PDPC'S PUBLIC CONSULTATION ON APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Submitted by:
AIG Asia Pacific Insurance Pte. Ltd.

Contact persons:
Priscilla Soh
General Counsel
Priscilla-KT.Soh@aig.com

Lim Bee Lee
Data Protection Officer
Bee-Lee.Lim@aig.com

Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

We agree that the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent. We would like to share some thoughts surrounding this:

- As insurers, we sometimes receive requests from customers to completely withdraw their consent for us to collect, share and disclose their personal data. To accede to such a request would effectively mean that we are not able to administer, process and service their policies, in which case, it may not be possible to continue with the contract of insurance.

Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?

We are of the view that the Notification of Purpose approach should not be subject to conditions. However, if the PDPC chooses to proceed with the conditions, please consider our feedback below.

The conditions should include situations where the organization cannot provide a service if there is no consent. In our context, an example would be when a policyholder wants to withdraw consent totally for collection, use and disclosure of personal data (as opposed to just withdrawing consent to marketing). In such cases, it would be impossible for an insurer to continue with the policy since it will not be able to process, service or administer it.

We have the following queries:

- What constitutes impracticality in the obtaining of consent? Would it include considerations of commercial reasonableness, e.g., a particular mode of obtaining consent may outweigh its benefits in a cost-benefits analysis? Will the PDPC be providing further guidance or examples on this in published guides?

  This is too vague. It may lead to argument between individual and organisation as to why an organisation deems it impractical to obtain consent. Does it mean that an organisation must exhaust all avenues to contact the individual to get his consent before it is considered to be impractical? If such condition is imposed, it will defeat its intent which is to provide an avenue for organisation to use PII without consent for legitimate business purpose.

  Further, it is arguable that it may be impractical to seek consent of individual where data is collected using drones or IOT etc. In such instance, it would not be possible for organisation to determine if the collection would have any adverse impact on the individual and hence, not possible to conduct a DPIA.

  The practical approach to protect individual PII is to ensure that there is no ill intent on the organisation's part in collecting the data and the organisation must have reasonable security measures to protect the PII from data breach.

- What amounts to "adverse impact" on an individual? Would the PDPC be providing any guidance on this?

- If an organization chooses to notify individuals on a one-to-many basis, e.g., through a notice on its website, is there a minimum period when the notification must be up for? Upon the end of this period, can the organization proceed on the basis that it can remove the notification on the assumption (which must be the case) that the individuals have read it?

  Or is it a case that once the notice is up, anyone who provides the data going forward would be deemed to have consented? We would like to seek PDPC's clarification with regards to data collected prior to the notice. Can we post the notice on our website for 1 month and thereafter, deemed consent is obtained from all individuals who had previously provided the data unless the individual opted out?

- Will there be a threshold for before a DPIA is required to be conducted? The collection, use and disclosure of personal data may sometimes be confined only to a specific group of individuals for a particular purpose.

- There is currently no clarity on the scope of the DPIA to be conducted if there is a legitimate Legal or Business Purpose for not obtaining consent and notifying the individual(s) for collecting, using and disclosing personal data. Will the PDPC prescribe the form and substance of the DPIA? What is the scope of the DPIA? We are of the view that the DPIA should not be overly onerous. Otherwise, if the time, effort and cost in conducting a DPIA outweighs the obtaining of consent, organizations may be better off continuing with the current practice. This is likely to be the case if the DPIA concept under the EU General Data Protection Regulation is adopted.

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

Yes, the PDPA should provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification.

The current framework assumes that individuals exercise their consent right. More often than not, an individual will give consent if he wishes to get a service or purchase a product without having regards to the terms of the consent. The "consent" framework merely creates an "artificial" control, right or choice to an individual. Allowing a notification to collect PII for legitimate business purpose with an opt out option may be a better approach. The key is that organisation must use the data for legitimate business purposes and protect the data from data breach.

In today's connected world, every user leaves a digital foot-print that can allow one to uniquely identify each user. Digitally speaking, the definition of user identifier is growing from traditional PII (NRIC, email address, Name, etc.) to device IP, social media account, etc. Additionally, when it comes to user identifiers online, there is a thin line between a prospective customer and an existing customer when they use our digital platforms, and it may not be easy to differentiate between them.

Here are few digital marketing use-cases where user consent/notification may not be possible (as proposed in section 3.2 and section 3.9 in the consultation paper):

- Site retargeting is a display advertising technique used to display advertisements to people who have previously visited their website. The marketer includes a pixel within their

webpage which sets a cookie in the user's browser. That cookie allows the marketer to target the website visitor with advertising elsewhere on the internet.

- People-Based Targeting online where digital footprints enable identification of single individuals as they engage across every device, every browser and every channel both on and off the website. It results in the ability to create individualized behavioural profiles that follow consumers throughout their journey, empowering brands to create seamless digital experiences on a one-to-one basis.

- Dynamic creative (also known as personalized retargeting), allows an advertiser to display a banner created on-the-fly for a particular consumer based on specific pages that they viewed. For example, if a consumer visits an website and browses products A, B and C - they will then be retargeted with a display banner featuring the exact products A, B and C that they previously viewed.

- Interacting with customers or potential customers on social media.

We have some queries:

- What is the definition of "Legal Purpose" and "Business Purpose"?

- What constitutes necessity for Legal or Business Purpose? Will PDPC be providing guidelines or a definition or will it leave it to the organization to determine?

- How does the organization determine if the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual? Will the PDPC be providing any criteria for such determination?

  If it is for the legitimate interests of an organisation without causing risk to the individual, it should be allowed to use the PII by way of notification.

  As PDPC has stated in its consultation paper, the "fast emerging Digital Economy is presenting challenges for consent-based approaches to personal data protection". We should take this opportunity to amend the law greater use of data via notification approach. Note that Australia adopted the notification approach and it has served its purpose. In this digital world of new technologies such as Internet of Things, Autonomous Vehicles, Drones, Artificial Intelligence, it is not possible to get all the consent necessary in anticipation that PII may be collected at certain points.

  As the world relies on data to drive business, it will not be possible to anticipate every scenario where data may be used for legitimate business purposes including data analytics. Hence, notification rather than consent is the viable approach.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

There is currently no clarity on the scope of the DPIA to be conducted if there is a legitimate Legal or Business Purpose for not obtaining consent and notifying the individual(s) for collecting, using and disclosing personal data. Will the PDPC prescribe the form and substance of the DPIA? What is the scope of the DPIA? We are of the view that the DPIA should not be overly onerous. Otherwise, if the

time, effort and cost in conducting a DPIA outweighs the obtaining of consent, organizations may be better off continuing with the current practice. This is likely to be the case if the DPIA concept under the EU General Data Protection Regulation is adopted.

Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?

We would like to share the following observations and queries:

- We are of the view that the criteria of "**any** risk of impact or harm" is too low a threshold. We suggest that it be revised to "**real and significant** risk of harm" instead. It is important to define the criteria and/or combination of criteria carefully to avoid panic and anxiety to the affected individual(s) especially when an organization has taken all reasonable steps to contain the breach. This is especially so if the breach arose from an isolated incident of human error without malicious intent. In addition, a low threshold for reporting will also result in increased costs of doing business. The approach taken by Australia makes sense ie "sufficient grounds to believe that the data breach is likely to result in serious harm to the individual" especially when the intent for the notification is to mitigate any real harm to individual due to a data breach.

- If the intent for mandatory notification is to protect individual from real risk, then this criteria for mandatory notification is not relevant. If there is a breach involving more than 500 individuals PII but would not cause harm to individual, it should remain under the current framework where no mandatory notification is required. If PDPC is still of the view that this is one criteria for mandatory reporting, this criteria should be condition on other factors. Otherwise, it may inadvertently catch situation of "unauthorised disclosure" due to genuine mistakes but unlikely to cause harm. Further, if the threshold is set at a low level, it may lead to huge volume of notifications to PDPC and this could lead to notification fatigue.

- In terms of the post breach guidance from PDPC, will this include mediation between organization and the affected individual(s) who may take the opportunity to unreasonably demand "compensation" from organization? If not, which independent third party can the affected individual(s) escalate their grievances to?

- PDPC should create awareness amongst the public and provide organisations with example templates of data breach notification communications to affected individuals.

We seek the PDPC's clarification on the following:

- In the event affected individual(s) ask(s) the organization for updates on the outcome of the notification to PDPC, i.e., action taken by PDPC (if any) against the organization, please clarify that the organization is not under any obligation to provide the information since the correspondence between PDPC and the organization is confidential to the parties.

- In relation to Paragraph 6.2(a): if the data breach does not contain information which poses a risk of impact or harm to the affected individuals, is the organization still required to notify the PDPC/individuals? For example, the breach involves a document which only contains name, address and a table showing the sum insured under the policy.

- Will the PDPC be publishing any guidelines on what constitutes risk or impact or harm to individuals?

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

We are of the view that the proposals are practical. Organizations will not have to file separate notifications for the same incident of breach.

Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

Public agencies should not come under the general exclusion of Section 4 of the PDPA. Oftentimes, they handle large volumes of sensitive personal data and are often the targets for cyber attacks.

In respect of Paragraph 6.10(a), does the law enforcement exception only apply if the law enforcement agency directs the organization in writing not to notify affected individuals because it may impede investigations? What can an organization do if it does not receive such a direction but is of the view that notifying affected individuals may impede investigations? Should the organization then engage with the law enforcement agency or PDPC or both?

In respect of Paragraph 6.10(b), please clarify if the PDPC will prescribe what amounts to reasonable standards of encryption.

In respect of Paragraph 6.11, please clarify what criteria the Commissioner will apply in deciding whether or not to exempt organisations from the breach notification requirements to cater to exceptional circumstances where notification to affected individuals may not be desirable.

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

We agree with the proposed time frames for data breach notifications to affected individuals and to PDPC.