THE LAW SOCIETY OF HONG KONG 香港律師會

Comments on Consultation Paper on "Review of the Personal Data (Privacy) Ordinance ("PDPO")"

The Law Society makes the following comments on the Proposals in the Consultation Paper:

Proposal No.1: Sensitive Personal Data

As the size of each organization and complexity for handling data access request in each case is different, it would be impractical to research into organizations / cases in order to determine an average or a reasonable administrative cost to be charged. We suggest that the administrative fee shall be absorbed into the non-refundable processing fee of HK$50.00 payable upon lodgment of a data access request, as suggested by the Commissioner, in addition to the fees chargeable under the proposed fees schedule.

It is also agreed that that the handling of sensitive personal data should only be permitted in the specific circumstances set out in paragraph 3.09 of the Consultation Paper. However, the exemptions should be amended as follows:

3.09 The collection, holding, processing and use ("handling") of sensitive personal data would be prohibited except in the following circumstances:

(a) the prescribed consent (i.e. express consent given voluntarily) of the data subject or a person authorised to act on the data subject's behalf has been obtained;

(b) it is reasonably necessary for the data user to handle the data to exercise his right as conferred by law or perform his obligation as imposed by law;

(c) handling of the data is necessary for protecting the interests of the data subject or others where prescribed consent of the data subject cannot be reasonably obtained in a timely manner;

(d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure to third parties without prescribed consent of the data subject;

(e) the data has been made public by the data subject or through other lawful means;

(f) handling of the data is reasonably necessary for medical purposes and is undertaken by a health professional or other person who in the circumstances

owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional; or

(g) handling of the data is reasonably necessary in connection with any legal proceedings.

We do not agree that a higher level of fine should be applicable for the contravention of these requirements. The existing sanctions are, in our view, adequate. It is not necessary that non-compliance with the DPPs should be considered an offence as this may have the consequence of making the regulatory regime too restrictive for businesses to carry out their normal functions without risking inadvertent breaches. In addition, such a step would increase the difficulty of establishing that an actionable breach has occurred.

It should be made clear that a data user should not be sanctioned for breach by a person to whom data processing etc. has been properly outsourced. Liability in such situations should be an unreasonable burden for businesses to assume in an international centre such as Hong Kong where offshore outsourcing is necessary in order to keep operational costs at internationally competitive levels.

Transitional arrangements should be implemented such that data handlers are given a certain period during which sensitive personal data is exempt from the new requirements, so that they may have time to adapt to the new regime. Given the extent to which data processing is outsourced, the transitional period should be at least 12 months. It is possible that a longer period may be necessary. Once this period is over all sensitive data must be processed in line with the new requirements. This is considered a preferable arrangement to grandfathering as it avoids the issue of sensitive personal data being processed differently depending on whether it was collected before or after these provisions come into force.

Proposal No.2: Regulation of Data Processors and Sub-contracting Activities

We agree there is a need for regulation of third party data processors given the rise in outsourcing data processing. However, imposing direct regulation upon the third party data processor is not a viable solution. Especially in light of the prevalence of overseas outsourcing (which is the norm for Hong Kong), it would be extremely difficult, if not impossible, to enforce these standards.

It is also hopelessly unrealistic to expect to be able to enforce either the PDPO or commercial contracts in all (or, in some cases, any) circumstances in the jurisdictions to which data is typically outsourced and it would place Hong Kong businesses at a competitive disadvantage if regulations were to make it impossible, impracticable or overly expensive to outsource to such countries.

It is also considered too burdensome and inflexible, given the difficulty in defining the purpose for which data is collected. Instead, the regulations should be imposed indirectly, via the data user. This approach is more in line with common international practice.

The regulations should impose an obligation on the data user to use contractual means to require the data processor and any other sub-contractors take all practicable steps to ensure the security and safekeeping of the data, to ensure the data is not misused and to delete it once it is no longer required. Contravention of this requirement would warrant enforcement

action by the PCPD, including serving an enforcement notice against the data processor. However, it is unrealistic to expect the data user to be responsible for breaches by the data processor or to have to take enforcement action at its own costs in most circumstances – the costs would be generally disproportionate to the benefits obtained (if any). This is a practicable solution as the flexibility of outsourcing data processing to third parties is retained whilst the organisation against whom an aggrieved data subject may claim redress is still the identifiable data user to whom they provided their personal data.

The blunt reality is that unless data users are able to outsource data processing etc offshore without being subject to unduly onerous restrictions or being held accountable for breaches by the data processors or subject to burdensome and expensive regulatory requirements, Hong Kong businesses will be placed at a competitive disadvantage. Accordingly, data subjects will continue to be exposed to certain risks (as at present) and appropriate risk disclosure to the effect that outsourcing/offshore transfer involves greater risk of unauthorised use or disclosure of personal data and that remedies may be limited should be provided.

Proposal No.3: Personal Data Security Breach Notification

We agree that given the widespread and increasing use of information, data users should be subject to a mandatory obligation to notify the data subjects concerned and the PCPD after becoming aware of a breach of data security which leads to the leakage or loss of personal data. This is necessary to mitigate the potential damage, including identity theft, which could result from such leakage or loss. Notification should be made as soon as possible so that data subjects may take steps to minimise potential damage. It is also important that the PCPD is notified in order to keep records up to date, to monitor organisation practices and to allow guidelines to be drawn up.

It is recommended that a system of notification should be introduced initially by voluntary guidelines issued by the PCPD. This is important in order to balance the need for notification with the costs that will be involved for businesses. These voluntary guidelines should be applicable to all industry sectors and should override any industry policies already in place to ensure a consistent approach. We note that most data users will have contact details for relevant data subjects (e.g. banks, phone companies, ISPs, insurance companies and most other businesses) and so it such not be too difficult to notify all affected data subjects of a breach. We consider the numerical approach toward notification is unnecessary.

The timing of these notifications should be as soon as possible following the breach or suspected breach, except where a delay is required by law enforcement agents. Notifications should be made individually in writing up to a certain number of data subjects but should then be made publicly, for example in a national newspaper, where the number of data subjects affected is above that threshold, e.g. 50, when it would no longer be practicable to notify each person individually. It is agreed that the notifications should include the content set out in paragraph 4.30 of the Consultation Paper. Finally it is recommended that no penalty be applied while the notification system is introduced on a voluntary guidelines basis but that once these guidelines are fine-tuned and the policy is finalised then an appropriate fine for contravention of such requirements should be implemented.

Proposal No.4: Granting Criminal Investigation and Prosecution Power to the PCPD

The question of whether the powers of criminal investigation should be granted to the PCPD will depend largely on whether some or all the offences set out in the proposals of this consultation document ultimately become law. If so, the nature of such offences are such that they are probably more suited to being investigated by the PCPD with attendant criminal investigation powers granted to it. However, if none of these offences become law, then there is no proper basis for granting the PCPD such powers for pre-existing offences with a privacy angle.

As for prosecution powers, it is not clear in the case of data privacy offences why there is a need for the PCPD to have such powers when the Department of Justice would likely be in a better position to make prosecution decisions based on wider considerations of public interest.

Proposal No.5: Legal Assistance to Data Subjects under Section 66

We agree.

Proposal No.6: Award Compensation to Aggrieved Data subjects

We agree, subject to the fact that any compensation notices are not automatically enforceable as if they were court orders, so that the PCPD would not be considered as seeking to exercise judicial power. Instead, they are treated as indicative compensation figures that are subject to being upheld and enforced by a court (with the PCPD being given statutory standing to make the necessary applications to uphold such notices) if the parties do not agree to their terms.

Care should be taken not to intake an element of punitive damages. However, we note the proposals in the latest consultation in England and Wales on breaches of the Data Protection Act[1]

[1] The Government has published its long awaited proposals on fines for serious breaches of the Data Protection Act 1998. The proposal is for a maximum fine of £500,000, with discretion for the information Commissioner's Office to assess the actual level of fines imposed on a case by case basis. The consultation period ends on 21 December, and the new fines could come into force as soon as April 2010.

The proposals are set out in consultation paper published on 9 November entitled "Civil monetary penalties: setting the maximum penalty".

The penalties will significantly boost the Information Commissioner's (currently very limited) enforcement powers. They are being introduced response to the seemingly endless tide of serious security breaches, which began to come to light almost two years ago with the HMRC debacle.

The new powers are to be found in the recently added section 55A of the DPA (introduced by section 144 of the CJIA 2008) and will apply to serious breaches of the Act which are likely to cause substantial damage or distress, and which are committed deliberately or recklessly.

The new provisions received Royal Assent in May 2008. However, the sanction is still not "live", as the amount of the penalties will need to be set by statutory instrument.

The MoJ has dropped the idea of fines based on a percentage of turnover model, similar to that used by other regulators, in favour of a fixed maximum fine which the ICO can then assess according to the seriousness of the breach and the resources of the data controller in question.

Proposal No.7: Making Contravention of a DPP an offence

Only deliberate breaches should be made an offence. Inadvertent breaches (including breaches resulting from recklessness or negligence) should not be an offence.

Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We agree with the proposal provided that "obtain" is defined as such a way to mean obtained as a result of an act intended to obtain the personal data. Unsolicited or inadvertent receipt of personal data should not be included.

Proposal No.9: Repeated Contravention of a DPP on Same Facts

We agree with the proposal.

Proposal No.10: Imposing Monetary Penalty on Serious Contravention of DPPs

We disagree. The offensive mechanism in Proposal No 7 is sufficient.

Proposal No.11: Repeated Non-compliance with Enforcement Notice

We agree with the Proposal.

Proposed No.12: Raising Penalty for Misuse of Personal Data in Direct Marketing

We agree with raising the penalty for deliberate misuses of personal data (e.g. a fine at level 6). The enforcement of opt out/do not call regulators should be given greater priority.

Proposal No.13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

(a) We agree to impose the proposed conditions to allow third parties to give prescribed consent on behalf of a data subject. We suggest the PCPD consider issuing a code of practice or guidelines to guide data user on the necessary enquires required to be made before the data user could form a reasonable belief that the conditions are fulfilled, and to advise on the possible liabilities for failing to make necessary enquires leading to contravention of the PDPO. Please also consider the balance between protection of vulnerable classes of data subjects and business/organization interests as the code of practice should not impose excessive liabilities on business/organization or affect their normal operation.

(b) We agree to expand the definition of relevant person to include the guardians of data subjects whom meet the conditions specified under this Proposal.

The consultation document poses a single question, namely whether the fine of up to £500,000 provides the ICO with a "proportionate sanction" for serious DPA contraventions. The cap seems modest when compared with fines imposed by the FSA for data breaches in the financial services sector.

The MoJ and the ICO have both indicated that the plan is for the new fines to go live in April next year.

Proposal No.14: Parents' Right to Access Personal Data of Minors

(a) and (b) Inevitably there will be a judgement call when a data user decides what would constitute reasonable grounds in order to comply with a request by a relevant person on behalf of a minor. We are of the view that such power conferred to data users shall not be a statutory right. There would be more flexibility if comment is provided in the data user's code of practice or in guidelines issued by the PCPD which would have the benefit of avoiding ambiguity. The PCPD could therefore consider issuing guidelines.

Proposal No.15: Access to Personal Data in Dispute

We agree that when access to personal data is in dispute, the relevant personal data should not be disclosed to the data requestor and other parties whom would be bound by the outcome of the decision of AAB, the court or a magistrate.

Proposal No.16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We agree with the proposed amendment to the PDPO to allow a data user to refuse a data access request on grounds of compliance with secrecy requirements under other legislation.

Proposal No.17: Erasure of Personal Data

We agree with this proposal subject to clear guidelines being issued by the to be taken to meet the requirements of reasonable practicable steps to erase personal data.

Proposal No.18: Fee Charging for Handling Data Access Requests

As the size of each organization in each case is different, it would be impractical to research into organizations / cases in order to determine an average or a reasonable administrative cost to be charged. We suggest the administrative fee shall be absorbed into the non-refundable processing fee of HK$50.00 payable upon lodgment of a data access request, as suggested by the Commissioner, in addition to the fees chargeable under the proposed fees schedule.

Proposal No.19: Response to Data Access Requests in Writing and Within 40 days

(a) We agree.

(b) We agree.

Proposal No.20: Circumstances for Issue of an Enforcement Notice

We agree.

Proposal No.21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We agree.

Proposal No.22: Removing the Time Limit to Discontinue an Investigation

We agree.

Proposal No.23: Additional Grounds for Refusing to Investigate

We agree.

Proposal No.24: Transfer of Personal Data in Business Mergers or Acquisition

We agree the transfer of personal data in mergers or acquisitions, or proposed mergers and acquisitions, is necessary to facilitate business and to promote Hong Kong as a centre for business. Therefore the conditions mentioned at paragraph 52 of the Consultation Paper should all be included.

Proposal No.25: Provision of Identity and Location Data on Health Grounds

We agreed the benefits of including location and identity of the data subject within this exemption would outweigh the risks that such inclusion may present to their data protection. Provided that the disclosure is restricted by certain conditions such as the threat of serious harm and the exemption is limited to being applied only for the purpose of lessening the risk of serious harm then sufficient protection of personal data would still be in place.

For the avoidance of doubt, neither this exemption nor any other provision of the PDPO should be used to disclose to the public (or any section of the public) the identities and addresses of persons who have been convicted of criminal offences. Such action typically makes it impossible for such persons to reintegrate with society.

Proposal No.26: Handling Personal Data in Emergency Situations

We agree that DPP 1(3) and DPP3 should not apply in cases of emergency or catastrophe but this exemption must only be employed for the purposes of lessening the threat or harm from such emergency or catastrophe. In other words, an emergency or catastrophe will not trigger a total disapplication of these principles for all users and processors for any purpose. Therefore it is important the drafting adequately limits the exemption by purpose and duration.

Proposal No.27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We agree this exemption to DPP3 should be introduced for the purpose of protecting vulnerable minors and others who may be at risk. In order to ensure the personal data of minors is still adequately protected, the language should retain the need for input from the police or other authorities, although the threshold should be much lower than the previous "concrete proof": a reasonable basis for suspension should be sufficient.

Further, the condition that such disclosure should only be permitted if it is in the best interests of the minor should not be incorporated – such a provision will only add an unnecessary element of subjective uncertainty.

Proposal No.28: Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result

- **To relieve the PCPD's obligation to notify the complainant of the investigation result and related matters under Section 47(3) when the complainant has withdrawn his complaint.**

We agree.

Proposal No.29: PCPD to Disclose Information in the Performance of Functions

- **To amend Section 46 to allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of his functions and exercise of his powers.**

We agree provided that, like corresponding provisions in legislation governing statutory bodies such as the Securities and Futures Commission and the Equal Opportunities Commission, the situations under which disclosure under this proposed ground may be made should be enumerated. Further, personal data may be disclosed to overseas data protection authorities to facilitate cross-border cooperation in the enforcement of personal data privacy rights only if the act being investigated by the overseas data protection authorities will constitute a violation of the DPPs or an offence under the PDPO if committed in Hong Kong.

Proposal No.30: Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

- **To protect the PPCPD and his prescribed officers from being held personally liable for any act done or omission made in good faith in the exercise or purported exercise of PCPD's functions and powers under the PDPO.**

We agree.

Proposal No.31: Power to Impose Charges for Educational and Promotional Activities

- **To provide the PCPD with an express power to impose reasonable charges for undertaking educational or promotional activities or services.**

We agree provided that the charges are for covering expenses and reasonable time charge and not for profit, since PCPD is exempt from taxation.

Proposal No.32: Power to Obtain Information to Verify a Data User Return

- **To confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return filed under Section 14.**

We agree in principle, provided that it is clearly indicated in the legislation that for the purpose of verifying the information in a data user return, PCPD is exercising a general inspection power comparable to inspection powers under Section 36, rather than investigation powers under Section 38, which should only be invoked when complaints are received.

Proposal No.33: Use of Personal Data Required or Authorized by Law or Related to legal Proceedings

- **To create an exemption from DPP 3 for use of personal data required or authorized by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.**

We agree that furthering legal rights is a legitimate exception to DPP3.

Proposal No.34: Transfer of Records for Archival Purpose

- **To create an exemption from DPP3 for the transfer of information containing personal data of historical, research, educational or cultural interests to the Government Records Service ("GRS") for archival purpose.**

The proposed exemption should extend only to materials already in the public domain.

Personal data collected by Government bureaux and departments which are not in the public domain should not be transferred to the GRS because:-

- It is contrary to the spirit of the PDPO for personal data to be used without consent of the data subject;

- The records kept in the GRS archive are, subject to a few exceptions, accessible to the public. Although it is proposed that after transferring the archival records to GRS, the subsequent handling of the archival records containing personal data (including access to and use of records by members of the public) will continue to be subject to the provisions of the PDPO, in the Code of Access to Information published by GRS it is provided that information about a person may be disclosed where the "public interest in disclosure outweighs any harm or prejudice that would result". There is concern that, while the PDPO does not empower the Government to make disclosure of personal data under "public interest", transferring the data to GRS will leave a door open for personal data to be disclosed to the public, without the data subject's consent, by the Government using "public interest" as a reason. The concern is aggravated by the fact that there is no mechanism under the Code of Access to Information for determination of whether or not public interest in disclosure outweighs any harm or prejudice that would result from disclosure of the personal data.

- Currently when government departments collect personal data, the stated purposes are usually limited in scope, and there is no sharing of personal data between government departments. There is concern that by allowing transfer

of personal data to GRS, data about a person can be aggregated at the GRS, contrary to the understanding of the data subjects when they first provided their personal data to the government departments.

Personal data not in the public domain has no historical, research, educational or cultural value and should not be transferred to the GRS without the data subject's consent.

Proposal No.35: Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

We agree that such an exemption should be introduced. However, it should not be applicable where the request is made by a data subject who should only be permitted to access their own personal data. A data subject's right to access his own personal data should not be conditional upon whether granting such a request would incriminate the user. The principle of privilege against self-incrimination should apply to general data access requests only.

Proposal No.36: Definition of Crime under Section 58

- **To clarify the scope of application of the exemption provision under Section 58 by defining "crime" to mean a crime under Hong Kong law, or a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation.**

We agree.

Proposal No.37: Expand the Definition of "Relevant Person"

- **To expand the definition of "relevant person" under Section 2 to include the guardian of data subjects with mental incapacity, who are appointed under Sections 44A, 59O, 59Q of the Mental health Ordinance (Cap.136).**

We agree.

Proposal No.38: Exclude Social Services from the Definition of "Direct Marketing"

- **To amend Section 34 to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.**

We agree provided that a suitable definition of "social services" is added to Section 2 of the PDPO.

Proposal No.39: Exemption for Personal Data Held by the Court or Judicial Officer

- **To add a new provision so that the PDPO shall not apply to personal data held by the court or judicial officer in the course of the exercise of judicial functions.**

All the Exemptions contained in the PDPO are either very specific (stating which Section of the ordinance or which DPP is not to apply in what situation) or very limited in scope. This is so even for very serious issues such as safeguarding the security of Hong Kong. If a full scale exemption to the PDPO is to be given to the court or judicial officers, we expect to see more explanation or justification in the Consultation Document. Furthermore, some provisions in the PDPO should apply to all data users (such as DPP4 – security of personal data) and has nothing to do with judicial independence and immunity.

Absent appropriate justification, the Law Society objects to the proposed full scale exemption of the PDPO to the court or judicial officers.

Proposal No.40: Extend Time Limit for Laying Information for Prosecution

- **To specify that the time limit for laying information for prosecution of an offence under the PDPO shall be two years from the date of commission of the offence.**

The reasons given in the Consultation Document in support of Proposal No. 40 apply to all offences and there is no justification why the time limit should be increased from 6 months to 2 years. If from past experience of the PCPD has difficulty laying information for prosecution within the 6-month time limit, we suggest that the time limit be extended to one year rather than two years. There should be a balance between convenience to the PCPD and the anxiety to the party being investigated.

Given that breach of the PDPO may not be disclosed until some time after the event, the time period should run from when the PCDP becomes aware of the offence.

Proposal No.41: Duty to Prevent Loss of Personal Data

- **To amend DPP 4 in Schedule 1 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.**

We agree. Please see responses to Proposals No. 1 and 2 above for issues relating to outsourcing. Specifically, taking legal action should not be required given the expensive and, in many jurisdictions, the futility of taking such action.

Proposal No.42: PCPD to Serve an Enforcement Notice together with the Results of Investigation

- **To amend Section 47 to allow the PCPD to serve an enforcement notice together with the results of investigation upon the relevant data user.**

We agree.

Proposal No.43: Contact Information about the Individual Who Receives Data Access or Correction Requests

- **To amend DPP 1(3) to permit a data user to provide either the job title or the name of the individual to whom data access or correction requests may be made.**

We agree.

The Law Society of Hong Kong
25 November 2009

129061v5