Client Alert | Intellectual Property / Technology

Singapore and Hong Kong agree to strengthen data protection cooperation

June 2019

Authors: Tim Hickman, Melody Chan, Jon Bowden, Berny Chong

On 31 May 2019, the Data Protection Authorities of Singapore and Hong Kong signed a Memorandum of Understanding ("**MoU**") intended to strengthen cooperation in data protection in the two jurisdictions.

Under the MoU, Singapore's Personal Data Protection Commission ("**PDPC**") and Hong Kong's Privacy Commissioner for Personal Data ("**PCPD**") have agreed to exchange best practices, carry out joint research projects, and cross-share experiences and information on potential and ongoing breaches. The commissioners explained that the MoU was a reflection of the joint efforts of Hong Kong and Singapore to strengthen cooperation between them and provide a reliable framework for promoting data sharing against the background of an evolving digital economy.

The MoU arrives at a time when privacy and data protection issues are increasingly in the public consciousness. Since the introduction of Singapore's Personal Data Protection Act in 2012, data protection has developed significantly as an area of law in Singapore. The PDPC continues to issue guidance on different aspects of data protection and enforcement action has been stepped up in the past few years (with close to 30 enforcement cases decided in 2018).

In the last 18 months, companies based in Singapore and Hong Kong have suffered significant data breaches. In early 2018, a Singaporean health conglomerate was fined following a data breach that impacted 1.5 million individuals, and only a few months later a Hong Kong-based airline disclosed a breach affecting the data of 9.4 million users. As both Singapore and Hong Kong are members of international data privacy organisations such as the Asia Pacific Privacy Authorities ("**APPA**") and the Global Privacy Enforcement Network ("**GPEN"**), the PDPC and PCPD have a working history of collaboration in global personal data. The MoU provides a mechanism to facilitate further cooperation in addressing data protection issues across the two jurisdictions.

New guide on Data Protection by Design

As part of their efforts to step up cooperation, the PDPC and PCPD have released a jointly developed Guide to Data Protection by Design for ICT Systems (the "**Guide**"). The Guide offers practical tips to organisations developing information and communications technology ("**ICT**") systems, encouraging them to incorporate data protection principles into software development from the onset.

The approach promoted by the Guide is termed Data Protection by Design ("**DPbD**") and is predicated on the following seven principles:

- **Proactive and preventive:** assessing, identifying, managing and preventing data protection risk through good design and data management practices.
- **Data protection as the default:** integrating data protection measures as default settings in processes and features of ICT systems.

- **End-to-end security:** implementing good security features and practices in each phase of software development.
- **Data minimisation:** only collecting data relevant and necessary to the intended purpose for which the data is processed.
- **User-centric:** developing user-centric ICT systems which help individuals to understand how their personal data is processed (by including informative notices) and offer them more control over their personal data (for example, through customisable settings).
- **Transparency:** taking an active role in informing individuals on what personal data is collected and how it is being used.
- **Risk minimisation:** systematically identifying and mitigating data protection risks by implementing adequate processes and security measures.

The Guide offers businesses useful practical guidance on how to implement these principles in each phase of software development and deployment as well as general advice on good data protection practices for ICT systems.

Impact on businesses

Global businesses operating in Singapore and Hong Kong need to take into account the impact of enhanced cross-border cooperation heralded by the MoU. To avoid falling foul of data protection laws, businesses should ensure that compliance measures are implemented to a high standard in both jurisdictions. As flows of information become increasingly globalized, regional cooperation between data protection authorities is likely to grow. The coming into force of the General Data Protection Regulation ("**GDPR**") has crystallized this trend in the European Union, and the Singapore-Hong Kong MoU may signal the spread of multilateral cooperation efforts in data protection across other regions.

Paula Melendez, a Trainee Solicitor at White & Case, assisted in the development of this publication.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000