Wider Reach of the General Data Protection Regulation – What Hong Kong Businesses Should Know

December 2017

Introduction

The EU General Data Protection Regulation (**GDPR**) will take effect on 25 May 2018. It marks a significant expansion of the territorial scope of the EU data protection regime, bringing a larger number of overseas businesses within its reach.

The GDPR considers not only the location of the data processing (as in the current EU Data Protection Directive (the **Directive**)), but also the location of the individual whose data is being processed. See the section on "Extraterritorial scope" in the next column for further details.

Hong Kong businesses, even those with no physical presence in the EU, should therefore assess whether they fall within the wider reach of the GDPR.

If a Hong Kong business falls within the GDPR, action will likely be required to be taken in order to comply with the regulation. The GDPR, while retaining many of the principles and rules established by the current Directive, introduces a wide range of reforms to the European data protection regime and is generally more onerous than the existing EU and Hong Kong regimes.

This briefing provides a high-level overview of the key aspects of the GDPR.

Extraterritorial scope

When determining whether activities fall within its scope, the GDPR considers not only the location of the processing, but also the location of the individual whose data is being processed. The GDPR applies to companies established outside of the EU which process personal data in relation to:

- the offering of goods or services to individuals in the EU (regardless of whether payment is taken); or
- the monitoring of the behaviour of individuals within the EU.

Examples of the wider application of the GDPR

Scenario	GDPR applies
HK company without any EU subsidiaries offering free social media services via a website hosted in the US to individuals in the EU	✓
HK hotel booking business using cookies to track past customers' (including EU-based customers) browsing in order to target specific hotel adverts to them	✓
HK flower delivery company allowing individuals in the EU to make orders for fulfilment only in HK. The price for the flower delivery services is denominated in an EU currency	✓
HK retailer with a website for orders/deliveries. The website is accessible to individuals in the EU in English. The currency is the HK dollar and the address fields only allow HK addresses	x

Offering goods or services

An overseas company will be considered to offer goods or services to EU individuals where it is the company's intention and it is apparent that an offer to an EU-based data subject was 'envisaged'. The availability of a company's website to EU individuals is not sufficient to establish an intention to offer. However, if the website is in an EU language which is not that of the company's jurisdiction, is offering goods or services in an EU currency or explicitly targeting EU citizens, this could provide proof of intent and bring the company within the scope of the GDPR.

Monitoring Behaviour

The GDPR makes clear that where individuals are 'tracked on the internet', this will constitute monitoring and bring a company or relevant entity within the scope of the GDPR. All websites that use cookies and mobile applications that track usage will be caught to the extent that the information they collect, in aggregate, renders an individual identifiable.

The use of cookies

An overseas company that carries out cookie profiling (i.e. by using persistent, as opposed to session only, cookies to track a user's overall online activity across websites) will most likely be processing personal data to monitor behaviour. The use of cookies that do not collect personal data or that do not track or profile a user (such as session only cookies that regulate website functionality) is unlikely to be caught by the GDPR.

IP addresses

Individuals can also be tracked or monitored through the sharing of IP addresses. Many website owners keep logs of the dynamic IP addresses that have visited their website. Such IP addresses may amount to personal data, especially where the user's internet access provider has data that, in combination with the IP address, can identify the user.

Representatives

The GDPR requires overseas companies falling within its scope (and whose processing is not occasional) to designate a representative based in an EU Member State. The designated representative will act as the point of contact for the relevant data protection authorities. The designation of a representative is 'without prejudice' to the liability of the data controller, but the degree of responsibility ascribed to representatives varies across the Member States. For example, in Greece, representatives are subject to sanctions alongside the data controller; whilst in the UK, it is largely an administrative role.

The GDPR clarifies that a nominated representative is only required in the Member State of the 'main establishment' of a company. The 'main establishment' of a company will be its place of 'central administration', unless decisions regarding the purpose and means of processing are taken elsewhere.

Overseas businesses with no clear EU establishment, or with a number of establishments in the EU taking decisions regarding processing, are likely to encounter practical difficulties in complying with this requirement to designate a single 'main establishment'.

What obligations does the data controller have?

If your company makes the decisions about why and how the personal data is collected, used or otherwise processed, such as with employee or customer data, it will be a 'data controller' under the GDPR (equivalent to the concept of a 'data user' under Hong Kong's Personal Data (Privacy) Ordinance (**PDPO**)). Legally, it is the 'data controller' who is responsible for ensuring that

personal data is processed in accordance with the GDPR.

If your business falls within the scope of the GDPR, you will be required to be able to demonstrate compliance with the data protection principles under the GDPR. The GDPR retains the fundamental principles applicable under the current Directive, but the requirement to not only comply with the principles, but also to demonstrate compliance, is new and is referred to as the 'accountability principle'.

What obligations does the data processor have?

The GDPR imposes new obligations directly on 'data processors' (i.e. organisations that process personal data on behalf of data controllers), albeit less extensive than those obligations imposed on data controllers. This a departure from the existing EU and Hong Kong regimes.

The GDPR imposes direct obligations on data processors in areas such as security, record keeping and international transfers, resulting in direct enforcement measures if they do not comply. In practice, the GDPR's requirements may not be entirely new if you are a processor as many of the obligations under the GDPR are currently already contractually imposed on processors by the relevant data controller in many data processing agreements.

What other key reforms are being made?

Data protection impact assessment

A data protection impact assessment (**DPIA**) is a tool to help organisations identify and minimise privacy risks when planning new (and revising existing) projects, policies and systems. It is essentially a risk assessment for your proposed use of personal data. Under the GDPR, conducting a DPIA will become a legal requirement, not just best practice (as it is in Hong Kong), in circumstances where you are processing personal data in a way that can be considered as 'high risk' to individuals' rights and freedoms.

Lawful basis for processing

There must be a lawful basis for processing personal data. The lawful bases under the GDPR are similar to those under the existing EU regime - such as where the individual consents to the processing or where the processing is necessary for your or a third party's legitimate interests. Many businesses may not have considered their lawful bases for processing data, as this concept does not generally have practical implications under the existing EU or Hong Kong regimes. This will change under the GDPR.

Consent

The concept of consent under the GDPR is now stricter, and involves more onerous requirements in relation to both the content of the consent and the way in which it should be obtained. For example:

- Consent must be freely given, specific, informed and unambiguous. In certain circumstances, consent must, in addition, be explicit. This explicit consent is required in more circumstances under the GDPR than under the Directive and the PDPO, and is the required standard of consent to process special categories of data. The requirement for consent to be 'freely given' is likely to affect consent obtained by standard data protection clauses in, for example, employment contracts.

- Multiple items should not be bundled together with one consent covering all of them. Instead, the individual should have the ability to choose to consent to some but not all of the processing.

- Where consent is given as part of a written declaration which also concerns other matters, the request for consent should be 'clearly distinguishable' from the other matters and be presented in an 'intelligible

and easily accessible form'. It is important, therefore, to ensure that an individual's consent to processing is not buried in standard T&Cs but instead is set out separately from other provisions.

- Individuals must be able to withdraw consent to processing at any time. They should be made aware of this right before giving consent. You should ensure that it is 'as easy to withdraw as to give consent'.

- Clear records should be kept of who has consented to what. Personal data should be processed in line with such consents.

It is unlikely that the consents your company has obtained (even if compliant with the Directive) will meet all the requirements of the GDPR. Whether you are required to 'refresh' an existing consent will depend on whether you are relying on the individual's consent as the lawful basis for processing their data. If the existing consent does not meet the GDPR standard, you should either see if you are able to rely on an alternative lawful basis for processing data (such as 'legitimate interest') or seek a fresh GDPR-compliant consent.

Relying on the legitimate interest ground will involve assessing (on a case-by-case basis) whether the processing of personal data is necessary for the purposes of your company's legitimate interests or those of a third party to whom the data is to be disclosed. However, this must be balanced against any prejudice to the rights and freedoms, or to any interests, of the affected individual.

Profiling

Profiling covers a wide range of activities. Examples are: (i) online retailers using information on the shopping habits of their customers to suggest items that customers may be interested in purchasing; and (ii) automated decision-making, such as insurers tracking customer behaviour to predict the risks of claims when setting premiums.

The GDPR places significant restrictions on profiling where this has 'legal effects' for individuals or 'similarly significantly' affects them. The restrictions would cover, for example, automatically refusing an online credit application or e-recruiting practices without any human intervention. In circumstances where profiling does have legal or similarly significant effects, additional requirements (including the provision of specified information to customers) must be satisfied.

Transferring personal data

Transfer to a data processor

If your company engages the services of a third party to help process data on its behalf, the third party is likely to be a 'data processor'. The GDPR imposes certain requirements (such as data processing agreement content requirements) on the engagement of data processors. Your company will still retain ultimate responsibility for the data. Existing data processor agreements will likely need to be amended to be GDPR compliant.

Transfer to another data controller

In some circumstances, the third party assisting you in processing personal data may be deemed to be a data controller rather than a data processor. This depends on, among other things, whether the third party can make its own decisions about how to use the data and to what extent the third party must seek your consent or instructions. It may also be the case that you pass personal data to a third party for their own purposes. In these cases, both your company and the third party would be a data controller with legal responsibility for compliance with the GDPR.

Where the two data controllers have entered into clear and reasonable arrangements setting out their roles and responsibilities, enforcement action is likely to be brought only against the data

controller who acted in breach of those arrangements.

When negotiating contracts with third parties, do not agree to disclose information to them unless you are confident that the GDPR would permit this, for example because your company has relevant consent. If information is requested by a third party that is not covered by a contract you have with them, then, unless you are confident that the disclosure is permitted by the GDPR, you should normally reject such requests.

If you pass information to a third party, you should ensure that, wherever possible, the information is anonymous (since this takes the data outside the GDPR restrictions), or otherwise that sufficient controls and confidentiality provisions are placed around the data.

Transfer of personal data outside the EEA

Personal data may be transferred freely between the EU and EEA Member States. If your company intends to transfer personal data to Hong Kong or anywhere outside of the EU or EEA Member States, one of a number of conditions must be satisfied in order to ensure the data receives an adequate level of protection. These conditions include (but are not limited to): (i) the European Commission having determined the destination jurisdiction as offering a level of protection for personal data 'essentially equivalent' to EU law (currently, this does not include Hong Kong or China); (ii) binding corporate rules (made between organisations within a corporate group) are put in place; (iii) model contractual clauses (in the form approved by the European Commission) are signed; or (iv) the individuals concerned have given their informed consent to the transfer.

The rights of individuals

The GDPR retains and modifies certain existing rights under the Directive, including: (i) rights of access to personal data; (ii) rights to object to or prevent certain processing; and (iii) a right to claim compensation for damages caused by a breach of data protection law. There are also new rights, including: (i) the right to be 'forgotten'; (ii) the right to restrict processing; and (iii) the right to data portability, which may apply in certain circumstances.

Data protection officers

In certain circumstances, your company may be required to appoint a data protection officer (**DPO**), whose primary duty will be to ensure compliance with the GDPR. The DPO must: (i) be given adequate resources in order to enable the DPO to carry out its tasks effectively; (ii) carry out its role in a completely independent manner; and (iii) not be dismissed or penalised for performing the DPO duties.

You will need to appoint a DPO if:

- your core activities require regular and systematic monitoring of individuals on a large scale; or
- your core activities include large scale processing of special categories of data or personal data relating to criminal convictions and offences.

Notification

Under the GDPR it will no longer be necessary to make an annual notification of data processing activities. However, you must notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of a data breach. There is no notification requirement if the breach is unlikely to result in a risk to individuals whose personal data was affected. If the breach is likely to pose a 'high risk' to an individual's rights and freedoms, then the relevant individuals must also be notified.

Records should be kept of all breaches including those where there was no obligation to notify.

Enforcement

One-stop shop

The 'one-stop-shop' mechanism means that companies carrying out cross-border processing will only be required to liaise with their lead regulatory authority. However, only data controllers established within the EEA will benefit from the one-stop-shop principle. In practice this means that if, for instance, a non-EEA based company suffers a data breach which necessitates a notification, it may be required to notify more than one authority. It will also be open to regulatory action from all those authorities concerned.

Fines

One of the more significant changes brought in by the GDPR is a significant increase in the level of fines for non-compliance. The GDPR provides for fines of up to the higher of 4% of annual worldwide group turnover or €20 million (equivalent to approximately HK$180 million).

Next steps

The wider reach of the GDPR will lead to more Hong Kong businesses falling within the EU data protection regime. Businesses which were not previously caught by the EU regime, as well as those which already fall within its scope, should review their data protection policies, processes and documentation and take steps to become GDPR compliant by 25 May 2018.

Please feel free to get in touch with your usual Slaughter and May contact if you require any assistance.

Hong Kong Team

Peter Lake
T +852 2901 7235
E peter.lake@slaughterandmay.com

Mark Hughes
T +852 2901 7204
E mark.hughes@slaughterandmay.com

Kevin Warburton
T +852 2901 7331
E kevin.warburton@slaughterandmay.com

London Team

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com