds data controllers and data processors legally responsible for breaches or non-compliance. Therefore, both the organisation and a processing partner (such as a cloud provider) may be liable for penalties, even if the fault is entirely that of the processing partner.

Subject	PDPO	GDPR
Personal data	Personal data is any data: (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable. * Examples of personal data protected by the ordinance include names, phone numbers, addresses, identity card numbers, photos, medical records and employment records.	Personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier (such as a name, an identification number, location data or an online identifier) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data subject	In relation to personal data, the data subject is the individual who the data is about.	The data subject is an identified or identifiable natural person.
Data controller	This is the 'data user'. In relation to personal data, the data user is a person who, either alone or with others, controls the collection, holding, processing or use of the data.	The data controller is the natural or legal person, public authority, agency or other body that, alone or with others, determines how personal data is processed and for what purpose. If the purposes and methods of data processing are set by the EU or member state law, the controller or the specific criteria for its nomination may be provided for by Union or member state law.
Data processor	As part of the 2012 amendment, a data processor: (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes. In relation to personal data, a 'third party' is any person other than: (a) the data subject; (b) a relevant person in the case of the data subject; (c) the data user; or (d) a person authorised in writing by the data user to collect, hold, process or use the data (i) under the direct control of the data user; or (ii) on behalf of the data user.	The data processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. A 'third party' is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and people who, under the direct authority of the controller or processor, are authorised to process personal data.
Sensitive data	None	**Article 9:** It is forbidden to process: • personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

		• genetic data and biometric data for the purpose of uniquely identifying a natural person; and • data concerning health or a natural person's sex life or sexual orientation.
Transfer of personal data to third countries or international organisations	There are no requirements on the cross-border transfer of personal data.	Any transfer of personal data that is being processed or is intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions of **Articles 44 – 50** are complied with by the controller and processor to ensure the level of protection of natural persons that is guaranteed by the GDPR. Transfers on the basis of an adequacy decision and methods such as Business Card Recognition (BCR), contract clauses, etc or in the case of transfers from the European to the United States, the Privacy Shield.
Data portability	A data subject must be given access to his or her personal data and allowed to make corrections if it is inaccurate.	**Article 20:** The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
Penalty	Non-compliance with data protection principles does not constitute a criminal offence directly. The commissioner may serve an enforcement notice to tell the data user to remedy the contravention or it may instigate the prosecution action (or both). Contravention of an enforcement notice is an offence which could result in a maximum fine of HK$50,000 and imprisonment for two years. An individual may seek compensation from the data user if the person suffers damage, including injured feelings, due to a contravention of the ordinance in relation to his or her personal data. The ordinance also criminalises misuse or inappropriate use of personal data in direct marketing activities (Part VI); noncompliance with data access requests (section 19); unauthorised disclosure of personal data obtained without the data user's consent (section 64), and other offences.	**Under Article 83:** • Up to EUR10,000,000 or in the case of an undertaking, up to two per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements of obligations such as controllers and processors, the certification body, and the monitoring body. • Up to EUR20,000,000, or in the case of an undertaking, up to four per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements of obligations such as principles of processing, conditions for consent, data subject's rights, transfer beyond the EU, and so on. • Under **Article 84**, each member state can lay down the rules on other penalties applicable to infringements of GDPR in particular for infringements that are not subject to **Article 83**, and can take all measures necessary to ensure that they are implemented.

Source: The Privacy Commissioner for Personal Data, Hong Kong

Members of senior management team should undertake a holistic review of whether their organisations are ready for GDPR compliance. Your organisation may consider taking the following steps to prepare:

1. Conduct an information audit to map data flows and document what personal data you hold, where it came from, who you share it with and what you do with it. Address the risks of cross-border transfer of personal data, especially in virtual and cloud environments, where cross-border data replication and movement is common.

2. Designate a team of key members of the senior management team, IT and various operational and support departments to develop a plan for GDPR compliance and educate others about its impact on operations.

3. Appoint a Data Protection Officer to implement and monitor your GDPR compliance plan. This person should act as the head of your data protection governance structure and report directly to the senior management. If your business operates outside the EU, you will need to appoint a representative within the EU in writing.

4. Ensure an appropriate data-protection policy is in place and review the basis for collecting, processing and maintaining personal data, especially the rights to access, accuracy, quality, retention and disposal of personal data.

5. Implement a new compliance system with built-in technical and organisational measures for integrating data-protection functions into all processing activities from your end points.

6. Review your contracts with third parties and customers with whom personal data is shared and, where necessary, renegotiate terms of business to ensure appropriate supervision over the processing of personal data and compliance with the GDPR.

To minimise the risk to your business operations after the regulation takes effect on 25 May 2018, you should act immediately to address the requirements of the GDPR.

BDO'S SUPPORT AND ASSISTANCE

If you have any questions regarding this publication, please feel free to contact us:

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

JOSEPH HONG
Director & Head of Payroll & HR Outsourcing Services
Tel: +852 2218 8286
josephhong@bdo.com.hk