Consultation Document on Review of the Personal Data (Privacy) Ordinance

Submissions of the Hong Kong Bar Association

Preliminary

1. According to the Consultation Document (§4(a) refers), the first guiding principle for conducting the review of the Personal Data (Privacy) Ordinance (Cap 486) ("PDPO") is:

   "*the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests.*"

   This should not be the first guiding principle for the review. The first guiding principle – which is not included at all among the principles stated in the Consultation Document – should be that the right to privacy is a fundamental right guaranteed by Article 39 of the Basic Law, which provides for the continuation in force of the ICCPR wherein is enshrined both a general right to privacy and the right to protection of the law against arbitrary or unlawful interference with privacy, family or correspondence.

2. It is a matter of regret that the Consultation Document makes no reference to the fundamental status of the right to privacy. It is accepted that the right to privacy has to be balanced against other rights and public and social interests, but the balancing exercise must be done with the fundamental status of the right to privacy fully in mind.

3. In this Submission, the Hong Kong Bar Association sets out its response to the key proposals in the Consultation Document and also puts forward additional proposals not included in the Consultation Document.

Key Proposals

Sensitive Personal Data

Proposal 1: Sensitive Personal Data

§8: "*At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. More stringent regulation of sensitive personal data is in line with international practices. However, there is no universally agreed set of sensitive personal data and perception of sensitive personal data is culture-bound. Given the challenges posed by the development of biometric technology on an individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data.*"

4. (a) Unrecognised by the Consultation Document, the Law Reform Commission ("the LRC") in its Report on Reform of the Law Relating to the Protection of Personal Data (August 1994) ("the LRC Report") considered, but rejected, a proposal for "*a specific restriction on the collection of specific categories of data*" (§§9.40 to 9.55). The LRC was of the view that the essential issue was whether the collection of the data was relevant to the data user's functions. It also considered that concerns about the use and abuse of sensitive data would be more efficiently addressed by "*the use of declarations and affording the individual an input prior to the implementation of adverse decisions.*" (§9.55)

(b) Addressing the LRC's arguments in turn. First, the fact that collection of a particular category of sensitive personal data must be relevant to a data user's functions does nothing to subject the processing of such data to stricter control in recognition of its greater potential to do harm. Second, the system of declarations proposed by the LRC, which was implemented (in modified form) by data protection principle 5 in Schedule 1 to the PDPO, does not serve to inform individuals that particular categories of sensitive information concerning them are being held by particular data users. Lastly, the only opportunity afforded to an individual for input prior to the implementation of an adverse decision is in relation to an adverse decision consequent on a "matching procedures" (s 30(5) of the PDPO refers), which covers a relatively narrow ambit of data processing.

(c) It follows that the rationale for the LRC's rejection of specific restrictions on the processing of sensitive data does not hold good.

(d) As the Consultation Document points out, the EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data ("the EU Directive") requires Member States to apply more stringent requirements to the processing of sensitive data.

(e) Specifically (by Article 8(1)) Member States are required to prohibit "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*". This requirement does not apply in five specified circumstances, including where the data subject has given his "explicit consent" (Article 9 refers).

(f) As the Consultation Document also points out, the application of greater restrictions to the processing of sensitive data is not confined to EU Member States. This is also the case in Australia under the federal Privacy Act, as well as, for example, Japan, Korea and Macau.

(g) In line with international practice, given the higher risks posed to individuals by the processing of sensitive data (and having considered and rejected the LRC's contrary arguments), the proposal that there should be more stringent control of the processing of such data is supported. (h) However, the proposal to "*start [by] ... classifying biometric data ... as sensitive personal data*" is too narrow. Other than pointing out that "*perception of sensitive personal data is culture-bound*" (§3.03), the Consultation Document does not address the issue of why none of the types of personal data defined as sensitive in the EU Directive (see above), or variations on them, should be included within any definition of "sensitive data" at the start.

§9: "*To provide a higher degree of protection to sensitive personal data, we have set out in the consultation paper a possible regulatory model to limit the handling of sensitive personal data by data users to specified circumstances in order to narrow down the scope of collection and use of such data.*"
§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 has been obtained;
(b) it is 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 vital interests of the data subject or others where prescribed consent cannot be obtained;
(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 manifestly made public by the data subject;
(f) handling of the data is necessary for medical purposes and is undertaken by a health professional or 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 necessary in connection with any legal proceedings.*"

5. (a) There is no explanation in the Consultation Document as to why the proposed exceptions have been formulated in the way they have. While the justification for some of the proposed exceptions, such as (a) and (c), is obvious. The same cannot be said for others. It is not clear, for example, why proposed exception (g) should be necessary given proposed exception (b).

   (b) There is some overlap between the proposed exceptions and the exceptions provided for in the EU Directive. For example, proposed exceptions (a), (c) and (e) are similar to exceptions (a), (c) and (e) under Article 9 of the EU Directive. However, proposed exception (b) is broader that its equivalent under Article 9, which is restricted to obligations and rights "*in the field of employment law in so far as authorised by national law providing for adequate safeguards*", and proposed exceptions (d), (f) and (g) have no equivalents at all under the EU Directive.

   (c) Proposed exception (d) is of particular concern because it would render the proposal for special control on the processing of "sensitive data" close to being nugatory. Save for the addition of "*appropriate safeguard against transfer or*

disclosure to third parties without prescribed consent of the data subject", exception (d) is in fact the *status quo* under the PDPO pursuant to which there is no special control on the processing of "sensitive data". As a result, if exception (d) were adopted, data users could continue to collect, hold, process and use "sensitive data" as they did before *so long as* they did not transfer or disclose the data to third parties or only did so pursuant to exemptions to DPP3 as provided for in Part VIII of the PDPO (bearing in mind the recommendation to apply all the exemption provisions of Part VIII of the PDPO to "sensitive data": see §3.10 of the Consultation Document).

(d) The inclusion of exception (d) is objected to accordingly.

§3.12: "*We may consider making non-compliance with DPPs with regard to handling of sensitive personal data an offence.*"

6. For the same reason that this proposal should not be adopted generally (see below), viz. the DPPs are not precise enough to allow for sufficient certainty as to what they prohibit or permit to found criminal offences, so too should this proposal not be adopted in relation only to "sensitive data".

§§3.13 & 3.14: "*It may be advisable to apply the new requirements only to sensitive personal data collected after the relevant legislative provision comes into force ... Alternatively, we may specify a transitional period following the enactment of the new provision during which the processing of sensitive personal data will be exempted from the additional requirements.*"

7. (a) Sensitive personal data collected before the proposed new restrictions on the processing of such data come into force should not be excluded from the application of the new restrictions indefinitely. Accordingly, a transitional arrangement is preferred whereby such data will be made subject to the new restrictions upon the expiry of a specified period.

(b) For the avoidance of doubt, the transitional period should *not* apply to sensitive personal data collected after the new provisions come into effect.

Data Security

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

§§10-12: "*The rising trend of data users sub-contracting and entrusting data processing work to third parties has increased the risk to which personal data may be exposed. At present, the PDPO does not regulate processors which process personal data for data users. To strengthen security measures governing personal data entrusted to data processors, we have set out possible regulatory options.*
"*Under such options, a data user who transfers personal data to a data processor for holding, processing or use, would be required to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the personal data, and to ensure that the data are not misused and are deleted when no longer required for processing.*
"*As part of the options, we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted. Recognising that compliance with certain requirements may pose problems for some data processors due to the operational constraints unique to specific industry sectors, we have also included the option of subjecting different categories of data processors to different obligations.*"

8. (a) The reason why the PDPO (by virtue of s 2(12)) does not impose obligations on persons who hold, process or use personal data solely on behalf of other persons and not for their own purposes is that many such persons have no knowledge of whether or not the data they hold, process or use are personal data and/or have little or no control over the processing of the data other than at the highest level. Operators of webmail services or social networking websites are two examples. On the other hand, there are data processors of the out-source and other types who are entrusted to carry out data processing with respect to data they know to be personal data (such as customer records) and which have full control over the processing of such data (within the terms of their contracts with the parties entrusting the data to them).

(b) Data processors of the former type are not in a position to ensure compliance with the requirements of the PDPO. Nor are their "users" generally in a position to require

them to do so. Accordingly, data processors of the former type should continue to be excluded from direct regulation under the PDPO and their "users" should not be made subject to any requirement to ensure they comply with the PDPO. For such data processors, it is sufficient that the "users" are themselves subject to the PDPO.

(c) There is no good reason why data processors of the latter type (i.e. out-source data processors and the like) should not be made subject to direct regulation under the PDPO subject to a satisfactory definition of what constitutes such a data processor.

(d) The proposal that a data user be required to use contractual or other measures to secure compliance with relevant obligations of the PDPO when contracting out the processing of personal data to third parties is *not* supported as an alternative to direct regulation (but is supported in conjunction with direct regulation). Given the doctrine of privity of contract, a data subject would not be able to enforce such a requirement; nor would a data subject have any remedy for its breach as against the data processor but may have a remedy against the principal via ss 65 and 66 of the PDPO.

Proposal No. 3: Personal Data Security Breach Notification

§13: "*Following the spate of personal data leakage incidents, questions have been raised on whether a personal data security breach notification ("privacy breach notification") system should be instituted to require data users to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data so as to mitigate the potential damage to affected individuals. A mandatory notification requirement could impose undue burden on business operations. Bearing in mind that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we consider it more prudent to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community. For this purpose, the PCPD can issue guidelines on voluntary privacy breach notifications.*"

9. Given the extent and size of the known data leakage incidents that have occurred in the last few years in Hong Kong, this problem is of sufficient seriousness to be

addressed by appropriate measures. A voluntary breach notification system under a framework provided by guidelines issued by the PCPD is a positive first step to take.

Enforcement Powers of the PCPD

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

§14. "*At present criminal investigations are conducted by the Police and prosecutions by the Department of Justice. We have considered if these powers should be conferred on the PCPD. Since some offences proposed in this review are not technical in nature and involve a fine and imprisonment, there could be concern if such powers are delegated to the PCPD. Moreover the existing arrangements have worked well. We do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases.*"

10. (a) There is no good reason for granting the PCPD criminal investigation and prosecution powers.

(b) The lack of such powers may mean that in some cases 6 months will have elapsed before a complaint case has been considered for referral to the police for criminal investigation or to the Secretary for Justice for possible prosecution, thereby rendering any prosecution time-barred. This problem is best addressed by extending the time within which prosecutions under the PCPO may be brought (as proposed in proposal 40) rather than by granting criminal investigation and prosecution powers to the PCPD.

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

§15: "*Under Section 66 of the Ordinance, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user. The PDPO does not empower the PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings. To achieve greater deterrent effect on acts or practices which intrude into personal data privacy and enhance the overall effectiveness of sanctions provided for under the PDPO, views are invited on whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject.*"

11. (a) Compared with the position with respect to the anti-discrimination ordinances, there has been a marked lack of claims for compensation for breaches of the PDPO. In fact, the Bar Association is aware of only one that has gone to trial and that claim was misconceived (Kwan Chi Shan v Yeung Yin Fong (關子山訴楊燕芳) (unreported, 4 December 1997, DCCJ 7812 of 1997)).

(b) One reason for the lack of such cases may be the fact that breaches of the PDPO are generally less likely to result in claims for substantial damages than in the case of breaches of the anti-discrimination ordinances, which often involve substantial claims for loss of income.

(c) Undoubtedly, however, the fact that the EOC has an express mandate to assist claimants making claims for breaches of the anti-discrimination ordinances has resulted in the development of the jurisprudence on the meaning and effect of those ordinances and encouraged claimants to bring cases without such assistance.

(d) In order to achieve a similar result, the proposal to empower the PCPD to provide legal assistance to claimants under s 66 of the PDPO along the lines of the EOC model is supported.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

§16. *"We have considered whether the PCPD should be empowered to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement by a data user, as an alternative to the existing redress avenue to seek compensation through the court as provided for under Section 66 of the PDPO. The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC") Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1994. The LRC opined that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the Data Protection Principles ("DPPs"). It would be for a court to determine the appropriate amount of compensation payable. Views are invited on*

whether it is appropriate to introduce an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects."

12. (a) The reasons for the LRC's objection to granting the PCPD the power to award compensation still hold good.

(b) Two of the main reasons why claimants do not seek or obtain compensation for breaches of the PDPO at present are an under-developed jurisprudence on the meaning and effect of the PDPO (particularly in relation to claims for compensation) and the costs-risk for the "sandwich class" (in theory legal aid is available to claimants who pass the means and merits tests). Mandating the PCPD to assist claimants (see response to proposal 5 above) should go some way to addressing these obstacles to compensation claims under the PDPO.

(c) The proposal is accordingly not supported.

(d) As an alternative avenue for claimants to receive financial recompense for claimed breaches of the PDPO it is proposed that the PCPD be mandated (by amendment to the PDPO) to offer complainants and parties complained against the option of mediation in complaint cases he has decided to investigate (before commencing his investigation).

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

§§17&18: *"The PCPD is empowered to remedy contravention of a DPP by issuing an enforcement notice to direct the data user to take remedial steps. Contravention of the enforcement notice is an offence ... One option is to consider making contravention of a DPP an offence. Bearing in mind that DPPs are couched in generic terms and can be subject to a wide range of interpretations, to make contravention of a DPP a criminal offence would have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether we should make contravention of a DPP an offence."*

13. The DPPs are not precise enough to allow for sufficient certainty as to what they prohibit or permit in order to found a criminal offence. This is why breach of the DPPs was expressly excluded from the general offence provision of the PDPO (s 64(10) refers). The Proposal is accordingly not supported.

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

§19: "*Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. To curb irresponsible dissemination of leaked personal data, we may consider making it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.*"

14. (a) The Proposal is supported.

(b) Any such offence should include an express *mens rea* element, e.g. obtaining or procuring the obtaining of personal data and disclosing the data with the intention of making a profit thereby and/or to cause harm to a subject of the data *knowing* the data user that is the source of the data has not given consent to their disclosure or being *reckless* as to whether such consent has been given or not.

(c) The appropriate level of penalty should be in line with the more serious offences provided for in s 64 of the PDPO which carry maximum penalties of a fine at level 3 and imprisonment for 6 months.

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

§20: "*Under the PDPO, if a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently does the same act or engages in the same practice, the PCPD would issue another enforcement notice. Since the enactment of the PDPO, PCPD has not come across any such case of circumvention. To forestall possible circumvention of the regulatory regime, one option is to consider making it an offence if a data user repeats such contravening act. However, this would be*

moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether this is appropriate."

15. (a) It is not accepted that the proposal and the "*original intent of adopting the DPPs in the PDPO*" are in some way incompatible.

(b) Breach of the DPPs was not made an offence because the DPPs are too imprecise to afford reasonable certainty as to compliance for the purpose of imposing criminal sanctions. An enforcement notice issued by the PCPD, on the other hand, should state with particularity what a data user is required to do in order to comply with whatever DPP is in issue. (If the enforcement notice does not do this, it would be liable to be set aside on appeal to the Administrative Appeals Board.) Accordingly, the proposed new offence should not place data users in jeopardy of unwitting contravention unlike the position that would pertain if breach of the DPPs *simpliciter* was made an offence.

(c) The Proposal is accordingly supported.

(d) The penalty should be less than for a breach of an enforcement notice (fine at level 5 and imprisonment for 2 years: s 64(7) of the PDPO refers) because there would be no element of directly flouting a requirement imposed by the PCPD. On the other hand, the penalty should be greater than that for the general offence provision (fine at level 3: s 64(10) of the PDPO refers). The Bar Association proposes a penalty of a fine at level 5.

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

§21: "*We have considered the option of empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. It is not common for non-judicial bodies to have the statutory power to impose monetary penalties. Under the PDPO, the DPPs are couched in generic terms and can be subject to wide interpretations. Although we may require the PCPD to issue guidance on the circumstances he considers appropriate to issue a monetary penalty notice, whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. Views are invited on whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.*"

16. (a) For the reasons given in §§6.19 and 6.20 of the Consultation Document the proposal is not supported.

(b) The Bar Association is of the additional view that the imposition of a monetary penalty is a fine by another name. For the same reason that a breach of the DPP should not carry a criminal sanction (including a fine) so too should this not expose someone to a "monetary penalty". Adding the subjective element of "serious" does not make the risk of unwitting non-compliance any less.

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

§22: "*The PDPO does not provide for heavier sanction for data users who repeatedly contravene an enforcement notice. Since the enactment of the PDPO, there has not been a problem with repeated offenders. We have considered the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect. Views are invited on whether there is a need to impose a heavier penalty for such repeated offenders.*"

17. (a) The penalty for contravention of an enforcement notice is a fine at level 5 ($50,000) and to imprisonment for 2 years: s 64(7) of the PDPO refers. In line with usual sentencing principles, if someone is proved to have contravened an enforcement notice more than once, this should (all other things being equal) result in a heavier penalty up to the maximum than would be imposed on someone who has done so only once.

(b) In any event, the lack of any incident of repeat contravention of an enforcement notice suggests that the deterrent effect of a higher maximum penalty in such a case (than is currently provided for in s 64(7)) is unnecessary.

(c) The Proposal is accordingly not supported.

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

§23: *"Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of a fine at Level 3 (up to $10,000) may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. To curb misuse of personal data in direct marketing activities, we may consider raising the penalty level for misuse of personal data in direct marketing. Public views are invited on the appropriate level of penalty."*

18. The Proposal to raise the penalty (for contravention of s 34 of the PDPO) is supported.

(b) The Bar Association proposes that the penalty be increased to a fine at level 5 ($50,000).

Proposals not contained in the Consultation Document

To relieve data users from the obligation to redact the name or other information explicitly identifying another individual as the source of personal data that are the subject of a data access request when complying with the request if it is reasonable in all the circumstances for the data user to believe the requestor knows who the source is or would be able to infer this from a copy of the data from which the name or other information explicitly identifying the source have been redacted.

19. (a) Pursuant to s 20(1)(b) of the PDPO a data user *must* refuse to comply with a data access request if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the other individual consents to such disclosure.

(b) The refusal obligation of s 20(1)(b) is subject to s 20(2) of the PDPO. There are two parts to s 20(2). The first part, s 20(2)(a), provides that where the "other individual" (as referred to in s 20(1)(b)) is the source of the personal data that has been requested, s 20(1)(b) shall not operate unless that other individual is *named* or *explicitly identified.* The second part of s 20(2), s 20(2)(b), provides that s 20(1)(b) shall not operate if the data user can comply with the data access request without disclosing the identity of the other individual by the omission of names, or other identifying particulars, or otherwise.

(c) The combined effect of ss 20(1)(b) and 20(2) is to require a data user to redact copies of personal data provided in compliance with a data access request in order to remove data that identify any other individual. In the case of an individual who is the source of the requested data, the requirement is met if the *name* or *other information explicitly identifying* the individual is redacted. In relation to any other individual it is necessary to remove all information that would identify him: see generally *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450.

(d) In practice, compliance with this redaction requirement can be extremely onerous for a data user because each document containing personal data within the scope of the request must be reviewed for any references to any other individuals. Where a document contains such a reference, a decision must be taken as to what (if anything) must be redacted in order to comply with ss 20(1)(b) and 20(2) of the PDPO. This is often not obvious. Nor can this redaction obligation be taken lightly because non-compliance without reasonable excuse is an offence (s 64(10)).

(e) It is certainly accepted that the redaction requirement is necessary to protect the privacy of other individuals referred to in documents containing personal data that are the subject of an data access request. However, in the case of an individual who is the source of the requested personal data, redaction is often unnecessary because the requestor knows who the source of the data is or can infer this from the data remaining after the source's name or other information *explicitly identifying* him has been removed. For example, where a data access request is made to personal data in an employment performance appraisal, the data user is required to remove the name and title of the appraiser in order to comply with ss 20(1)(b) and 20(2). However, the requestor will usually either remember who the appraiser was or will be able to infer this from the period to which the appraisal relates. As a result, the redaction (in such a case) serves no meaningful purpose.

(f) In order to relieve part of the burden of the redaction obligation on data users in complying with data access requests, therefore, it is proposed that the PDPO be amended such that this obligation does not apply where the other individual referred to in the requested data is the source of the data and it is reasonable in all the circumstances for the data user to believe the requestor knows who the source is or would be able to infer this from a copy of the data from which the name or other information explicitly identifying the source have been redacted.

To publish or otherwise make available to the public and the legal profession all decisions of the Administrative Appeals Board on appeal from a decision of the PCPD.

20. (a) Judgments on the interpretation of the PDPO are few and far between. Apart from the single case of a claim for monetary compensation, there are only a handful of judgments from applications for judicial review of decisions of the PCPD. The vast majority of cases of persons aggrieved by the decisions of the PCPD are determined by administrative appeal to the Administrative Appeals Board which does not publish its decisions. A valuable source of jurisprudence is closed to the legal profession and appropriate advice cannot be given to lay clients. The summaries of selected Administrative Appeals Board decision are not adequate for the purpose giving appropriate advice since it is often necessary to consider the relevant decision in context with appreciation of the full submissions and reasoning.

(b) The Bar Association proposes that all decisions of the Administrative Appeals Board to date on an appeal from a decision of the PCPD be published or made available online.

Dated this 16th day of November, 2009
Hong Kong Bar Association