To

Mr Stephen Kai-yi WONG
Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong

Mr. Patrick Nip
Secretary for Constitutional and Mainland Affairs, Government of Hong Kong

Hon CHEUNG Kwok-kwan, Chairman
Legislative Council Panel on Constitutional Affairs, Hong Kong

Subject: AIC Submission on the Review of the Personal Data (Privacy) Ordinance (PDPO)

Dear Mr Stephen Kai-yi WONG,

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Legislative Council Panel on Constitutional Affairs for allowing the AIC to submit comments on the **Review of the Personal Data (Privacy) Ordinance (PDPO).** As an introduction, AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com. In the past AIC has submitted several policy positions to the key agencies in the Government and can be accessed here. In these unprecedented times we also commend Hong Kong government efforts in fighting the COVID-19 pandemic and express our solidarity with the government's efforts.

First and foremost, we commend the Hong Kong Government for proposing reforms to the PDPO. It's becoming an everyday occurrence to see news articles on personal data protection due to an increased global conversation on privacy legislation. As technological advancements continue to evolve and become more sophisticated so do the choices individuals face when it comes to managing their data privacy. Therefore, it is critical to protect individual data particularly when economies and companies become more digital in nature. Given this, we understand the government's motivation and believe that this is a timely initiative to introduce reforms to the PDPO.

As responsible stakeholders in this policy formulation process, we appreciate the opportunity to submit our views on the proposed legislative amendments. **As such, please find appended to this letter, detailed comments and recommendations which we would like to respectfully request you to consider when reviewing the PDPO.**

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue for the advancement of data protection framework in Hong Kong.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)
Jeff@aicasia.org
www.aicasia.org

Comments and Recommendations

1. Introduction of a mandatory breach notification mechanism

It is proposed that the roles of data controllers and data processors be differentiated and clearly stated in the mechanism. It is proposed that the mechanism should include:

a. Definition of "personal data breach" along the lines of the GDPR definition, being "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed";

Recommendation: The definition of "personal data breach" should be limited to breaches involving specific types of data that inherently pose a risk to users if subject to breach only (e.g. credit card info, residential addresses), and not other types of data (e.g. ad interests, IP addresses).

b. A notification threshold so the mechanism will only apply to data breaches that have a "real risk of significant harm" taking into account factors such as the type and amount of data leaked and the security level of the data (encrypted or not);

Recommendation: Considering the PCPD proposed a threshold that is data breach having "a real risk of significant harm" we suggest the following:

- We support the anchoring threshold of "that breaches which have a real risk of significant harm" as this is aligned with many other mandatory data breach notification regimes.
- A materiality, harms-based threshold ensures that regulators have visibility into actual risk posed to users, and allows regulators to focus guidance and prioritize oversight into areas most needed.
- A threshold that is too low could result in over-notification to the PCPD and/or individuals. Within the first nine months after the GDPR took effect, 64,684 data breach notifications were made to EU DPAs.[1]
- Should the mandatory data breach regime pass into law, we would welcome written guidance from the PCPD on:
    - How companies should interpret "real risk of significant harm". The threshold for "real risk" could benefit from written guidance such as

[1] https://iapp.org/news/a/edpb-authorities-received-65k-data-breach-notifications-in-first-nine-months-of-gdpr/

that issued by Australia's OAIC, which defines "likely to occur" as being "more probable than not".[2]

- Examples of what significant harm would like
- Counter examples of what would not meet the significant harm criteria, e.g. an email exposing a group of email addresses in the CC line, or an incident involving data which the data subjects have posted publicly or to large groups of individuals online.

Comments on notifying individuals vs PCPD:

- We consider that any legal requirement to notify individuals should focus on the effect of notifications to the individuals impacted.
- Individuals should only be notified if the harm threshold (described above) is met AND, where informing the individual would reasonably likely result in the individuals being able to take action to mitigate any risk of harm caused by the data breach, e.g. changing their passwords.
- In situations where individuals cannot reasonably take any mitigating action, widespread notifications to all 'potentially impacted' individuals could cause unnecessary alarm and panic, and divert attention and resources of the company away from breach remediation at a critical time.

c. A time frame for notifying the breach to the Commissioner and individuals. An example of, "as soon as practicable and, under all circumstances, in not more than five business days" is included in the Paper; and

Recommendation: We seek clarity on the proposed five business days timeframe for giving breach notification and when exactly does it start to run? Does it start to run from the time when a data user completes an investigation and concludes that the data incident meets the reporting threshold? Given this, we are not supportive of prescribing a fixed number of hours or days within which to conduct an investigation into a suspected breach as businesses should be given a reasonable time frame which permits sufficient fact-gathering, investigation and mitigation, which will vary based on the nature, scale and severity of the incident.

Specifically, we consider that the example of five business days is not realistic. In reality, the immediate period after a potential data breach is uncovered is a very fluid period of uncertainty and fact finding. A short timeline like this adds unnecessary pressure to the incident management team and diverts resources from the most important task of containing the incident.

[2] https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

One study cites 66 days as the average time to contain a breach, during which companies are still in the "fog of the breach" and may not have accurate information to share.[3] A legal requirement that forces companies to rush to notify could result in premature information sharing that doesn't reveal the actual root causes of the incidents, and may even perpetuate security risks, if this information is exposed to bad actors.

It is a business reality that many companies of all sizes, big and small, across different sectors process large datasets and offer multiple different products and services. This will affect the time required to accurately investigate a data breach. Other factors which affect this include the size of the company, the number of individuals impacted, and the complexity of the root causes. Furthermore, there are often multiple teams involved in managing a data breach and often a different team handling breach remediation and "reporting the breach". For example, forensic and security teams, product engineers, lawyers, communications, customer service.
A one-size fits all timeline ignores the real complexities which businesses face, and therefore, we recommend a threshold like "as soon as practicable" or "without undue delay". Should PCPD prefer to prescribe a fixed number of days, we propose that the clock should only start after the company has determined that a data breach has occured which meets the notification threshold.

d. Details on the method of notification, as well as the content.

Recommendation: We support a flexible approach to user notification. Businesses should provide notification in a manner which makes sense given how they usually communicate with their users.

2. Certainty around data retention periods

It is proposed that data users will be required to have clear retention policies. The Paper recognizes that it is not practicable to set a uniform retention period applicable to all types of personal data held by various organizations for different purposes. As such, the Paper proposes requiring data users to have in place a clear retention policy that specifies:

a. A maximum retention period for different categories of personal data collected;
b. Legal requirements that may affect the retention periods (for example, tax, employment and medical regulations); and
c. How the retention period will be counted. For example, from the date of collection of personal data, or from the expiry of a data subject's membership with the organization.

[3] Ponemon Institute, 2017 Cost of Data Breach Study

Recommendation:

We agree with the government's view that specifying a fixed retention period for all organisations or all data types is not appropriate. We support mandating transparency and helping individuals be informed about how companies collect and use data, and placing reasonable limitations on retention. However, each company has its own specific business needs and unique operating environment, so a one size fits all retention limitation period would not be practical. Instead, any rules around retention should be principles based and assessed on a standard of reasonableness, considering the original purposes for which the personal data was collected and other legal or business purposes for which companies may need to retain data. We urge the PCPD to introduce a flexible balancing mechanism or exceptions to enable businesses to consider deletion requests against legitimate business purposes for retaining data.

Apart from requiring data users to have a clear retention policy, the law should expressly recognize that personal data may be retained for such periods to comply with any and all laws (e.g. Business records are required to be kept for a period of not less than 7 years after the completion of the transaction by the Inland Revenue Ordinance Cap 112 s512C).

3. Changes to the Commissioner's sanctioning powers

In order to enhance the deterrent effect of the PDPO and strengthen the Commissioner's powers, the following changes are proposed:

a. Increasing the relevant criminal level fines and potentially linking the fines to a percentage of annual turnover and a scale which would have different levels of fines depending on the turnover of the data user;
b. Conferring powers on the Commissioner allowing him to directly impose administrative fines for breaches of the PDPO. Such fines should take into consideration a number of factors including the types of data compromised, severity of the data breach, whether the data user intended the breach to happen and its attitude towards the handling of the breach, remedial actions are taken, track record etc. Data users should have the right to appeal the fines, and be given appropriate time to do so, and
c. A mechanism for the imposition of the administrative fine.

Recommendation:

The level of criminal fines was raised in the 2012 amendment of the PDPO. There is no detail on the proposed level of criminal fines increment. Without such detail, it would be hard to assess the impact of this proposal and whether this imposition of increasingly onerous criminal sanctions would be a disproportionate response to the harm it is seeking to address. We propose that any fines should be proportional to the injury and how the fines are linked to the harm should be clearly articulated.

Further, GDPR-type, turnover-linked fines imposed by the Commissioner lacks due process and transparency. There is no equivalent power for the regulatory authorities for Australia, Canada, New Zealand, and Singapore. It is preferable that the judiciary enforces the law and imposes penalties and we would object to criminal sanctions for data breaches. If the government does wish to introduce administrative fines, it should remove the criminal fines to reduce overlap or, at the very least, limit their application to the most serious and egregious contraventions. The proposal to base the administrative fines on worldwide turnover of a company would have a negative impact on foreign businesses. To the extent that fines are tied to revenue, fines should be a percentage of the domestic, but not global, gross revenue. Also, the fines should not be based on per-instance violations (i.e. per user action, per photo).

4. Regulation of data processors

The purpose of this amendment is to share responsibilities for data protection between data users and processors and prevent data processors from neglecting the importance of preventing personal data leakage. Data processors would be held directly accountable for data retention and security, equal obligations would be imposed on data processors and they would be required to notify the Commissioner and the data user upon becoming aware of a data breach.

Recommendation:

We are supportive of direct regulation of data processors by the PCPD. This would be consistent with international best practices and the global trend to directly regulate data processors. However, we are also of the view that the law should be explicit in the division of obligations between the data user and the data processor, in a manner which reflects the realities of each parties' control over the processing of personal data. Not all the obligations which apply to a data controller should equally apply to a data processor. For example, a cloud provider has control over certain security mechanisms of the infrastructure, but the customer has control over other mechanisms. If there's a data breach, it's important to differentiate which mechanism failed and who has control over such mechanism and the obligations correspondingly assigned.

Data processors should not have obligations to report a breach to a regulator or a data subject directly. All actions should be funneled through the data controller. Not all data processors have insights into a breach. For example, cloud service providers do not monitor the usage/configuration/operation of enterprise customers, and cannot judge what is appropriate / inappropriate access or detect/identify a breach. We propose following the GDPR under which the role of a processor should be to report the breach (if the processor is aware of it) to the data controller and let them proceed with appropriate actions.

5. Regulation of disclosure of personal data of other data subjects

This change is proposed primarily to curb the effect of doxxing of which we have seen an increase recently in Hong Kong. Since 14 June, 2019, the Commissioner has received over 4700 doxxing related complaints and enquiry cases since 14 June, 2019. Proposed measures include conferring statutory powers on the Commissioner allowing a request to remove doxxing content from social media platforms or websites, as well as criminal investigation powers and prosecution.

Recommendation: It is unclear that the PDPO is the appropriate legal instrument for enacting these requirements and there does not seem to have any precedent in overseas data protection legislation.

There are existing legal remedies available to individuals who may have a claim for harassment and established legal process for request for assistance under the PDPO (see section 38 and section 50). It is not clear if there is a necessity for creating an express anti-doxxing provision with criminal sanction in the PDPO given the powers conferred on the PCPD.

The definition of doxxing behavior has to be clarified and it should be clear the harm it seeks to mitigate. We support the requirement that intermediaries have clear policies which seeks to prohibit harmful content on their services but note that any effort to address harmful content should respect freedom of expression and other fundamental human rights. Not all disclosure of information about an individual would be considered to be a privacy contravention. For example, the mere disclosure of a photo online does not meet the definition of "personal data" as it does not identify the person in the photo. Requiring platforms to remove such photos on risk of prosecution would have a chilling effect on speech. Any requirement in relation to content removal and data requests should have clear definitions, take into account international human rights law and right of judicial appeal. We welcome further clarity and discussion on this important issue.