CLYDE&CO
其禮律師行

The impact of GDPR on businesses in Hong Kong

April 2018

Authors

Joyce Chan
Partner, Hong Kong
T: +852 2287 2752
E: joyce.chan@clydeco.com

Kevin Martin
Partner, Hong Kong
T: +852 2287 2867
E: kevin.martin@clydeco.com

Gillian Morrissey
Senior Associate, Hong Kong
T: +852 2287 2755
E: gillian.morrissey@clydeco.com

Contributors

Dino Wilkinson
Partner, Abu Dhabi
T: +971 2 494 3595
E: dino.wilkinson@clydeco.com

Kellie Blyth
Senior Associate, Dubai
T: +971 4 384 4291
E: kellie.blyth@clydeco.com

Introduction

On 25 May 2018, the EU General Data Protection Regulation (**GDPR**) will replace current data protection laws in every European Union (**EU**) country. The GDPR represents the most significant change to data protection law in Europe in more than two decades.

Why should Hong Kong companies care?

Although the GDPR is European legislation, its reach will not be limited to Europe. This article highlights how international businesses, including those Hong Kong, will be affected by the GDPR. The GDPR will potentially impact companies in Hong Kong – and anywhere else in the world – if they are offering products to individuals within the EU or monitoring the behaviour of EU-based individuals.

It may also impact Hong Kong companies as group policies and many international business partners will mandate compliance with GDPR standards, the latter through contractual terms, and consumer expectations around privacy are higher than ever.

Why is the GDPR important?

The way we generate and handle data has changed beyond recognition in the last 20 years. The GDPR aims to strengthen the control that individuals have over their personal data and to improve transparency about how that data is processed. It also seeks to facilitate business by simplifying rules for companies in the digital market in the EU.

The GDPR will replace the current EU Data Protection Directive 95/46/EC, which every EU country implemented at country level and on which the Hong Kong Personal Data (Privacy) Ordinance (**PDPO**) was largely modelled. It will automatically apply to every EU member state from the effective date. It is expected that the GDPR will be incorporated into the European Economic Area (**EEA**) Agreement and apply in Norway, Liechtenstein and Iceland from 1 June 2018.

> 'The GDPR will potentially impact companies in Hong Kong – and anywhere else in the world – if they are offering products to individuals within the EU or monitoring the behaviour of EU-based individuals.'

The EU recognises the right of an individual to the protection of his/her personal data as a fundamental human right. Accordingly, the provisions of the GDPR place significant weight on ensuring fairness and enabling individuals to maintain control over their personal data. This translates into a high compliance standard for organisations that handle personal data and heavy sanctions for non-compliance. New rules under the GDPR include:

- **Appointment of representatives:** If an organisation based outside Europe is processing personal data in relation to the offering of products to data subjects (i.e. the individuals to whom the personal data relates) in the EU or monitoring the behaviour of EU-based data subjects, that organisation must designate a representative in the EU unless an exemption applies.

- **Tougher sanctions for non-compliance:** Businesses may be subject to fines of up to €20 million (approximately HK$193M) or 4% of annual global turnover, whichever is higher, for certain infringements.

- **Data breach notifications:** A data controller (the organisation that controls the personal data) (**Data Controller**) must notify the relevant supervisory authority (i.e. independent public authority established by a member state) of a personal data security breach within 72 hours of becoming aware of such breach, where feasible, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. It may also be required to inform affected individuals where the incident could cause them serious harm.

- **Accountability and privacy-by-design:** Businesses will be required to demonstrate compliance with the rules and adopt a privacy-by-design approach. This includes carrying out a privacy impact assessment before carrying out any high risk data processing and adopting appropriate measures to address those risks.

- **Data Protection Officers:** Public authorities and private companies whose core activities involve large-scale processing of sensitive data must appoint a Data Protection Officer (**DPO**) to monitor compliance with the rules. Their data processors (the person or organisation which processes personal data on behalf of the Data Controller) may have to do likewise (**Data Processor**).

- **Greater rights for individuals:** Individuals will have enhanced rights in respect of their personal data, such as the right to be forgotten. Businesses must review their procedures to ensure they can comply with these rights.

How will the GDPR impact organisations outside Europe?

The current EU Data Protection Directive primarily affects Data Controllers established in Europe. Many non-EU businesses may not realise that it also has some effect on Data Controllers who are established outside the EU. The use of equipment by non-EU Data Controllers within Europe for the processing of personal data (other than purely for transit purposes) is caught by the current regime.

Given the European view of data protection as a fundamental human right, it is perhaps unsurprising that EU case law sought to expand the reach of the EU Data Protection Directive. The Court of Justice of the European Union found in the case of *Google Spain SL v Agencia Española de Protección de Datos* that the search engine activities carried out by Google US were deemed to be "*inextricably linked*" to the sales generated by Google Spain for the purposes of the Directive.

This principle has been carried into the GDPR along with additional scenarios where non-EU Data Controllers may be deemed caught within the territorial scope of the GDPR. Article 3 of the GDPR sets out the circumstances when the GDPR applies to:

1. Data Controllers or Data Processors which have an EU establishment and personal data is processed in the context of the activities of the establishment. If this requirement is fulfilled the GDPR applies regardless of whether the data processing takes place within the EU or not (Article 3(1)).

2. Non-EU-established Data Controllers or Data Processors are subject to the GDPR where they process personal data of data subjects in the EU in connection with:
   a. the offering of goods or services (regardless of whether payment is required in the EU), or
   b. monitoring the behaviour of data subjects where their behaviour takes place within the EU (Article 3(2)).

3. Non-EU Data Controllers processing data in a location where EU member state law applies by virtue of public international law (Article 3(3)).

Limb 1: Processing in the context of the activities of a European establishment

Article 3(1) of the GDPR makes clear that the processing of personal data in the context of the activities of an establishment in the EU will be caught by the law regardless of whether the processing takes place inside or outside the EU.

Accordingly, this will impact corporate groups that have operations in both Europe and Hong Kong. If personal data that is operationally relevant to the European business is processed in Hong Kong, it could be deemed to be processing in the context of the European establishment. This would be consistent with the principle already established under case law in the *Google Spain* decision.

The recitals to the GDPR state that establishment "*implies the effective and real exercise of activity through stable arrangements*", and that the legal form of such arrangements is not the determining factor. It is not necessary to have a legal entity (such as a branch or a subsidiary) in Europe in order to create an establishment. The appointment of a local agent to act on the non-EU business' behalf will suffice.

Limb 2(a): Offering goods or services to EU-based data subjects

In determining whether a non-EU Data Controller is offering goods or services to data subjects who are in the EU, the key question is whether the Data Controller "*envisages*" offering its products to individuals in the EU. Prior European case law similarly considered whether services were "*directed towards*" the EU.

The fact that a website is merely accessible in the EU is not sufficient to establish an intention to offer goods or services to EU residents. Equally, the use of English in Hong Kong would not create an assumption that the offer is being directed to the EU. However, the use of a European language (more so if not English) together with the ability to pay using the corresponding currency of that European country would be much more likely to create the assumption that the Data Controller "*envisages*" offering the goods or services to data subjects in the EU. Any direct references to EU customers would create a similar assumption.

By way of example, a Hong Kong hotel operator promoting offers to European tourists and taking bookings in euro on its website would likely be deemed to be offering its products to EU data subjects. The GDPR would apply to its processing of personal data (including names, addresses and payment details) of European visitors.

Alternatively, an online retailer in Hong Kong with a website in Chinese and English that only accepts payment in Hong Kong dollars and delivers its products exclusively within Hong Kong is unlikely to be caught by this provision. This would be the case even if the website was accessible by individuals in Europe.

It is irrelevant whether the offering of goods or services is connected to any payment. Free (or ad-supported) services would still be caught by the GDPR if they target individuals within the EU from outside Europe.

Limb 2(b): Monitoring the behaviour of EU-based data subjects

This limb captures the processing of personal data of EU-based individuals relating to the monitoring of their behaviour, where such behaviour occurs in the EU. This includes tracking behaviour on the internet to profile individual usage, particularly where such monitoring is undertaken to make decisions about the individual or for analysing or predicting the individual's preferences, behaviours or attitudes.

A wide range of automated analytical techniques may therefore be caught within the ambit of "*monitoring*" for these purposes, including the use of cookies, logging IP addresses or obtaining location data via a mobile app. Retailers in Hong Kong– such as airlines, hotels and others in the hospitality industry – should be particularly aware that the use of such online marketing or monitoring practices may create an additional burden if they are being used to profile European individuals.

Appointment of a representative

Any organisation outside the EU caught by Article 3 of the GDPR must appoint a representative in the EU for the purposes of the GDPR, subject to certain exemptions (see below). Such representative should act on behalf of the non-EU entity and may be addressed by any European supervisory authority. The representative won't shield the Data Controller from any legal action but the recitals to the GDPR state that the representative "*should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*" and may be addressed instead of the Data Controller or Data Processor.

The representative must be located in one of the European countries of the individuals who are offered products or subject to behavioural monitoring.

A non-EU Data Controller or Data Processor will be exempt from appointing a representative if it:

1. fulfils a cumulative three-part test, that the data processing:
    a. activities are occasional;
    b. does not include the large-scale processing of categories of data (including personal data revealing race, ethnic origin, political opinions or beliefs, health records, genetic or biometric data, or criminal records); and
    c. is unlikely to result in a risk to the rights and freedoms of individuals; or
2. is a public authority or body.

The meanings of "*occasional*" and "*large scale*" will be critical to the implementation of the GDPR by non-EU businesses going forward.

Contractual terms and self-regulation

The impact of supply chain pressure should not be underestimated as a driver for GDPR adoption. Many international business partners will be mandating GDPR compliance throughout their supply chain.

EU contracting parties that are subject to the GDPR will have to impose equivalent obligations on their Data Processors by way of contract to avoid their own compliance issues.

Customer expectation and the common practice of multinationals to adopt the highest compliance standards are also expected to create a level of self-regulation outside Europe. The cross-border nature of the internet and widespread adoption of cloud computing make it difficult to confine data processing to specific geographic borders. We expect companies to adopt a risk-based approach to compliance that will be influenced by the potentially heavy fines for breaches of the GDPR.

Next steps for Hong Kong organisations

All organisations in Hong Kong with any connection to Europe – whether through customers, affiliates or business partners – should as a matter of urgency be considering the potential impact of the GDPR given it fast-approaching implementation date and potentially significant penalties. A number of companies have already started this process. In many cases, the GDPR compliance steps will supplement existing measures that many corporates in the region adopt as a matter of good practice or to comply with local regimes, such as the PDPO.

Key differences between the PDPO and the GDPR

The Office of Privacy Commissioner for Personal Data, Hong Kong (**PCPD**) has identified key differences between the PDPO and the GDPR.[1] The impact of the GDPR on organisations in Hong Kong will depend on the gaps between the PDPO and the GDPR. Key differences between the two legislations include:

- **Extra-territorial application of the GDPR:** The GDPR applies to Data Processors or Data Controllers established outside the EU, whereas the PDPO applies to data users processing or using data in or from Hong Kong.
- **Mandatory breach notification:** Under the GDPR Data Controllers are required to notify the supervisory authority unless exempted and to notify affected data subjects if the breach is likely to result in a high risk to their rights and freedoms, whereas breach notification under the PDPO is given on a voluntary basis. Under the GDPR Data Processors are required to notify Data Controllers without undue delay.
- **Sensitive personal data:** The GDPR allows the processing of sensitive personal data only under specific circumstances, whereas the PDPO does not distinguish between sensitive and non-sensitive personal data.
- **Additional obligations on Data Processors:** Pursuant to the GDPR, Data Processors have additional obligations including maintenance of processing records, ensuring processing security, and designating a DPO. Under the PDPO, there is no direct regulation of Data Processors. Data users must ensure Data Processors comply with security and data retention requirements.
- **Sanctions:** Under the GDPR the maximum administrative penalty is a fine up to the greater of €20 million or 4% of the total worldwide annual turnover. Breach of the Hong Kong PDPO data protection principles does not constitute a criminal offence directly but contravention of an enforcement notice constitutes an offence resulting in a maximum fine of HK$50,000 and imprisonment for 2 years. Breach of certain substantive provisions of the PDPO is a criminal offence and penalties range approximately from a fine of HK$10,000 to HK$1,000,000 and 5 years' imprisonment.

The PCPD is encouraging organisations in Hong Kong to adopt and maintain a comprehensive Privacy Management Programme (**PMP**) from the coming into effect of the GDPR. The PMP is a strategic framework used to assist in building a privacy infrastructure including the designation of a DPO, setting up a reporting mechanism for breach notification and developing risk assessment tools, and an effective review and monitoring process, as outlined in the PCPD's 2014 Best Practice Guide.

Compliance with the GDPR: Summary of key practical steps

1. Inform your organisation's senior management of the GDPR and how it might impact the business.
2. Examine and assess the impact of the GDPR, and determine which business activities must comply with the GDPR.
3. If determined that activities of your organisation will be caught by the GDPR (directly through the application of the GDPR or indirectly due to the requirements of group policy or your contract counterparties), prepare a compliance plan and programme to identify and address gaps in policies, processes and procedures.

1 The Office of Privacy Commissioner for Personal Data, Hong Kong (26 October 2017); Observations on the GDPR 2018 from Hong Kong's Perspective (https://www.pcpd.org.hk/english/news_events/whatison/files/20171026_Symposium.pdf)

4. Conduct a data mapping exercise of how you collect personal data, the purposes for which it is processed, how it was obtained and who it is shared with; record and manage the legal bases on which it was collected; and consider whether existing consents need to be refreshed to ensure compliance with the GDPR.

5. Implement training programmes regarding the GDPR's practical impact to your businesses.

6. Update your policies on internal and external cross-border transfers of personal data to ensure compliance with the GDPR.

7. Prepare a mechanism to handle data access requests within the GDPR timeframe (one month, compared with 40 days under the PDPO) and reform your organisation's procedures regarding how personal data will be provided electronically or deleted.

8. If within scope of the GDPR, appoint a GDPR EEA representative.

9. If required by the GDPR, designate a DPO to monitor compliance with the GDPR.

10. Conduct privacy risk assessments where there are high risks to the rights of individuals and identify and minimise these.

11. If necessary, renegotiate third party contracts to provide sufficient supervision over the processing of personal data under the GDPR.

For those organisations where data protection compliance has not previously been a consideration, some of the steps necessary for compliance with the GDPR will seem onerous. Those companies that take immediate action should be better placed to mitigate the risks under European law.

Click here for the infographic.