

Submission in response to the Consultation Document on Review of the Personal Data (Privacy) Ordinance

Executive summary

HKITF's key submissions are as follows:

- HK should retain the principles-based, technologically neutral approach to privacy regulation as currently provided for in the Personal Data (Privacy) Ordinance (“**PDPO**”) and the Data Privacy Principles (“**DPPs**”);
- Data protection obligations should vary in proportion to the sensitivity of the personal data, and this principle can be better achieved by tailoring the existing DPPs rather than creating a separate regime to define and protect sensitive personal data,
- A voluntary breach notification scheme with clear and effective guidelines is appropriate for a city like HK;
- Indirect regulation of data processors and sub-contractors is preferred;
- Proposals to grant criminal enforcement powers to the PCPD and to make the contravention of a DPP an offense not supported; and
- HKG to engage key stakeholders in order to identify and implement the best methods of advancing health privacy.

Proposal No. 1 - Sensitive Data

1.1 Sensitive personal data

HKITF appreciates that certain types of personal data are more sensitive than other types, and that the degree of sensitivity should be a crucial factor in determining the appropriate level of regulation for personal data.

However, the creation of a separate statutory regime for “sensitive personal data” may not be the best solution, and may even cause greater confusion and higher compliance costs for businesses in HK, that are mainly SMEs. We believe that differential treatment based on different personal data types is more effectively achieved by incorporating the differential treatment concept into the DPPs, rather than by creating a separate regime. As discussed in the APEC Privacy Framework 2005, data controllers should be required to implement **appropriate safeguards** that are **proportional** to:

- (a) the likelihood and severity of the harm threatened;
- (b) the sensitivity of the information; and
- (c) the context in which it is held.

With technology advancement and changing market conditions, the degree of flexibility afforded by this kind of test is critical and cannot be matched by a statutory scheme that arbitrarily partitions personal data into “sensitive” and “not sensitive”. This flexibility also avoids the risk of data users adopting measures to artificially move data from “sensitive” to “not sensitive”, since it requires a consideration of all of the circumstances surrounding the data, rather than just the application of a single statutory definition.

1.2 Biometric information

HKITF advocates that technological neutrality promotes the adequacy and effectiveness of the PDPO and should be maintained wherever possible, and is concerned that the classification of biometric information as sensitive personal data inappropriately focuses on the methods of data collection and storage, rather than the inherent characteristics of the data. Indeed, as paragraph 3.06 of the Consultation Document states (emphasis added):

*“Biometric data **could reveal** sensitive personal information such as health, genetic information, or ethnic origin.”*

As far as HKITF is aware, there is no internationally accepted test for “sensitivity” or definition of “sensitive personal data”. If HK were to define biometric information as sensitive information and impose its own standard, this may have the unintended impact of stifling innovation and R&D efforts in the area of bio technology. This is contrary to the HKG policy of encouraging innovation and technology, and to have HK as the IT hub for the region. Any local standards that are inconsistent with international practice will further discourage MNCs to invest in HK.

One alternative to address the public concern for protecting HK citizens data against fraudulent use of personally descriptive data (such as in the case of identity theft and impersonation) may be to review HK’s existing criminal laws. The risks we are concerned about may be better dealt with under cybercrime legislation rather than privacy laws.

Proposal No. 2 - Regulating Data Processors and Sub-contracting Activities

2.1 Indirect regulation preferred

With the explosion of Web 2.0, data is incredibly mobile, and that it is now common for data to be collected and then transferred to another entity, to another country, or both. HKITF urges HKG to exercise caution in establishing a mechanism that will ensure that adequate data protection obligations are preserved at each link in this chain of custody, while avoiding excessive regulations that would discourage e-commerce and inhibit innovation.

The current indirect regulation regime allows the interests of consumers to be preserved without sacrificing flexibility. We support the proposal that require the data user and data processor in each instance to adopt suitable measures to regulate the transfer and processing of customer data, contractual or otherwise, to ensure compliance with the PDPO.

The indirect regulation model is also consistent with the model described in Principle 9 (Accountability) of the APEC Privacy Framework, which requires personal information controllers remain *accountable* for the protection of personal information they collect, use or hold even if that data is transferred from one jurisdiction to another. Importantly, as with the indirect regulation model in the Consultation Document, the accountability principle allows data users to tailor their compliance method to a given context.

On the contrary, direct regulation of data processors fails to offer the flexibility and consistency benefits associated with indirect regulation. With the popularity of social network and cloud computing services, personal data is frequently transferred to a data processor, but remains under the control of the data user. Under such circumstances, it would be unreasonable to simply deem the data processor as being equivalent to the data user, since clearly the user and processor do not have the same ability to ensure the security and lawful use of the data.

HKG should also be mindful of the practical challenges in enforcing direct regulation against data processors. The commercial reality is that many data processors that serve data users in HK are off-shore and not subject to HK jurisdiction. Given that HK privacy law has no extraterritorial effect on those off-shore entities, having direct regulation on data processors will only create additional burdens for those providing data processing services in HK, but fail to offer the kind of control and protection it intends to achieve.

2.2 Regulation by category of data processor?

The Consultation Document also requests comments in relation to the proposition that different types of data processors should be made subject to different categories of regulation. HKITF believes that privacy regulation should be phrased in terms of outcomes and principles, and that implementation is a matter best left to data subjects, data users and data processors. Consequently, we do not support the categorisation of data processors in the PDPO, as HKITF is not convinced that such categories could be drafted sufficiently generically and in a technology-neutral manner to ensure that the categories remain relevant in the future. A suitable general obligation, along the lines of the indirect model discussed above, is a more effective regulatory strategy.

Proposal No. 3 - Breach Notification

3.1 Introduction of breach notification

HKITF supports the introduction of a voluntary breach notification obligation in the PDPO, as an appropriately structured mechanism of this kind promotes public confidence in the data custody practices of data users. However, to be effective and offer protection to consumers, such voluntary

breach notification system should be supported with clear guidelines from the PCPD.

On the other hand, the introduction of a mandatory breach notification at this time may have unknown and potentially significantly detrimental impact on data users.¹ HKITF considers that the policy goals associated with breach notification can be effectively achieved by a voluntary scheme, and agrees with the Consultation Document conclusion that implementing a mandatory scheme as an outcome of the current consultation process would be premature.

There is not a consistent international approach in the area of breach notification, and in particular there is no agreement on the whether breach notification requirements should be tied to the citizenship of the affected data subjects, or to the location of the breach, or to some combination of both. In this context, a mandatory regime imposed by Hong Kong may potentially conflict with the regimes of other jurisdictions, and that this would place multinational companies in a difficult, and potentially costly, compliance position.

3.2 Guidance on breach notifications

As recognised in the Consultation Document, one of the key issues associated with the introduction of a breach notification obligation is identifying the types of data breaches where a breach notification would be an appropriate step for a data user to take. HKITF believes that an individual should be informed of a security breach if that breach could reasonably result in the misuse of that data subject's unencrypted sensitive financial information. This threshold marks an appropriate balance between empowering data subjects to minimise the more serious consequences that might flow from a security breach involving their personal information, and avoiding a situation whereby security notifications are so frequent that data subjects disregard them or are unable to differentiate between those that indicate a significant risk and those that do not.

If the HKG were to introduce a voluntary notification regime, it would be useful if the PCPD were to publish guidance on the factors that data users should take into account when deciding whether to issue a breach notification to data subjects.

3.3 Form and timing for notification

In HKITF's view, data users should be afforded discretion as to the method by which they provide breach notifications to affected data subjects. Data users should be able to take into account factors such as:

- (a) the size of their organisation;
 - (b) the number of recipients of the notification;
 - (c) the relative cost of different methods of providing the notification;
- and

¹ See Consultation Document paragraph 4.34.

- (d) the ways in which the data user typically communicates with its customers,

when determining when and how to notify data subjects of a data breach.

More generally, the HKG may draw reference from the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice² (which interprets s 501(b) of the United States' *Gramm-Leach-Bliley Act*), which provides a useful model for fleshing out a breach notification obligation. The Interagency Guidance considers matters such as how to identify data subjects affected by a regulated security breach, the timing and content of any breach notification and the manner in which any breach notification should be delivered.

Proposals No. 4 – 12 - Criminal Sanctions

4.1 Criminalisation of PCPD provisions

In general, HKITF opposes to the criminalisation-related proposals in the Consultation Document, as the principle-based drafting of privacy obligations is generally inconsistent with the imposition of criminal penalties. Criminalising such obligations would create significant uncertainty, as businesses will not necessarily know when particular behaviour becomes criminal. HKITF is particularly concerned about the adverse effect that criminalisation would have on the IT industry, where businesses are often engaged in new or innovative activities.

In relation to the DPPs, as pointed out in paragraph 6.04 of the Consultation Document, the *"DPPs are couched in generic terms and can be subject to a wide range of interpretations"*. We agree with the Consultation Document that criminalising non-compliance with the DPPs would be counter-productive (see Proposal No. 7), and consequentially recommends that contravention of the DPPs not be made an offence.

HKITF believes that civil remedies in general should provide adequate protection to citizens affected by any non-compliance. There may be exceptions in cases of identity theft or malicious dealing of personal data, but again we feel those situation may be better dealt with under cybercrime law regime.

Others

5.1 Health Privacy

The current consultation does not cover health related information in general. The health sector presents unique and complex privacy issues, many of which have only recently emerged due to the relatively recent update of technology in this sector.

² Issued by the Office of the Comptroller of the Currency (Department of the Treasury), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (Department of the Treasury). Available at: <http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf>.

The plan of HKG to launch a SAR-wide electronic health record (eHR) system presents a number of privacy concerns. HKITF considers it critical that there be control by patients over tiered access to his/her health data. A privacy-sensitive approach to the development of the eHR system is needed to ensure that the system is designed with built-in checks and balances to lower the risk (both in terms of the likelihood and magnitude) of data security breaches. HKITF urges HKG to engage as early as possible in consultation with government, industry and other key stakeholder groups in order to identify and implement the best methods of advancing health privacy.

By Hong Kong Information Technology Federation

November 30, 2009

Established in 1980, the Hong Kong Information Technology Federation is a nonprofit, non-political trade association that acts as a forum in which the IT-related businesses in Hong Kong can work together for the benefit of the industry and to maintain a high level of business practice amongst the members.

Web: <http://www.hkitf.org>