The British
Chamber of Commerce
in Hong Kong
香港英商會

Ms Ada Chung Lai-ling
Privacy Commissioner for Personal Data
Room 1303, 13/F, Dah Sing Financial Centre,
248 Queen's Road East, Wanchai,
Hong Kong

24 June 2022

Dear Commissioner,

The purpose of this Submission on behalf of the Data Governance Working Group of the British Chamber of Commerce in Hong Kong is respectfully to encourage the Privacy Commissioner to develop as an urgent priority Hong Kong's data laws along the following lines:

1. Implementation of the remainder of the areas of modernisation of the Personal Data (Privacy) Ordinance ("PDPO") as brought before LegCo in January 2020;
2. bringing into force Section 33 PDPO;
3. engagement with other Greater Bay Area authorities to drive cross-border exchanges of data (whether through sandboxes, certified usage or otherwise); and
4. at the same time, preserving the essence of data protection laws, namely to enhance consumers' and individuals' ability to control their data use (rather than data laws acting as instruments of control).

**Background**

When it was drafted in 1995, the PDPO was arguably ahead of its time. With one eye on the European Union Data Protective Directive of the same year, it predated the UK's Data Protection Act 1998 by three years and made the UK's existing Data Protection Act 1984 seem outdated. Understandably, during the early years since enactment, the emphasis of successive Privacy Commissioners was on raising public awareness. Although there were lengthy periods of public consultation during the 2000s as to ways in which the PDPO could be upgraded, these did not result in change until 2012, following a scandal relating to overuse of personal data in direct marketing during the summer of 2010. The result was a partially updated law which had a decidedly lopsided approach to penalties, (only those transgressions added in 2012 giving rise to even potentially harsh penalties). The effect of this was exposed in subsequent high profile data breaches, in which data users seemingly escaped without meaningful financial penalties.

**Planned areas for development of PDPO**

Much has happened in worldwide data, privacy and cyber laws over the past 25 years. In recognition of this the PCPD presented six areas for development of the PDPO to LegCo in January 2020. Of these, only the anti-doxxing legislation has been formulated and enacted (at record speed).

We are keen to voice our members' support for modernising the PDPO to cater for the remaining developments, with the following comments.

1. Mandatory data breach notifications
   Given the limited size of Hong Kong's data economy, it would be sensible to adopt a more moderate approach (e.g. the Australian model) to minimise the compliance burden of businesses whilst ensuring adequate data protection.

   - *Notification threshold*
     We agree that there should be a clear and quantifiable threshold for obligations to notify. The test of "real risk of significant harm" may be too vague unless there are clear criteria used to measure the level of risk involved e.g. type or quantity of data involved; number of data subjects affected; and availability of encryption and anonymisation. A clearer threshold will enable data users to submit more meaningful notifications.

   - *Timeframe*
     We agree that data users should be given time to investigate suspected incidents of data breach, after which they should notify PCPD and affected users within a specified timeframe. The notification should focus on identifying the major issues (e.g. cause of breach, risk of harm, remedial steps) and PCPD can ask for subsequent elaborations.

2. Fines
   We note that PCPD is looking into introducing direct administration fines. But linking fines to companies' turnover is arbitrary and may not be proportionate to the damages caused by non-compliance. Such a move may also undercut the attractiveness of Hong Kong as a place for data-related business.

3. Data processors
   It is now common practice to directly regulate data processors. But there should also be clear guidance on (i) specific obligations for data processors; (ii) extent to which data users are responsible for non-compliance by their processors; and (iii) transition arrangements for data users and regulators to meet the new obligations.

4. Data retention
   We are supportive of the suggestion that data users should be required to have clear retention policies. Properly adopted, use and adherence to meaningful retention periods is ultimately for the benefit of all parties.

5. Definition of personal data
   We are also supportive of the suggestion that the PDPO definition be expanded to include information that relates to an "identifiable natural person", rather than an "identified person". As data analytics becomes more sophisticated, it is necessary to expand the definition in this way for consumer protection. This is entirely consistent with equivalent definitions adopted in other jurisdictions.

**Cross-border data transfer and section 33 PDPO**

It is welcomed that PCPD has recently published Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data. Such clauses have from the outset been an important building block of the section 33 PDPO arrangements.

Although section 33 has never featured in the public consultations of the 2000s, the 2012 PDPO amendments, or the PCPD's January 2020 suggestions to LegCo, we are aware that successive Privacy Commissioners have been working behind the scenes to make progress on arrangements for bringing section 33 into force. Anecdotally, regulatees of the SFC and HKMA routinely adhere to section 33 in any event, both out of best practice and to align themselves with the requirements of most other leading financial centres.

It is perhaps ironic that the provisions of section 33 – which were market leading in 1995 – unlike other elements of data protection legislation remain market standard now. It is suggested that:

a) With the possible exception of subsections (3) and (4), section 33 is brought into operation; and
b) the business community is given a viable roadmap to enable it to accommodate the necessary changes.

This would be consistent with what we understand to be the legislative intent of the PDPO, namely to enhance and protect the rights of citizens when marshalling the use of their personal data.

**Data sharing amongst data users in the Greater Bay Area ("GBA")**

There is a need for a more accommodative cross-border data flow regime aimed at closer integration with the GBA. While high-level policy documents have been supportive of data sharing and trading along the GBA, China's Personal Information Protection Law ("PIPL") has imposed stringent cross-border transfer requirements that could likely affect Hong Kong's role in the GBA data economy. (It is noted that PIPL envisages use of Model Contractual Clauses in the same way as section 33, so there is commonality there).

Our members are keen to see progress being made in this area, perhaps through a sectoral approach (for example cross-border medical records for retirees; cross-border support for wealth products etc).

**Cybersecurity Law**

Our members are keen to participate in consultation surrounding the potential Cybersecurity Law for Hong Kong's critical infrastructure presaged by the outgoing Chief Executive in her final Policy Address. Again, it is important that such legislation is reflective of the legislative intent to safeguard the personal data of citizens, and to maintain the integrity of systems upon which civic society depends.

**Request**

We would humbly request the opportunity to meet with you at your earliest convenience to discuss this Submission. Modernising Hong Kong's data laws is a key component of ensuring Hong Kong retains its competitiveness as an international financial and trading hub.

With best wishes

Yours sincerely,

**David Graham**

Executive Director

The British Chamber of Commerce in Hong Kong