HKITF and HKISPA

Joint Submission in response to the Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance ("PDPO")

---

1 Executive summary

The Associations' key submissions are as follows:

1.1 **The Associations support the following proposals in the Consultation Report**

(a) not to proceed with separate regulation for sensitive data (Proposal No. 1 in the Consultation Document; Proposal No. 38 in the Consultation Report);

(b) to regulate data processors indirectly rather than directly (Proposal No. 2 in the Consultation Document; Proposal No. 5 in the Consultation Report);

(c) to have a staged implementation of a breach notification scheme, with the first stage to be a voluntary scheme (Proposal No. 3 in the Consultation Document; Proposal No. 6 in the Consultation Report); and

(d) not to grant the Privacy Commissioner for Personal Data ("the Commissioner") criminal investigation and prosecution powers, or to empower PCPD to award compensation to aggrieved data subjects, or to make contravention of a Data Protection Principle ("DPP") an offence, or to empower PCPD to impose monetary penalty on serious contravention of DPPs (Proposals No. 4, No. 6, No. 7 and No. 10 in the Consultation Document; Proposals No. 39. No. 40, No. 41 and No. 42 in the Consultation Report).

1.2 On specific proposals

The Associations' key submissions on specific proposals are as follows:

(a) if the Constitutional and Mainland Affairs Bureau ("the **Bureau**") elects to proceed with a strengthened offence related to direct marketing (Proposal No. 1), the Associations submit that the status quo should be maintained and the provision of an opt-out notice should be required at the time of first use of the personal data;

(b) the Associations oppose the creation of new criminal offences for the unauthorised sale or disclosure for profit of personal data (Proposals No. 2 and 3);

(c) if the Bureau nevertheless moves to enact offences for the unauthorised sale or disclosure for profit of personal data (Proposals No. 2 and 3), adequate safeguards should be put in place;

(d) guidelines rather than mandatory clauses should be introduced for indirect regulation of data processors and sub-contractors via contractual means (Proposal No. 5); and

(e) voluntary data breach notification guidelines published by the Commissioner should take into account the sensitivity of the information disclosed and the need for notification to occur.

2 Collection and Use of Personal Data in Direct Marketing (Proposal No. 1)

2.1 Current PDPO position - opt-out on first use

Section 34 of the PDPO currently provides that a data user shall (emphasis added):

> *(i)* ***the first time he so uses those data*** *after this section comes into operation, inform the data subject that the data user is required, without charge to the data subject, to cease to so use those data if the data subject so requests;*
>
> *(ii) if the data subject so requests, cease to so use those data without charge to the data subject.*

Contravention of this requirement is an offence punishable on conviction by a fine at level 3 (section 64(10)).

2.2 Opt-out on first use should be preserved in the strengthened offence

If the Bureau elects to proceed with a strengthened offence related to direct marketing, the Associations submit that the provision of an opt-out notice should be required at the time of first use of the personal data, rather than on or before the data user's initial collection of the data as proposed in the Report. The Associations are of the view that this strikes an appropriate balance between the interests of data subjects and the interests of businesses that are data users.

Direct marketing has been a thriving industry in the Hong Kong economy, and any changes to the law would impact many data users engaging in one form of direct marketing or another. According to a report recently released by Office of the Telecommunications Authority ("OFTA") on two surveys conducted on person-to-person telemarketing [1], nearly half of respondents would not reject person-to-person calls straightaway. The surveys also revealed that person-to-person marketing calls do bring about economic benefit to the community. The proposals OFTA made in moving forward with regulating person-to-person marketing calls do not include imposing any criminal sanctions. Rather, OFTA calls for closer collaboration with industry to formulate voluntary code of practice with in-house unsubscribe list and rules to honour unsubscribe requests and enhancing public awareness of right to unsubscribe and ways to protect them from unwanted person-to-person calls. The Associations' view on first use opt-out would be consistent with these survey results and OFTA's recommendation.

2.3 Collection of personal data for direct marketing

It is proposed in the Consultation Report that when collecting personal data from data subjects for direct marketing, the intended marketing activities, the classes of persons to

[1] UCAC Paper 1/2010 http://www.ofta.gov.hk/en/ad-comm/ucac/paper/uc2010p1.pdf

whom the data may be transferred and the kinds of data to be transferred should be "reasonably specific". If data user does not comply with these requirements and subsequently uses the personal data for direct marketing purposes, it may lead to criminal liability (paragraph 3.2.35).

The Associations believe that the creation of this criminal offence is harsh, as there is high uncertainty relating to the requirement of "reasonably specific". The Associations also fear that the proposal may not achieve the purpose it sets forth to achieve. Some firms are already thinking that in order to comply with this paragraph, they would have the scope drafted as wide as possible in their Personal Information Collection Statements ("PICs"), and put down every possible (even though remote) use of the data, the potential transferees and data that may be transferred, while remaining as "reasonably specific" as possible in the description. This totally defeats the purpose of having the requirements in the first place, which is to give data subjects a better understanding of how their personal data might be used and transferred. PICs with such wide scope will mean little to data subjects trying to understand their rights.

Hence the Associations would urge the Bureau not to make non-compliance of these requirements relating to direct marketing elements of a criminal offence. These requirements are already enshrined in the DPP No.1. the Associations fear that the current proposal would set an undesirable precedent of making contravention of a DPP an offence, a proposal that the Bureau has made clear not to pursue (Proposal 41). The requirements would be more appropriately dealt with in the form of guidelines issued by PCPD.

2.4 Other proposals relating to use of personal data for direct marketing

The Associations commented above that the status quo of opt-out on first use should be maintained. If however the Bureau decides to move forward with giving data subjects the choice on or before collection of personal data, the Associations still support the opt-out, rather than the opt-in model. The Associations also support the Bureau's view that it is not appropriate to introduce a territory-wide do-not-call register against direct marketing activities.

---

3 Unauthorised Sale of Personal Data and Disclosure for Profit or Malicious Purposes (Proposals No. 2 and 3)

3.1 New criminal offences

The Consultation Report proposes introducing two new criminal offences. One on unauthorised sale of personal data (Proposal No. 2) and the other on unauthorised disclosure for profits or malicious purposes (Proposal No. 3).

3.2 Comparable offences in other jurisdictions

Jurisdictions with similar legal systems to that of Hong Kong only impose criminal liability for mishandling of personal data in a limited range of circumstances, and in a manner that requires a high threshold to be reached before guilt can be found -

- United Kingdom - it is an offence to "knowingly or recklessly, with the consent of the data controller, obtain or disclose (or procure the disclosure of) personal data".[2] This offence is subject to a number of defences, including where use or disclosure is necessary for preventing or detecting crime, required or authorised by law, where the use of disclosure is in the public interest, or where the relevant person has a reasonable belief that either: (i) he had the right to obtain or disclose; or (ii) he would have had consent if the data subject had known the circumstances of the use or disclosure.
- India - it is an offence for any person, including an intermediary, to disclose personal information that has been accessed in the course of providing services under the terms of a lawful contract, where that disclosure is made (i) without the consent of the data subject or in breach of lawful contract, and (ii) with intent to cause, or knowing that the disclosure is likely to cause, wrongful loss or wrongful gain.[3] This offence is punishable by imprisonment for up to three years, a fine of up to five lakh rupees (approximately USD$11,000) or both.
- Australia and New Zealand - there is no specific criminal offence for the unauthorised sale of personal data. However, in a number of Australian jurisdictions, a person commits an offence if he or she deals with information for the purposes of committing an indictable offence,[4] and at the Federal level the data protection offences also require the "intent to commit a serious offence".[5]

3.3 The Associations' primary position – against criminalisation of non-compliance of privacy regulation

The Associations oppose the introduction of new criminal offences for the unauthorised sale or disclosure of personal data as part of the current PDPO reform process. The Associations believe that embedding such offences in the PDPO is not consistent with international practice, which is to create specific cybercrime offences to bolster existing fraud offences rather than by imposing criminal liability via privacy regulation.

The Associations' are therefore of the view that it is inappropriate to implement these new offences as part of the current consultation process, and the appropriate forum for new criminal offences to be considered is in the context of a review of Hong Kong's existing criminal laws, rather than reform of the PDPO.

3.4 The Associations' alternate position - form of offences should be modified

If Bureau does elect to proceed with new criminal offences for the unauthorised sale and disclosure of personal data as part of the current legislative reform process, The Associations strongly advocate that the form of the offences be redrawn so as to be

---

2 Data Protection Act 1998 (UK) s 55.

3 Information Technology Act 2000 (India) s 72A.

4 See, for example, Criminal Code Act 1899 (Qld) s 408D "Obtaining of dealing with identification information".

5 See Criminal Code (Cth) sections 477.1 " Unauthorised access, modification or impairment with intent to commit a serious offence" and 478.1 "Unauthorised access to, or modification of, restricted data".

consistent with the following principles (in addition to the general principles set out in section **錯誤! 找不到參照來源。** below):

(a) A single offence should apply to each event giving rise to "sales" or "unauthorised disclosures"

It is unclear whether the proposed offence applies to each item of personal data that is "sold" or "disclosed", or to each transaction, although the implication of the link between an unlawful sale or disclosure and user consent implies that it is intended to operate at an item level. In the Associations' view this is not appropriate, given that the sale or disclosure of data could involve thousands or tens of thousands of items. The offences should make clear that each "sale" or "unauthorised disclosure" transaction only gives rise to single offence, and the seriousness of the unlawful sale or disclosure should only be used as a factor in determining the ultimate penalty that is imposed.

In addition, the concepts of "sale" and "unauthorised disclosure" should also be clearly defined, and so as not to include co-operative marketing activities or other co-ordinated activities where there has not truly been a "sale" or "unauthorised disclosure" of personal data.

(b) The "opt-out model" should be adopted for both offences

The opt-out model is consistent with the position currently taken under similar Hong Kong ordinances,[6] and therefore represents the position that the Hong Kong business community is currently most familiar with. If the opt-in model were to be adopted, then this would impose a significant additional compliance burden on Hong Kong businesses in general, and particularly on those that currently operate in the direct marketing space and have processes in place to comply with the current legal requirements.

(c) Defences should be adopted as per the UK Data Protection Act

The defences applicable under section 55 of the UK Data Protection Act are summarised above, and the Associations are of the view that these should reflected in the drafting of the new offences. In particular, the Associations believes that the "reasonable belief" defences are important constraints on the scope of the offences, and appropriately tailor the offences to the circumstances most likely to be of concern to the general public.

(d) The "unauthorised sale" offence (Proposal No. 2) should apply to sale transactions only

The proposed unauthorised sale offence would be triggered by the sale of personal data for "a monetary or in kind gain". The Associations understand the

[6] See, for example, the Unsolicited Electronic Messages Ordinance s 10 (prohibition on sending commercial electronic messages after an unsubscribe request is sent) and the PDPO s 34 (a data user must cease using personal data for direct marketing purposes if the data subject so requests).

rationale for the prohibition to apply to monetary transactions, but are concerned that "in kind gain" is a general phrase that could be interpreted broadly, and in particular could apply to otherwise perfectly legitimate business activities such as joint promotional or marketing activities. In the Associations' view, it would be inappropriate for such activities, which are better characterised as data transfer or data sharing rather than data sale, to be subject to criminal liability as a result of inadvertent or accidental acts by the data user.

As a consequence, the Associations submit that the phrase "monetary or in-kind gain", rather than clarifying the scope of the proposed offence, in fact makes the offence more onerous and less certain. For this reason, the Associations' preference is for the phrase to be removed, and for the offence to simply related to the unauthorised "sale" of personal data.

(e) The PDPO should be the sole statement of each offence

Given the significance of the proposed criminal offences and the prejudice associated with any finding of criminality, it is imperative that the operation of each offence be clear and predictable. This can be best achieved by ensuring that all elements of each criminal offence are set out in the PDPO, including the applicable defences, and that policy and guidance documents (or other ancillary materials) do not have any role in determining whether or not an offence has been committed.

(f) The scope of each offence should be clearly defined so as to avoid overlap

The strengthened data protection offence (Proposal No. 1) will apply to misuse of personal data for direct marketing, the new unauthorised sale offence (Proposal No. 2) will apply to the sale of personal data for "a monetary or in kind gain", and the new unauthorised disclosure offence (Proposal No. 3) will apply to disclosure without consent for profits or malicious purposes. In the Associations' view, these formulations are quite similar, and it could be argued that the offences overlap, or are a subset of one of the other offences.

In order to remove areas of overlap, and to eliminate the associated uncertainty, the Associations believe that each offence should be clearly defined so as to operate in a discrete area. This could be achieved, for example, by eliminating the direct marketing offence (on the basis that it is a subset of the unauthorised sale offence), implementing the unauthorised sale offence in respect of all persons (as opposed to "data users" only), and modifying the unauthorised disclosure offence so that it only applies to malicious (in the sense of intentionally harmful) conduct.

(g) Intention to cause harm should be a clear element of each offence

In other jurisdictions, these types of offences (if they exist) generally require more than a factual finding that an unauthorised use, sale or disclosure has

occurred; the unauthorised use, sale or disclosure must have been accompanied by an intent on the part of the seller. The level of intention varies between jurisdictions, but the Associations' preference is for the Indian model: "intent to cause, or knowing that the [use, sale or] disclosure is likely to cause, wrongful loss or wrongful gain". The Associations believe that this formulation reduces the risk that inadvertent or careless conduct will be criminalised, while still appropriately targeting behaviour which is socially unacceptable.

(h) A specific due diligence defence should be inserted

The Unsolicited Electronic Messages Ordinance ("**UEMO**") contains a number of offences relating to the misuse of data. In each instance, it is a defence "for a person a person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence".[7] Given that the PDPO deals with similar subject matter to the UEMO, the Associations submit that it would be appropriate to incorporate this UEMO defence into the PDPO.

4 Regulation of Data Processors (Proposal No. 5)

The Associations support the proposed indirect approach to the regulation of data processors and sub-contractors, namely by requiring the data user to use contractual or other means to ensure that its data processors and sub-contractors comply with the PDPO.

The Associations also support an enhanced publicity and education campaign conducted by the Office of the Commissioner. However, the Associations are concerned that the proposal for the Office of the Commissioner to provide practical guidelines on the terms and conditions to be included in data processor contracts could be interpreted as mandating the creation of "approved" contract terms. In the Associations' view, this would be an undesirable outcome, because it is inevitable that such terms would be superseded by rapidly advancing technology and business models, and inhibit the flexibility with which high technology businesses are offered and conducted in Hong Kong. As a consequence, the Associations submit that the guidance issued by the Commissioner in this area should be of a general nature only, and not consist of "approved" or "model" terms.

5 Breach Notification (Proposal No. 6)

The Associations support the introduction of a voluntary breach notification system, with guidance notes issued by the Office of the Commissioner. In relation to the content of such guidance, the Associations re-iterate their view that the scope of the notification obligation should be sensitive to a balance between empowering data subjects, and creating an environment where notifications become common enough to lack force or be ignored by data subjects.

[7] See UEMO sections 16(4), 17(3), 18(4), 58(5).

The *Guidance on Data Breach Handling and the Giving of Breach Notifications* published by the Office of the Commissioner,[8] is an excellent starting point for the development of an effective and efficient notification process. The Associations believes, however, that the Guidance could be enhanced by the inclusion of a list of the scenarios most likely to require breach notification, with the unauthorised disclosure of unencrypted sensitive financial information at the top of this list.

The Associations also believe that the Guidance does not currently give sufficient weight to the burden that breach notification can impose on data users, and as a consequence the Associations advocate that the list of relevant factors to consider when deciding whether, and in what form, to issue a breach notice should include:

(a) the relative cost of different methods of providing the notification;

(b) the ways in which the data user typically communicates with its customers; and

(c) whether or not a delay in notification is reasonable (such as in the case where a law enforcement agency requests a delay).

Finally, the Associations submit that Bureau and the Office of the Commissioner should give consideration to measures that would provide data users with safe harbour in the event that they comply with the voluntary breach notification guidelines. In the Associations' view, such a protection would create a powerful incentive for data users to participate in the voluntary breach notification program, with its corresponding benefit to Hong Kong data subjects. Such a safe harbour could, for example, take the form of immunity from prosecution or private litigation in respect of a data breach event, provided that there has been compliance with the guidelines.

6 Other proposals

The Associations' view on some other proposals in the Consultation Report -

Proposal 4 - excluding "social services" from the definition of "Direct Marketing" - this should clearly exclude the offering of social services and facilities by social workers to individuals in need, and this should be broaden to cover activities of NGOs as many social workers are in fact employed by NGOs.

Proposal 10 - Time limit to discontinue investigations - if 45 days is too short, the Associations may explore lengthening it but in any event the time limit should not be over 3 months.

Proposal 34 - exemption for personal data held by the court or judicial officer – the Associations do not see why this exemption is necessary. This should not be an absolute immunity to this class of data users.

[8] See http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf

Proposal 37 - time limit to initiate formal prosecution – the time limit of 6 months as-is is not too short, and the proposed 2 years period is too long and creates inconvenience to business. The Associations consider that a time limit of 12 months would be acceptable.

Submitted Jointly by:
Hong Kong Information Technology Federation and
Hong Kong Internet Service Providers Association

December 31, 2010