Privacy Law in Hong Kong – No Hiding from Reform

March 2019

Background

Much fanfare heralded the GDPR's introduction. We have written about the effect of the GDPR and its enforcement outside the EU in previous Briefings, the latest of which can be accessed here. In this Briefing, we review how the GDPR has been enforced since it took effect, including how its reach has been felt outside the EU. We also explain why the GDPR is not the end of privacy law reform, but only the beginning, influencing regimes as far away as in APAC. As a result, privacy issues are now on the radar of senior management in organisations and appear to be here to stay.

The European Union's (EU) General Data Protection Regulation (GDPR) took effect on 25 May 2018 and represents the most significant reform of global privacy law in over 20 years. Its effect has been felt outside the EU and it appears to be the springboard for wider-ranging reform, including in China and the wider Asia-Pacific region (APAC)

Enforcing the GDPR

Our recent Briefing explained how the UK privacy regulator had, in July 2018 and October 2018, issued the first enforcement notices under the GDPR against a Canadian company located outside the EU, AggregateIQ Services Ltd (**AggregateIQ**). Pursuant to those notices, the UK regulator exercised the powers available to it to require AggregateIQ to carry out certain remedial measures, where failure to do so might result in a fine of up to EUR20 million (approximately HK$180 million) or 4% of worldwide turnover, whichever is higher.

Other EU regulators have also been prepared to impose large fines (at the higher scale) on non-EU companies (albeit ones with establishments in the EU). In January 2019, the French privacy regulator fined Google LLC (a US company) EUR50 million (approximately HK$450 million). The record fine followed Google's alleged breaches of the GDPR, in particular: (i) a lack of transparency and inadequate information provided to data subjects; and (ii) a failure to obtain valid consent from those data subjects in respect of personalised advertising. Google has said that it will appeal.

As such, it is important for organisations in APAC which might have exposure to the GDPR to bear in mind the steps to compliance referred to in our earlier Briefing. That is not just because of the GDPR, but also because of possible reform in Hong Kong, China and the wider APAC region.

Time for reform in Hong Kong?

On 21 February 2019, Hong Kong's Privacy Commissioner for Personal Data (**Privacy Commissioner**) served the first public enforcement notice on a party, in this case a telecommunications company, since 2017. The enforcement notice was in the context of an alleged data breach. The Privacy Commissioner found that the company had failed to take all practicable steps to ensure that personal data held in one of its databases was protected against unauthorised access, contrary to the Data Protection Principle 4 (Data Security) of Schedule

1 to Hong Kong's data privacy law, the Personal Data (Privacy) Ordinance (Cap 486) (**PDPO**).

What is of particular interest was the Privacy Commissioner's comments in relation to his office's current powers under the PDPO. The Privacy Commissioner noted that, at present, his office is not empowered to impose administrative fines, but only to issue an enforcement notice requesting data users to take measures to rectify their contraventions of the PDPO (and then only after a data user fails to comply with an enforcement notice does it commit an offence, punishable by a fine up to HK$50,000 and imprisonment for up to 2 years). The Privacy Commissioner referred to other statutory authorities which did have power to impose administrative fines, as well as the powers given to EU authorities under the GDPR. He stated that it is "*necessary to work with the government authorities to review the current legal framework…with a view to enhancing the deterrent effect of sanctions as appropriate and in line with other regulatory authorities, local and overseas alike*".[1]

The Privacy Commissioner emphasised that organisations should go beyond what is the minimum level required by law and should be "*held to a higher ethical standard that meets the stakeholders' expectations by doing what they should do…[O]rganisations should adopt an accountability approach in handling personal data by incorporating data governance, stewardship and ethics, namely being respectful, beneficial and fair, as part of corporate governance, and apply them as a business imperative throughout the organisation, starting from the boardroom*".[2]

Irrespective of: (i) the powers available to his office; and (ii) what reform might actually take place in Hong Kong (and when), the Privacy Commissioner has emphasised the ethics of how organisations in Hong Kong should approach data privacy.

In a recent article,[3] the Privacy Commissioner stated that "*the GDPR and the development of [the] global privacy landscape, together with recent data breach incidents, present a timely opportunity to review the law and propose updates as appropriate*". In the same article, he said that "*regulators should foster a culture of genuine respect for personal data to ensure that is protection its realistically effective and sustainable*" and that *"[o]rganisations should therefore think and act outside of the box of compliance simpliciter, and embrace data ethics as part of corporate governance for gaining stakeholders' trust*".

In an interview at the 2018 International Conference of Data Protection & Privacy Commissioners in Brussels,[4] the Privacy Commissioner noted that Hong Kong has "*one of the oldest pieces of legislation in terms of a single comprehensive data protection law in Asia*" and that adoption of some of the standards enshrined in the GDPR is "*inevitable if [Hong Kong is] going to maintain [its] role and status as: (i) a human rights-compliant jurisdiction; and (ii) an international centre in relation to data*". Further, in respect of enhanced powers for his office, the Privacy Commissioner stated "*that will remain as one of the requests we will continue to make. Every enforcement agency would like to have more power, but that cannot be done overnight. We have to revise or change the laws. In Hong Kong, that will take some time. So for*

[1] Investigation Report R19-579 by the Privacy Commissioner (21 February 2019), paragraph 58.

[2] Ibid, paragraph 57.

[3] Hong Kong Lawyer, February 2019, pages 30 – 31.

[4] https://globaldatareview.com/article/1178377/interview-stephen-wong.

now we continue to educate, publicise, get all stakeholders, individuals and organisations alike to be fully prepared for sanctions".

As to what any reform might look like, leading areas could include mandatory breach notifications (currently the scheme is voluntary) and transfers of data outside Hong Kong (section 33 of the PDPO is not yet in force).

What about reform in APAC generally?

Hong Kong is not alone in exploring reform of its privacy law in light of the GDPR. Indeed, other jurisdictions in APAC have already introduced, or are in the process of introducing, their own reforms:

- **India** passed a new data protection bill in July 2018, which is based on GDPR-type principles. In October 2018, the **Malaysian** government said it would revise its data privacy regime in 2019, possibly modelling it on the GDPR. In February 2019, **Thailand's** new data privacy legislation was passed. It has drawn on concepts in the GDPR, as well as drawing from other regimes, such as that in effect in Singapore;

- in February 2019 **Australia's** new Notifiable Data Breaches (**NBD**) scheme came into force. The NBD scheme applies to all agencies and organisations with existing personal information security obligations under the Australian regime. It includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm, including making recommendations to affected individuals regarding steps they should take in response to the breach; and

- in February 2019 the **Singapore** government and privacy regulator introduced proposals for the introduction of a data portability requirement, as part of a wider review of the Singapore regime. This is following similar developments on data portability in other APAC jurisdictions such as **Australia**, **New Zealand**, **India**, **Japan** and the **Philippines**.

In addition, in January 2019 the **Chinese** government published proposed amendments to its data protection standards. The proposed amendments are to China's Personal Information Security Specification, a non-binding standard. The reforms aim to enforce a higher standard for data collection, by imposing stricter requirements regarding consent and identification of processing grounds. While such reforms will not overrule China's new Cybersecurity Law (which itself introduced requirements regarding 'sensitive' personal data and mandatory consent), they will likely impact affected Chinese organisations.

What next?

Privacy reform is here to stay: the GDPR is a development milestone, not an outlier or an end in itself. In his annual report published on 26 February 2019,[5] the EU's independent data protection authority (the European Data Protection Supervisor) said that while organisations to date had "*rather than adapting their way of working to better protect the interests of those who use their services, [they seemed] to be treating the GDPR more as a legal puzzle, in order to preserve their own way of doing things" but "[w]e should expect this to change over the coming year, however*". Of

[5] https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2018-annual-report-new-era-data-protection_en.

particular relevance to organisations outside the EU will be the finalisation of the European Data Protection Board's draft guidelines on the territorial scope of the GDPR, which were published on 23 November 2018 and the public consultation in respect of which closed on 18 January 2019.[6]

As such, both the GDPR and wider privacy reform will continue to affect organisations throughout the world, including in Hong Kong. Moreover, organisations in Hong Kong will need to keep a close eye on developments closer to home, including taking the opportunity now to get their house in order. In particular, organisations should analyse the data they collect, what they use it for and why, how they keep it and how they respond to incidents regarding it. Doing so will enable organisations to not only understand their own business operations better, but foster a relationship of trust with their stakeholders, particularly their customers and regulators.

Throughout 2019, Slaughter and May will be working to help clients with their privacy compliance projects, through initiatives such as:

- a client seminar on Wednesday 15 May 2019 discussing the first 12 months of the GDPR, in particular how it has impacted (and will continue to impact) organisations in Hong Kong;
- a practical client workshop discussing how to plan for and react to a data breach; and
- various client publications, including handy overviews of general data privacy considerations in both: (i) mergers and acquisitions transactions; and (ii) regulatory investigations.

Details of those seminars and publications will be circulated to those on our Hong Kong office's email distribution list in due course. However, if you would like to ensure that you receive such information then please do not hesitate to contact Kevin Warburton by emailing kevin.warburton@slaughterandmay.com.

[6] https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en.

If you would like to discuss any of the contents of this Briefing, then please do not hesitate to contact those listed below.

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

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

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

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

Jason Cheng
Associate
T +852 2901 7211
E jason.cheng@slaughterandmay.com

March 2019