Making Provisions For GDPR

Source: The Bulletin (Issue Jul 2018)

Nick Chan, Partner, Squire Patton Boggs

Hong Kong companies with customers in Europe cannot ignore new E.U. legislation

"We have recently updated our Privacy Policy in compliance with the General Data Protection Regulation (GDPR). Please click here to confirm your acceptance of our updated Privacy Policy."

Has your inbox recently been flooded with emails like the one above? Have you noticed a surge in the number of privacy notifications that pop up when you visit websites?

In Hong Kong, many of us can simply click on "accept" without considering why these notifications have suddenly arisen. However, the driving force behind them is a lengthy new law called the General Data Protection Regulation (GDPR), and it is not something that can simply be ignored by Hong Kong businesses.

Failure to comply with the GDPR could result in a maximum penalty of 20 million euros (HK$180 million), or 4% of the global annual turnover of the offender's business (whichever is greater).

The GDPR is a regulation under European Union law on data protection and privacy, which took effect on 25 May.

Perhaps understandably, many Hong Kong businesses may have the following thoughts:

- Our company is not located in the E.U. The GDPR has nothing to do with us.
- No worries. We will just let our offices in the E.U. handle the GDPR.
- None of our contracts are governed by laws of E.U. member states, so the GDPR won't apply to us.

The truth of the matter is, the GDPR can still apply to Hong Kong companies operating out of Hong Kong.

GDPR's global reach

Unlike many other legislations and regulations, the GDPR has extra-territorial effect and impacts the entire world.

For example, the GDPR applies to the processing of personal data of natural persons who are in the E.U., even if the person or company processing the data is not located in the E.U., where the processing is related to the offering of goods and services or the monitoring of the natural persons' behavior.

Some Examples

A Hong Kong company selling goods online: A nonE.U. incorporated company that sells goods through its official website could be subject to the GDPR if it sells to, for example, a German national in Germany, or if the website monitors the German national's behavior.

A Hong Kong company operating a cloud service storage system: For example, personal data of customers, some from the E.U., are provided to a cloud service storage system which the Hong Kong company operates. As the cloud can be accessed in the E.U. and the personal data of those persons in the E.U. are being transferred to Hong Kong for storage and transferred to a third party for further processing, the Hong Kong company's handling of the personal data of those E.U. persons, and their relevant terms and conditions in the contracts with those customers and any third party processors, must be GDPR complaint.

Who is covered by the legislation?

Another question that Hong Kong companies must consider is: Does GDPR apply to all persons located in the E.U.?

It is a controversial issue as to whether the GDPR only applies to citizens of the E.U., or whether it applies to all persons who are located in the E.U. at the time when the personal data is collected. The wording of the GDPR text states that it will apply to not only E.U. companies that process personal data, but also to non-E.U. companies. It does not appear to restrict data subjects to those that are E.U. citizens or residents.

There are conflicting interpretations over this point. For prudence's sake, we suggest that businesses should take a cautious approach and assume that it applies to all persons located in the E.U. at the time when the personal data is collected, especially if the companies have global reach, and transfer data between various group companies.

Some businesses may say that they do not intend to offer any services to persons who are in the E.U. In this regard, the matter will be looked at on a case-by-case basis, taking into account factors such as the language involved (e.g. whether the online store offers any E.U. languages), currency (e.g. whether the price is shown in euros) and whether there is any mention of customers who are located in the E.U.

Additional protection of data subjects

The GDPR grants a number of additional rights to data subjects, including but not limited to right to object, special rights afforded to sensitive data, right to be forgotten, breach notification, and the need to include a fairly detailed listing of the types of personal data that are collected and processed. Detailed elaboration of these rights are beyond the scope of this article; suffice to say that they are highly technical in nature.

GDPR in action

On the day that GDPR commenced, WhatsApp, Facebook, Google and Instagram were hit with lawsuits under the new legislation. In the case of Facebook, the fine demanded is US$43 billion. Complaints have also been filed against corporations such as Apple, Amazon and LinkedIn, and more are expected to come.

In light of the significant potential exposure under the GDPR, we note that a number of non-E.U. businesses, such as the Los Angeles Times and USA Today, have decided to block visitors from the E.U.

Other actions taken include seeking declarations from customers that they are not in the E.U., and providing plain text versions of website without cookies to avoid collecting personal data inadvertently.

But as a Chinese saying goes, this is like "chopping off your toes to avoid the sand worms." In fact, it is questionable as to whether blocking all E.U. IPs will completely avoid any liability under the GDPR. To avoid the E.U., one of the world's biggest economies, may also not make much business sense.

What can Hong Kong businesses do?

What measures can Hong Kong companies take to ensure that they are GDPR compliant?

This is not as simple as adding a few references to the GDPR in the data policy. (Even without the GDPR, we would strongly recommend companies to adopt a data privacy policy under Hong Kong's Personal Data (Privacy) Ordinance.)

If the company has any activity or dealing with persons in the E.U., it should review its activity to establish if it would be subject to the GDPR. If so, it should undertake all necessary measures to confirm that these activities are GDPR compliant.

The actions that Hong Kong businesses can take include:

1. Updating their data privacy policy;
2. Ensuring that there are appropriate contract terms with subsidiaries (e.g. for the transfer of employee data held by E.U. subsidiaries to headquarters in Hong Kong, or a service provider handling personal data of data subjects in the E.U.);
3. Amending existing agreements to include new contractual provisions mandated by the GDPR, e.g. audit rights, appointment of sub-processors, security measures etc;
4. Carrying out due diligence into processors' security measures and GDPR compliance; and
5. Upgrading the website to be GDPR-compliant. In drafting, special care should be taken to consider whether the same notice should apply to non-E.U. customers. If the company can detect and separate out processing of E.U. traffic, it could use a separate E.U. notice.

Since the GDPR has already come into effect, if your business has not yet conducted any assessment of its exposure under the GDPR, it should do so immediately and carry out appropriate privacy impact assessment urgently.