New EU Data Protection Regulation Set to Have Impact on Hong Kong Companies Operating in the EU

01/06/2018
Source: Extract from HKTDC

On 25 May 2018, the new General Data Protection Regulation (the GDPR) became directly applicable throughout the European Union. This new instrument, which establishes a harmonised set of rules on the protection of the personal data of individuals, replaces the current framework of the old Data Protection Directive 95/46/EC and its national implementing laws.

The GDPR builds on existing concepts and strengthens requirements for the collection and use of personal data. In addition, it introduces a number of significant changes, in particular:

- Controllers will be obliged to document the tools and decisions they take to comply with the GDPR in order to be able to demonstrate compliance (principle of accountability). Certifications and codes of conduct can help Hong Kong businesses to demonstrate compliance.
- Many companies will have to keep an internal register of all their activities involving the processing of personal data. On the other hand, the obligatory registrations or notifications of data processing activities, which currently exist in many EU Member States, are abolished.
- Requirements for obtaining consent from individuals have become stricter. As a result, companies may need to review and adapt their consent mechanisms.
- The information that needs to be provided to individuals and the manner in which this information must be provided, are described in more detail under the GDPR. Accordingly, Hong Kong businesses need to update their notices to European data subjects, including website policies, user terms & conditions and/or employee notices.
- The rights of data subjects are strengthened and new rights are granted. These include, for example, a right for data subjects to transfer their data to another processor (data portability) and a right to require the data controller to erase their personal data without undue delay in certain situations, such as where they withdraw consent and no other legal ground for processing applies. Hong Kong businesses will need to set up procedures and processes to deal with such requests.
- Companies will have to notify data breaches (e.g., accidental or unlawful loss, theft, access or disclosure of personal data). This means that personal data protection breaches will need to be notified, within 72 hours, to the supervisory authorities; and, in certain cases, the individuals concerned will need to be informed.

- In addition, data processors (i.e., companies that process personal data on behalf of other companies) will be directly responsible (and liable) to comply with a number of obligations under the GDPR, including ensuring technical and organisational protection of personal data. Controllers also need to update their contracts with processors.
- Importantly for Hong Kong companies, the GDPR provides that companies established outside the EU will need to designate a representative in an EU Member State.

Consequences of non-compliance: Compliance with the GDPR is now mandatory and oftentimes crucial for companies' reputations. Hong Kong companies which fail to comply with their legal obligations under the GDPR could be exposed to potential sanctions including fines of up to EUR 20 million or 4% of the company's worldwide turnover (whichever is higher). Data protection authorities can also order companies to give up or modify non-compliant data processing operations, causing costly interruptions to business activities.

In addition, any data subject who has suffered damage as a result of a company's non-compliance may seek compensation from that company, including through class actions. Moreover, awareness has been raised throughout the world as to the importance of the protection of personal data. Therefore, any failure to adequately protect such data by companies would inevitably result in damage to that company's reputation and business.