HONG KONG INTERNET SERVICE PROVIDERS ASSOCIATION

CODE OF PRACTICE FOR RELEASE OF INFORMATION

Draft Version 0.9

27 Aug 2015

www.hkispa.org.hk

Gratitude to Squire Patton Boggs for preparing this documentation

1. BACKGROUND AND OBJECTIVE OF THIS CODE

1.1 Hong Kong Internet Service Providers Association ("**HKISPA**"), Hong Kong Customs and Excise Department ("**Customs**") and Hong Kong Police Force ("**Police**") recognise a commonality of interest between industry and government in prevention, detection and investigation of criminal activity whilst balancing the rights and privacy of individuals.

1.2 Safety, security and reliability of the Internet are dependent upon early detection of criminal activity that might undermine achievement of these objectives. However, this requires a balancing of such fundamental rights as the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.

1.3 To address the legitimate rights and expectations of law abiding citizens to the protection of their personal information, HKISPA together with input from Customs and the Police has developed this Code. This Code endeavours to set clear procedures for cooperation between ISPs, Customs and the Police in an effort to balance the interest of the parties involved.

2. CONTRACTUAL OBLIGATION TO KEEP INFORMATION CONFIDENTIAL

2.1 ISPs would often have contractual obligations to keep information confidential and not to release such information to any third parties except in certain circumstances such as disclosures made pursuant to a court order or a request for governmental authorities.

2.2 ISPs should bear in mind that unless disclosures are permitted under the relevant contract, it is likely a breach of contract even if the request was made by governmental authorities such as Customs and the Police, especially if such request are not legally binding on the ISPs. In such case, unauthorized disclosures may subject the ISP to liability towards its customers.

2.3 Moreover, some contracts would require the ISP to notify the intended disclosure to the relevant customer prior to the disclosure. These are important obligations that must be complied with unless restricted by legislations such as legislations that prevent the act of "tipping off".

2.4 In light of the above, prior to any disclosure, ISPs should ensure that such disclosures are permitted under the relevant contract.

3. PERSONAL DATA (PRIVACY) ORDINANCE

3.1 Even if ISPs are not contractually bound to keep information confidential, ISPs should take note that the Personal Data (Privacy) Ordinance ("**Ordinance**") may be applicable to the intended disclosure if the data concerned constitutes "Personal Data".

3.2 Pursuant to Section 2 of the Ordinance, "Personal Data" means any data:

3.2.1 relating directly or indirectly to a living individual;

3.2.2 from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

3.2.3 in a form in which access to or processing of the data is practicable.

3.3 It is important to note that "Personal Data" only covers data relating to a living individual. Therefore, corporate information such as contact details of staff and clients which constitute personal data of the relevant individuals will be covered under the Ordinance.

3.4 Pursuant to the Data Protection Principle ("DPP") 3 of the Ordinance, ISPs shall not, without the prescribed consent of the data subject, disclose the personal data of the data subject for a purpose unrelated to the original purpose of collection. The Ordinance contains certain exemption provisions, including section 58(2). If the exemption provision is applicable, the data will be exempted from the relevant requirement of the Ordinance, and a data user who discloses the personal data to a third party under such circumstances should not constitute a contravention of DPP3.

3.5 There is no provision in the Ordinance compelling ISPs to disclose the personal data of a data subject to a third party. Whether ISPs may rely on the exemption under section 58(2) of the Ordinance to disclose the data is for the ISP to decide. If the ISP decides to disclose the data by relying on the exemption provisions of the Ordinance, it will have to bear the risk of contravening the Ordinance in the event that it is adjudged that the data are not exempted. Under the Ordinance, ISPs has no duty and cannot be compelled to rely on the exemption provisions to disclose others' personal data.

3.6 If ISPs wish to rely on section 58(2) of the Ordinance in disclosing the personal data of a data subject to Customs and/or the Police, it must fulfil two major conditions:

3.6.1 the data are to be used for a purpose specified in section 58(1) of the Ordinance, e.g. detection of crime, prevention of unlawful or seriously improper conduct or dishonesty, etc; and

3.6.2 the application of DPP3 to such use would be likely to prejudice any of those purposes.

3.7 Even if the data fulfil the first condition, the ISP still has to consider the second condition. According to the Administrative Appeals Board's decision in Administrative Appeal No. 5 of 2006, whether or not the relevant purposes would likely be prejudiced does not depend upon the subjective belief of the data user, but an objective inference. ISPs must be prudent and should not hastily conclude that section 58(2) of the Ordinance is applicable by merely relying on general allegations made by data requestors; otherwise the requirements of DPP3 may be contravened.

3.8 A third party who requests for personal data of a data subject from a data user should provide sufficient information to the data user, including the purpose of requesting for the data (e.g. which kind of unlawful conduct he is trying to prevent?), on how the application of DPP3 to the disclosure of the data would likely prejudice the purposes, etc., so that the data user can consider whether section 58(2) of the Ordinance is applicable. On the other hand, if the ISP considers the information

inadequate, it should ask for explanation and provision of more information from the requestor. ISPs shall not hastily disclose the personal data of the data subject by just relying on the words of or general allegation made by the requestor.

3.9 Even if the data are intended to be used for prevention of crime or seriously improper conduct, disclosure of the data on a ground that is not substantiated by evidence may have serious harm on the data subject's data privacy. Therefore, ISPs may disclose the data to the third party only upon sufficient information to satisfy himself that the data are exempted.

4. REQUEST FORM FOR RELEASE OF INFORMATION

4.1 To standardize the manner in which Customs and/or the Police may request ISPs to provide information, HKISPA has prepared a standard form as annexed as ***Schedule 1*** that Customs and the Police have agreed to use when requesting information from ISPs.

4.2 An ISP is not legally required to comply with any request merely because Customs and/or the Police have completed the standard request form, especially if the request is not made pursuant to a court order or warrant.

4.3 ISPs are requested to exercise their own care and diligence in considering whether to comply with a request to ensure that it does not become liable in any manner by complying with a request. If in doubt, ISPs should seek legal advice immediately upon receiving a request. In most circumstances, Customs and the Police would wait for your lawyer to arrive at the scene even if there is a court order or warrant.

5. MINIMAL DISRUPTION TO ISPS

5.1 If ISPs decide to comply with a request, Customs and the Police have kindly agreed that, where possible, they can make a mirror copy of the data instead of physically removing the hardware and servers from the data centre of the ISPs so as to cause minimal disruption to the daily operations of the ISPs.

5.2 In such cases, it is likely that the officer from Customs and/or the Police would have to be in-charge and at least oversee the copying processing so as to maintain the "chain of evidence" so that the evidence can be used in court. As this copying process may take significant time, ISPs may have to provide manpower to support Customs and/or the Police in such operations.

Schedule 1

Date of Request: _____

Full Name of ISP: _____ ("**ISP**")

Requesting Party's Details

Full Name of Government Authority: _____ ("**Authority**")

Full Name of Requesting Officer: _____

Rank of Requesting Officer: _____
(Rank must be "Senior Officer" or above)

Telephone Number: _____

Fax Number: _____

Reference No.: _____

Information Requested

Please state clearly the details of the information requested:
(If necessary, please attach additional pages)

_____

_____

_____

Is the request made pursuant to a Court Order or Warrant: Yes / No*
(If yes, please enclose a copy of the Court Order or Warrant)

If the request is not made pursuant to a Court Order or Warrant, please answer Questions 1-6.

1. Please confirm if the requested data will be used for one of the purposes stated in section 58(1) of the Personal Data (Privacy) Ordinance, and that not disclosing the data will likely prejudice the purposes.

☐ **Yes** ☐ **No**

2. If you answer to question 1 is "Yes", please specify:

(a) the particular purpose under section 58(1) for which the data to be used.

_____

_____

_____

(b) the nature of the conduct involved.

_____

_____

_____

(c) how the said purpose would likely be prejudiced by the application DPP3 (i.e. obtaining the prescribed consent of the data subject for release of the data).

_____

_____

_____

3. Please state clearly any other legal basis for the request citing the relevant sections of the legislation and which kind of unlawful conduct is the Authority trying to prevent:
(If necessary, please attach additional pages)

_____

_____

_____

4. Please confirm if the data owner should be made aware of the act of this request.

☐ **Yes.** Please state the time when the data owner should be made aware of this request: _____

☐ **No.** Please state reason why the data owner should not be made aware of this request:

_____

_____

5. Please confirm that the present request is made because the Authority has no feasible alternative and this is the only way to obtain the data required for the purposes specified in section 58(1) of the Personal Data (Privacy) Ordinance.

☐ **Yes** ☐ **No**

6. Please confirm if the Authority will indemnify the ISP for complying with this request.

☐ **Yes.** The Authority confirms that it shall fully indemnify the ISP, to the extent permissible by law, for any loss and damage suffered by the ISP from any claim or law suit in connection with or arising from complying with this request.

☐ **No.** The Authority confirms that the ISP may refuse to provide the data requested. If the ISP complies with the Authority's request and releases the requested data, it shall bear on its own all the associated legal risk and cost consequences.

Note to ISPs: Regardless of Yes or No to Question 6 above, you have the right to refuse providing the data unless the request is pursuant to a Court Order or Warrant. However, if

Schedule 1

the answer to Question 6 is No or the answer is left blank, you are advised to carefully consider the legal risk associated with releasing the data.

By making this request, the Authority hereby confirms that this request is a lawful request and in the Authority's opinion, the ISP will not be held liable in any manner for complying with this request.

_____ _____

Signature of Requesting Officer Date

** Please delete as appropriate*