July 20, 2015

Mr. Allan Chiang
Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data
12/F, Sunlight Tower
248 Queen's Road East, Wan Chai
Hong Kong

Dear Mr. Chiang,

The Asia Internet Coalition (AIC) welcomes this opportunity to comment on the Guidance on Personal Data Protection in Cross-border Data Transfer.

The Asia Internet Coalition is a policy voice of the digital industry in the Asia-Pacific. Our industry is proud to provide inspiring and compelling content, platforms and applications that deliver significant economic, social and cultural benefits to the region.

Our aim is to ensure that the Asian policy and regulatory landscape allows users to enjoy the maximum economic, social and cultural benefits from the online world in the years ahead and ensure that they can do this safely, securely and confidently.

I. General Comments

We welcome the opportunity to first provide some broad comments around this Guidance. We respect the leadership role that Hong Kong has played in the region by developing and enforcing a strong privacy framework which protects individuals' privacy while permitting innovative business practices to flourish. It is with this leadership position in mind that we respectfully propose that the Privacy Commissioner for Personal Data (PCPD) consider evaluating data transfers through a risk-based lens that will stimulate innovation and commerce while protecting data from situations where actual risk occurs. The economic benefits of cross border data flows are significant. Access to foreign markets through trade liberalization and globalized supply chains are the major sources of growth, jobs and new investments – particularly in developing economies.

We note that Section 33 of the Personal Data (Privacy) Ordinance (the "PDPO" or "Ordinance"), upon which this Guidance is based, was included in the PDPO at the time of its enactment in 1995. Since then, however, it has not been brought into force through either discussions in the Legislative Council or specific proposals to practically implement Section 33. In March of last year, the Panel on Constitutional Affairs did have some conversations about its implementation but we have not heard of any developments since then. As a result, the very issuance of this Guidance

comes as unexpected to the AIC, given that it is meant to govern the implementation of a provision that currently seems to be inactive.

Secondly, the Guidance provides no direction on how this will affect personal data transfers from Hong Kong taking place before Section 33 is actually implemented, leading to a potential time period of uncertainty for businesses about whether they are in compliance with the Guidance and Section 33. More clarification on this would be very welcome.

Finally, the unexpected issuance of this Guidance is also of concern to the AIC. To the best of our knowledge, there was no public consultation or opinions sought before the Guidance was published, nor any expert third parties consulted on this issue. We urge the Commission to consider the potential unintended consequences such a rushed Guidance might have on Hong Kong's functioning as a world-class hub of business activity in the Asia-Pacific region, as well as the precedent it may set in the region. Hong Kong businesses may find themselves subject to similar or more stringent rules established by neighboring countries, which may have an adverse economic impact to Hong Kong industry.

Given today's globally interconnected economy, inadequately designed national policies that increase data processing costs have a severe economic impact as many sectors of the economy rely on digitally supplied services and goods. When data must be confined within a country, it does not merely affect social networks and email services, but potentially any business that uses the internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes.

Scope of Application

For the sake of clarity, we recommend that the Guidance specify that Section 33 applies to data users based in Hong Kong that transfer personal data outside of Hong Kong.

Nature of "Transfers" that are Covered by Section 33

The standard for defining "Transfers" seems overly broad and overreaching, from our initial assessment of the Guidance.

Transmission to third party processors
We note the case listed in the Guidance, in which a third party outside of Hong Kong processes personal data for a data user, storing data somewhere in the world, would be subject to Section 33. This example seems to be too broad and applies an expanded definition of Section 33 to data transfers from Hong Kong. Data users are already required to adhere to Hong Kong's Six Data Protection Principles under the PDPO and ensure that their service provider (the third party in this example) also follows the principles. As a result, imposing yet another layer of regulation does not seem to ensure any additional level of security while placing an additional compliance requirement on companies.

Cloud services
We are similarly concerned by the cloud services example listed in the Guidance Note. Given Hong Kong's position as a regional and international hub of commerce, the Guidance would unfairly penalize the many international businesses and employees based in Hong Kong, where the businesses qualify as data users under the PDPO.

Interoperability
We would seek additional clarification of this Guidance in the context of Hong Kong's international commitments and discussions. The Cross Border Privacy Rules (CBPR) established by APEC and the Privacy Recognition for Processors system provide a structure within which data can be transferred in APEC countries. The Guidance does not appear to permit a "safe harbor" where compliance with the APEC CBPR would satisfy the requirements of Section 33. We would appreciate clarification as to how the two will work together.

Exemption for web caching
It is unclear from this Guidance whether Section 33 would apply in relation to personal data sent to, and stored in, a web cache abroad. Web caching is used to enhance the speed and efficiency of displaying information to end users, but is not, alone, considered a permanent storage mechanism. For example, if the data is sent to, and stored in, a web cache abroad, but comes straight back to Hong Kong (e.g. the data leaves and comes back to Hong Kong during which the data is transmitted via a server situated outside of Hong Kong due to normal Internet routing), this ought not to be considered a transfer of data. Similarly, if the data is sent to, and stored in, a web cache abroad, and remains abroad, this should not be considered a transfer of data. It would be helpful to get clarification on this definition.

II. Specific Clauses

We understand that the purpose of the Guidance is to assist in preparation for implementation of Section 33 of the Ordinance. As such, we have only commented on the Guidance and the proposed model contract clauses (MMCs) and not Section 33 generally as this is already established. We have set out our concerns with the guidance and requests for clarification below:

1. **"Storing personal data in the cloud may also constitute a transfer outside Hong Kong if the cloud server is accessible outside Hong Kong."**

We suggest adding a qualification explaining that this will not be applicable "if practical steps have been undertaken to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use and other exceptions are met."

2. **"For example, when a telecommunication service provider transmits personal data for other data users, it is not required to observe section 33 in relation to the data it transmitted."**

It would be worthwhile clarifying by way of example that entities who transfer data in the context of providing infrastructure/storage services to a data user are also exempt – not just telecommunication service providers.

3. **"A list of jurisdictions, which the Commissioner determines to have in force 'any law which is substantially similar to, or serves the same purposes as' the Ordinance, will be specified by notice in the Gazette by the Commissioner (the 'White List') under section 33(3)."**

While this would allow data users to carry out their own assessments and deem a country adequate, it is only available for countries which the Commissioner's office has not yet assessed. The Guidance states that it has reviewed 50 countries for the purposes of its "White List" of

adequate countries but we are unable to find a public link to this list. We would therefore request to understand which countries have already been reviewed. It would also be helpful to understand how long the assessment of a country would remain valid, as regions may adopt privacy laws subsequent to a review by the Commissioner.

We are currently seeing tremendous pace of change in data privacy regulation across the Asia region and in the world more generally. The assessments made in the preparation of the White List, which we understand was compiled in 2012-2013, will already be out of date given recent enactments in places as close as China, Singapore and Malaysia. For this reason, a detailed understanding of the criteria applied to adequacy determinations under subsection 33(3) would be essential for data users' understanding of the law.

4. Section 33(2)(c) data subject's consent in writing to the transfer

Consent must be in writing, which is an impractical burden on technology companies. The Guidance is effectively requesting an additional tick box every time a user's data is transferred, which is onerous without providing a clear benefit to the user. We are concerned about consent fatigue and have looked at usability research confirming that too many consent dialogues and tick boxes degrade users' ability to understand and appreciate the terms to which they are consenting. Additionally, it would be helpful to get the PCPD's written clarification that there is no obligation to provide the service to the data subject where he/she declines consent.

Many businesses operating in Hong Kong are part of larger international groups of companies that seek to integrate PDPO compliance measures with global data subject consent mechanisms. We believe that this approach would make Hong Kong compliance impractical, without it being clear how a separate consent for international transfers would improve the position for data subjects.

Many multinational companies explain in their privacy policies (to which users agree when they register for the service) that they will transfer users' personal data to a number of foreign jurisdictions for a variety of purposes, including processing and storage, in order to fulfill the very services the users have requested. Thus, users are on notice from the time they register for the service that their data will be transferred globally, and provide their consent to these transfers. This additional requirement to notify and obtain consent from users will be onerous to both users and companies, and will not provide users with additional meaningful information regarding the use and transfer of their personal information. We strongly urge that the Guidance regarding this subsection be expanded to account for users' consent provided at the time of registration for services to bring this into line with existing international standards.

5. The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

The Guidance states that the data user can use the standard Model Contract Clauses or carry-out due diligence and adopt non-contractual mechanisms to ensure compliance (i.e. monitoring and auditing) with the Ordinance.

It is not clear whether or not this due diligence exemption applies to transfers to data users (i.e. controllers) only or also agents (i.e. processors). This confusion arises by virtue of the statement: "the transferees outside Hong Kong are required to observe the requirements under DPP2 to DPP6". Only data users are required to comply with such requirements in the DPP so it may be implicit that transfers to data processors are not permitted on this ground. We would appreciate clarification on this point.

6. "Section 33(2)(e) exemptions under Part VIII of the Ordinance…

A. Section 61 (news): the transfer of personal data by a person to a data user whose business consists of a news activity and there is reasonable ground for that person to believe that the publication or broadcasting of the personal data is in the public interest"

We would like to understand whether this exemption would extend to search engines or computer-generated news sites that aggregate headlines from news sources worldwide, as well as other platforms that host news content.

B. Section 62 (statistics and research): where personal data is transferred for preparing statistics or carrying out research and the resulting statistics or research does not identify the data subjects

Clarifications are needed to define the scope and purpose of "statistics" and "research".

7. "The recommended model clauses for the purpose of satisfying the due diligence requirement under Section 33 (2)(F)"

It appears that the Recommended Model Clauses are intended to cover transfers to agents (i.e. processors); we would appreciate your clarification on whether this is the case. If so, many of the provisions are not suitable for this arrangement so a separate set of clauses for transfers to processors should be created. If the clauses are intended to cover transfers to processors, the provisions appear unrealistic.

e.g. clause 3 seeks to make the parties jointly and severally liable for breaches; yet making data users liable for unlawful processing would appear to go beyond the scope of the Ordinance.

In addition, many multinational corporations already maintain thousands of negotiated contracts with third party service providers and other processors, which require processors to abide by the rules of the jurisdictions in which they operate. To require data users to update thousands of contracts – and particularly to require specific reference to the PDPO principles – would be impractical and onerous. More importantly, doing so would not necessarily provide enhanced protection to user data where the data is already protected through functionally equivalent, albeit non-specific, contractual provisions. We encourage the Commission to consider expanding the scope of accepted contractual provisions to include contracts that already constitute the functional equivalent of the PDPO data protection principles. Because these principles are already in line with internationally-accepted data protection principles, many companies would be able to demonstrate functional compliance.

8. **"2.1.1 The Transferee shall process or use the personal data for the purpose(s) as set out in Schedule 1 to this agreement to the exclusion of any other purpose. Where the transferred data is used for a new purpose, the Transferee shall obtain the prescribed consent of the data subject under the Ordinance."**

This is only appropriate for a data user to user transfer and not appropriate to a service provider context.

9. **"The Transferee shall not disclose, transfer or allow access to the personal data to a third party data user or data processor ("Sub-transferee") located outside Hong Kong unless it has notified the Transferor…"**

We would put forward that this be subject to data user's prior consent.

10. **"5.1 Should the Transferee breach any of its obligations under this agreement, the Transferor may, without prejudice to any rights which it may have against the Transferee, terminate this agreement by serving a written notice to the Transferee."**

We recommend that this clause be amended to introduce an element of materiality or the possibility for the breach to be fixed before the termination right is triggered.

III. Additional Suggestions

We would also like to put forward a number of additional suggestions that the Commissioner's office might consider when revising the Guidance document.

Publicly available personal data
Personal data that is publicly available should be subject to less rigorous transfer obligations. We would suggest that data users should be able to transfer such data without restriction. Personal data that is already in the public domain is at no greater risk when it is transferred than when it is available publicly in Hong Kong.

Fulfillment of contract between the data user and individual
Data transfer laws around the world permit international data transfers where the transfer is effectuated to fulfill a contract between the data user and the individual. Such a transfer is consistent with the individual's expectations that the data user will use reasonable means to execute the contract. The Guidance should also permit a transfer at the individual's request with a view to his entering a contract with the data user.

Fulfillment of contract between data user and third party
The Guidance should permit transfers where the transfer is necessary for the conclusion or performance of a contract between the organization and a third party which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest.

IV. Conclusion

The AIC appreciates the PCPD's consideration of our observations. We understand that preparatory work is underway to ensure that the conditions necessary for implementing the

provision are in place, and encourage you to consider the AIC as a resource during this process. We are available to share private sector perspectives on the potential implications of the Guidance on protection of individuals' data, business, and innovation and would welcome further discussion of these issues with the PCPD.

Should you have any questions please do not hesitate to contact our representative based in Singapore, Ms. Clara Koh (Phone: +65 6471 5269, Mobile: +65 9228 1093, Email: clara@vrienspartners.com).

The member companies of the Asia Internet Coalition (AIC) remain at your disposal to discuss the matters above in more detail.

Kind regards,

Hans Vriens
Secretariat
Asia Internet Coalition